ONLINE PAYMENTS: PAYING ONLINE SECURELY

Knowledge	Skills	Attitudes
Knows what online payment is	Able to pay online effectively and securely	Is curious about online payment tools
Is aware of the benefits and challenges in the use of online payment	Able to understand the logic and functionalities of online payment	Weighs the advantages and challenges of online payment and is capable to make a decision according to its personal situation
Understands how the online payment works	Able to identify its individual needs and use online payment functionalities accordingly	Is open to the usage of online payment tools
Knows what are the different types of online payment	Able to use the different types of online payment depending on concrete needs	Accepts to use online payment to perform multiple tasks, e.g. doing online shopping, paying for subscription
Understands how to use online payment safely	Able to ensure its own online payment security	Trusts the online payment environment and feels confident in its usage

Introduction to the module

If you have already clicked once on the *Pay* button, you might have already asked yourself how online payment works and whether it is safe or not to spend your money this way. Paying online for utility bills, insurance and other services, as well as doing online shopping, is less time-consuming and requires less effort. However, fraud and other cybercrimes question the security and thus reasonability of this payment method, making online payment feel sometimes like a curse and not a modern blessing.

Generally speaking, paying online is considered to be safer than any other payment methods, but it is crucial to keep in mind that some forms of payments are more secure than others, and some simple little steps may prevent some big losses.

In this module, having acquired some theory on online payment methods, some practical subjects, such as different online payment methods and security measures, will be discussed.

Co-funded by the Erasmus+ Programme of the European Union

This project has been funded with support from the European Commission under the Erasmus+ Programme. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein. [Project Number: 2021-1-FR01-KA220-ADU-000033422]

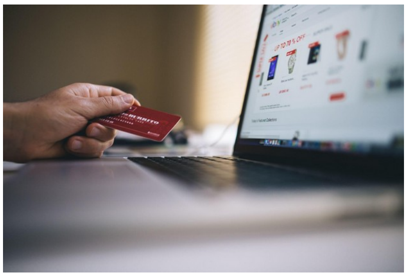
What are we going to learn in this module?

In this module we are going to learn:

- What is online payment?
- How does online payment work?
- What are the benefits of online payments?
- What are the different types of online payments?
- Is it safe to pay online and how to reinforce its security?

Why are those elements important in everyday life

Given the wide-spread nature of e-commerce and popularity of online payments while doing online shopping, understanding clearly how it works and how to reinforce its security will inevitably bring some clear benefits in our everyday life, or at least prevent some serious damages in the future.



Copyright: Pexels, Photo by Negative Space, [Black and Gray Laptop Computer With Turned-on Screen Beside Person Holding Red Smart Card in Selective-focus Photography · Free Stock Photo]

Understanding online payments, how it works

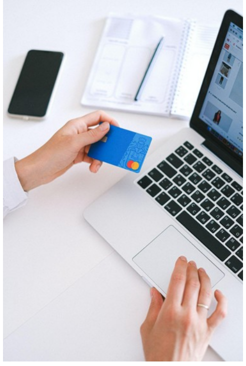
What is online payment?

Online payment is an electronic currency transfer through the internet between a merchant and a consumer in exchange for some services or products. The monetary funds transferred from a customer's bank or debit or credit card account, into the seller's bank account can come directly or from an online payment system that is linked to both the buyer and seller's bank accounts.

Nowadays online payments have a long-standing history dating back to 1994 with Pizza Hut executing an online payment for the first time to allow its customers to order pizza on its website. In 1997, Coca-Cola allowed customers to pay for their drinks by sending text messages from their phones, starting to take credit for the first mobile payment.

Co-funded by the Erasmus+ Programme of the European Union

This project has been funded with support from the European Commission under the Erasmus+ Programme. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein. [Project Number: 2021-1-FR01-KA220-ADU-000033422]



Copyright: Pexels, Photo by Anna Shvets from Pexels: Free Person Holding Bank Card Stock Photo

How does online payment work?

Clear understanding on how online payment works may be empowering and reassuring for all parties engaged in this process. In general, there are the following actors involved in this process:

- Customer
- Company, or a merchant selling products or services
- Payment gateway, i.e. software that handles the online transaction, and sends customer's payment information to a payment processing company
- Payments processing company that sends money to a merchant
- Customer's payment scheme, e.g. Visa or PayPal, and customer's bank issuing customer's credit/debit card

Online payment process obviously starts with a client selecting a particular service or product and proceeding to checkout. Then, a customer selects the most convenient payment option available to him and used by a merchant or a service provider. Once the customer's payment information is collected on the payment gateway, the purchase is sent to the payment processor as encrypted transaction data. Meanwhile, the payment processor uses customer information to collect payments on behalf of the merchant from the gateway which securely transmits data to the processor from the customer's bank. Once the transaction details are sent to the issuing bank, it authorises the payment. The acquiring bank receives an electronic payment transaction on behalf of the merchant and transfers it to his account. Online payment is completed!

Time for a quiz! Yes or no

Online payment starts with a merchant. **No**

Merchant selects the most convenient payment method for a client. **Yes**

At the final stage of the online transaction, the acquiring bank receives an electronic payment transaction on behalf of the merchant and transfers it to his account. **Yes**

Co-funded by the Erasmus+ Programme of the European Union

This project has been funded with support from the European Commission under the Erasmus+ Programme. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein. [Project Number: 2021-1-FR01-KA220-ADU-000033422]

Advantages of online payments

Online payment is **secure** and protects consumer information, thus decreasing the chance of personal information being stolen. Online payments are frequently instantaneous or **fast** and free of any time or distance constraints. Paying online is **convenient** and improves the buying experience taking less time and effort. Putting some security measures in place and choosing the most convenient online payment method for you will maximise the benefits of online payments for you and minimise the potential risks associated with it.

Payment methodss for online transactions

Online payment methods

There are numerous ways to make an online payment, e.g. via credit and debit cards, banking apps or web pages. The choice depends on your preferences and the availability of these options by the various service providers. Each online payment method has clear advantages and disadvantages, thus each consumer should choose what works best for them.

- PayPal

PayPal is an eCommerce payment processing company that allows users to set up a PayPal account without entering credit card details in each website. It’s popular because it is an easy-to-use, secure and simple way to checkout online. Today, PayPal has over 250 million users worldwide, and is well known across the globe. Rules and fees will vary, depending on the currency being used and the amount transacted. This can sometimes cause inconvenience to some customers.

- Amazon Pay, Google Pay and Apple Pay

Similar to PayPal, Amazon Pay is a payment processing service that allows customers to pay online on third party websites. Using the details entered previously on a customer's Amazon account, one can complete the transaction rapidly.

Just like Amazon Pay, if you have already bought something on Google, Google Pay or Google Wallet stores payment information of its customers and may be used for online payment on third party websites for free via mobile phones, tablets, or watches.

Much like with Google and Amazon Pay, Apple users can pay online using their IPhones, Mac computers, watches and IPads for free. The service allows authentication with Touch ID fingerprint or Face ID which makes the online payment even faster and easier.

- Credit card payments

Credit card payments are probably the most frequent and secure way of paying online available at almost each website. Most credit cards have very strong consumer protections and in addition to a two-factor authorisation (2FA), at an online checkout, i.e. an extra level of security to prove it’s you making the purchase, this method becomes highly secure.

Co-funded by the Erasmus+ Programme of the European Union

This project has been funded with support from the European Commission under the Erasmus+ Programme. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein. [Project Number: 2021-1-FR01-KA220-ADU-000033422]

One drawback of using this payment method is that it may take time to type in credit card details and some may want to avoid this to prevent misuse of the information typed in. Anyway, it is better to avoid saving your credit card details to prevent stealing.

- Direct debit payments

Direct debit payments are quite convenient for recurring, automated payments to be made instantly, e.g. for monthly subscription payments, but their security level is lower than in other online payment methods, according to some. Checking the security measures put in place by your bank may be a good idea in this case.

Copyright: Photo by Antoni Shkraba: https://www.pexels.com/photo/photo-of-a-person-shopping-online-6207736/

Paying online securely

Generally speaking, online payments are more secure than any other types of payments. However, given the number of frauds and other cybercrime, every customer should ensure that some security measures are implemented each time while purchasing.

Step 1: Avoid paying online while being connected to public wifi privileging mobile data networks instead.

Step 2: Check that you are on the provider's genuine site. Sometimes you can be forwarded to other websites without actually noticing it. Make sure that URL corresponds well to the merchant's website to avoid paying at clone websites. Usually, big retails are more secure than little ones, but a simple check should be made every time regardless of the website's popularity.

Step 3: Double check all details of your payment before confirming, i.e. the nature of your purchase, the quantity, etc.

Step 4: Before entering payment card details on a website, ensure that the link is secure, in two ways:

- Find a padlock symbol in the browser window frame, which indicates a secure communication channel between the browser and the server on which the website is hosted. Be sure that the padlock is not on the page itself (this will probably indicate a fraudulent site) but is near the URL bar (in most cases).
- Check that the web address starts with 'https://', with 's' standing for 'secure'.

- Check the address for subtle misspellings, additional words and characters and other irregularities.

Step 5: Read the website's privacy policy and log out of sites instead of simply closing your browser.

Step 6: Keep receipts in an electronic or any other form. Do not save your credit card details on a website.

Step 7: Once you made payment, check your credit card and bank statements to ensure that the correct amount has been debited, and also that no fraud has taken place as a result of the transaction.

Having effective and updated antivirus software is also a good online security measure.

Time for a quiz! True or False

1. It’s important to check the merchant’s URL to ensure that it is not a clone website. (**TRUE** - checking the merchant’s website URL should become a habit for all online purchases)
2. Subtle misspellings, additional words and characters and other irregularities in the merchant’s URL do not matter that the website is not secure. (**FALSE** - identifying subtle mistakes may prevent you from paying on clone websites and identify a potential scam, which may appear quite secure at the first glance)
3. There is no need to check your credit card and bank statements to ensure that the correct amount has been debited. (**FALSE** - checking your credit card and bank statements may permit you to ensure that you have been debited the right amount for the purchase you wanted to make, and if not to contact your bank immediately to block it if it is still possible)
4. ‘S’ in ‘https://’ in the website addresses stands for scams, so it is better not to have it included. (**FALSE** - ‘S’ in the website addresses means ‘security’, so it is important to check that it is well indicated in URL)

WRAP UP – most important points of this module

1. Online payment is a convenient and secure payment method well-developed and widely-spread all around the world.

2. There are various actors engaged in carrying our online money transactions making it sometimes a complex but easily understandable well-regulated payment method.

3. Depending on customer’s preferences and availability on merchants' websites, there are numerous ways to pay online securely and fastly.

4. Some simple security measures, that should rather become a habit, should be made every time to prevent some money or data losses.

Co-funded by the Erasmus+ Programme of the European Union

This project has been funded with support from the European Commission under the Erasmus+ Programme. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein. [Project Number: 2021-1-FR01-KA220-ADU-000033422]

ONLINE BANKING: Accessing banking services via your technological devices

Knowledge	Skills	Attitudes
Knows what online banking is	Able to understand the logic and functionalities of online banking	Is curious about online banking tools
Is aware of the advantages and challenges in the use of online banking	Able to identify its individual needs and use online banking functionalities accordingly	Weighs the advantages and challenges of online banking and is capable to make a decision according to their personal situation
Understands the procedure to create an online banking account and to connect to it	Able to use ICT tools and digital technologies (smartphone, computer and tablet) to access online banking	Is open to the usage of online banking tools
Knows what are the different functions offered by online banking	Able to use the different online banking functions: payment, transfer, consulting statement	Accepts to use online banking to perform multiple tasks; paying bills, transferring money, check statement
Understands how to use online banking safely	Able to protect its own devices: choose a safe password, find solutions to eventual usage problems and secure the use of ICT tools.	Trusts the online banking environment and feels confident in its usage

Introduction to the module

Online banking is also known as internet banking, net banking or e-banking. It allows you to access banking services via your technological devices: smartphone, tablets and computers. Through online banking you can pay your bills, transfer money, invest funds or contact your bank.

There are two types of online banking: your traditional bank can offer you an online platform service allowing you to manage your current account and investments, this comes as an extra service to physical branches and it is for free. Or your bank can be completely online meaning that all the services and relations with advisers are done through the online platform. This module was conceived to be usable in both cases.

Co-funded by the Erasmus+ Programme of the European Union

This project has been funded with support from the European Commission under the Erasmus+ Programme. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein. [Project Number: 2021-1-FR01-KA220-ADU-000033422]

What are we going to learn in this module?

In this module we are going to learn:

- What is online banking?
- What are its advantages?
- What are the main challenges in its use?
- What are the main services available online and how to access them?
- How to use online banking safely and with confidence?

Why are those elements important in everyday life?

New technologies and the internet have transformed our everyday life and banking activities are not an exception. The evolution of the banking sector is very rapid with the diminution and closing of physical branches and the multiplication of online services. It is important for seniors to know about these services and feel confident in using them as having access to banking is one of the essential components of societal inclusion. Moreover, in many aspects, online banking can simplify every-day life, as long as we can use it confidently and securely.

Understanding online-banking, its advantages and challenges

What is online banking?

Banks' online systems enable their customers to make financial and non-financial transactions online via the internet. It gives online access to almost every banking service, traditionally available through a local branch.

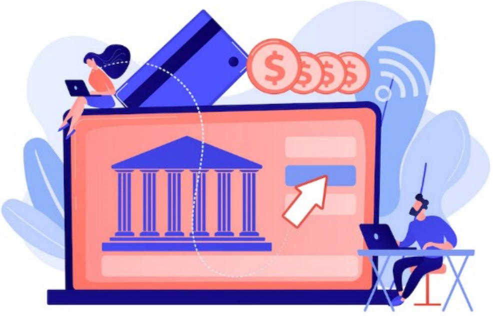
This service evolved simultaneously with the development of the world wide web. The first online banking platform started in the United Kingdom in September 1983. By 2017 already more than half of EU inhabitants were using it.

Online banking means any user with a personal device (smartphone, tablet, computer) and a browser can get connected to his/her bank´s website to perform any of the virtual bank functions:

- Balance enquiry
- Transfer of funds
- Online payment of bills
- Accrued interest, fees and taxes
- Transaction details of each account
- Accounts, credit card & home loan balances
- Transfer funds
- Open a deposit

Co-funded by the Erasmus+ Programme of the European Union

This project has been funded with support from the European Commission under the Erasmus+ Programme. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein. [Project Number: 2021-1-FR01-KA220-ADU-000033422]



Copyright: Vector Juice

Online banking use in Europe [1]

Online banking is particularly popular among 25 to 34-year olds, its use tends to increase in line with the education level of the user.

In 2021, among EU Member States, internet banking is most common in Norway, Denmark, the Netherlands and Finland being used by more than 90% of the population.

Online banking penetration is 61% on average in Europe, 72% in France and in the Czech Republic, 65% in Cyprus, 52% in Poland and 45% in Italy.

The lowest shares were registered in Bulgaria and Romania with 15%.

The advantages of online banking

For banks, online banking allows larger customer coverage, reducing the costs of operations and promoting their services and products nationally and internationally.

For customers, it is very convenient, being accessible 24 hours a day, seven days a week. It offers more beneficial rates, additional free services, facility in transactions, unlimited transfers at no costs and easiness of use. Transfers are faster, greener and easier to monitor.

The challenges of online banking

The main challenge in the use of online banking concerns the lack of person-to-person relationship.

There is a need for ICT skills for customers. People who are not familiar with ICT tools might find it difficult to use and time consuming.

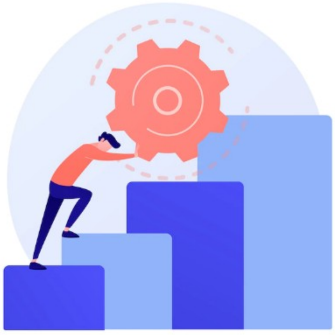
There is also a security issue: increasing number of fraudulent sites, fake emails, use of trojan virus to capture IDs and passwords, hacking…

[1] https://www.statista.com/statistics/222286/online-banking-penetration-in-leading-european-countries/

Co-funded by the Erasmus+ Programme of the European Union

This project has been funded with support from the European Commission under the Erasmus+ Programme. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein. [Project Number: 2021-1-FR01-KA220-ADU-000033422]

In the next parts of this module, we will address all these challenges in order for you to learn how to use internet banking with confidence and securely.



Copyright: Vector Juice

Time for a quiz! Select the right answers

What is online banking? (check all that apply)

- A tool to choose your bank online
- An online system managed by your bank giving you access to many banking services
- A tool to plan meetings online with your bank adviser
- A tool to transfer money and make payments online

What are the advantages and challenges of online banking? (check all that apply)

- It is very time consuming
- It allows to have 24h access to banking services
- You need to have certain ICT skills to use it
- It is not very secured
- You have limitations in its use (amount of transactions allowed, amount of connexions allowed)

Online banking services in practice

Opening an account

For “online only” banks

You can open a checking, savings, and other types of account online often without printing or physically signing anything.

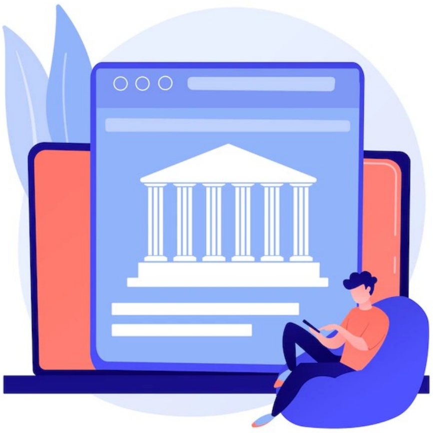
This project has been funded with support from the European Commission under the Erasmus+ Programme. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein. [Project Number: 2021-1-FR01-KA220-ADU-000033422]

With the electronic signature, the entire process might take you less than 10 minutes.

For traditional banks

If you're a customer of a traditional bank that offers online banking, you can register for online access through their website or directly with your personal advisor. At a minimum, you'll usually need the following items to get started online:

- An internet connection
- A device with a web browser: a computer, tablet, or smartphone
- Your bank account number
- Personal information to verify your identity, such as your birth date and Social Security number
- A password



Copyright: Vector Juice

Paying your bills

You can pay bills over the web from a bank account most often at no extra cost. It takes a few minutes to set up your online bill payment. Once it's set, you don't have to worry about missing your payments.

Here is the information you need to provide:

- Name of the person or business
- Address
- Bank account number

Co-funded by the Erasmus+ Programme of the European Union

This project has been funded with support from the European Commission under the Erasmus+ Programme. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein. [Project Number: 2021-1-FR01-KA220-ADU-000033422]

- Amount of money to transfer
- Reason of the transfer/Identification of the transfer
- Currency (ie. euros, dollars etc.)

The bank will issue an electronic payment using funds drawn from your account within one to five days. If a recipient is already set up within the bank's system, the money transfer is issued on the same day. Usually there is no limit on the number of bills you can pay through the feature.

Once the payment is set-up, your bank will generally give you the following options:

One-time payments: This is a payment you issue a single time. This option makes sense for services you use infrequently, such as a landscaper or a lump-sum payment on a car.

Future payments: This online bill pay option gives you the ability to schedule payments at a later date. Use this online bill payment option when your bill due date isn't in the near future but you want to set up a payment in advance so that you don't forget it later.

Recurring payments: These are generally payments you make at regular intervals, such as monthly or quarterly. Ex: Health insurance premium bills, utility bills, childcare etc.

Transferring funds and investments

If you need to move money from your current account to your savings account, you can carry out these interbank transfers online.

You can even link your accounts at different banks or send money to friends and family almost instantly through person-to-person services accessible through your bank.

You can also control your investments online through the dedicated page.

Copyright: Vector Juice

Co-funded by the Erasmus+ Programme of the European Union

This project has been funded with support from the European Commission under the Erasmus+ Programme. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein. [Project Number: 2021-1-FR01-KA220-ADU-000033422]

View transactions and get your monthly statements

Most banks make it easy to check your available balance, verify your latest transactions that went through, and review previous monthly statements online. You should be able to search transactions by time frame and type. There is also one section dedicated to monthly statements and you can get them within one click.

Copyright: Flaticon

Order a checkbook or cancel your credit card

There are also available sections to order a check book and cancel your credit card within a few clicks.

Staying informed

Through your online banking profile, you are able to set- up alerts. You can receive a text or email when your bank notices potentially fraudulent activity or your balance goes below a certain amount. You can also be notified when deposited money is available and when a check has cleared. These alerts are great for informational purposes, but more importantly, they can help you quickly stop fraudulent activity.

Co-funded by the Erasmus+ Programme of the European Union

This project has been funded with support from the European Commission under the Erasmus+ Programme. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein. [Project Number: 2021-1-FR01-KA220-ADU-000033422]

Copyright: Vector Juice

Using online banking safely and with confidence

Connecting

Step 1: Make sure your computer is connected to a private internet network protected by a password.

Step 2: Go to your bank's website. For security reasons, do not click on a link sent to you in an email – emails with links to fake websites can be quite common.

Step 3: In order to create your online banking profile, contact your bank (call your advisor, go to their website etc). You will need some key identification that is associated with your account, such as social security number, birth date and/or account number.

Step 4: You will be given your online bank identification number. You will also need a password. There is usually a double authentication system which means there are two passwords to be inserted. One password is chosen by you and is fixed. The other password is provided by your bank and is an automatically generated code that changes every time you connect. It is usually sent to your mobile phone by SMS or on a token given to you by your bank. This information is explained to you by your bank when you register to open your online banking profile.

Step 4: Once you have logged in, you will typically see a page listing all your accounts, along with their current balances. This page is usually called "My accounts" or "Dashboard", depending on your bank.

- You will see the different types of transactions that you can perform.
- Usually on the left side of the screen there will be a list of functions. Click on a function to open it.
- For example, if you want to transfer funds, click on the button or icon labelled "Transfer" or something similar. You will need to complete the required data.

Co-funded by the Erasmus+ Programme of the European Union

This project has been funded with support from the European Commission under the Erasmus+ Programme. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein. [Project Number: 2021-1-FR01-KA220-ADU-000033422]

Step 5: Once you have finished, be sure to log out from your account (usually on the top right corner of your profile). Most banks also have in place a „time out“ feature, which means that if you are inactive for a certain period in your internet banking session you will automatically be logged out.

Our security tips:

- Only access online banking on your **own computer** and not on a public computer
- Only use a **secured and closed** internet network
- Keep your computer or other device (tablet and smartphone) **up to date** with **anti-virus and firewalls** activated
- Enter the address of your bank yourself in the browser, **do not click on a link** sent by email or other. Make sure the address starts by “https” which means the **security certificate** of the page is up to date
- Be careful with **phishing** emails (*see dedicated module 11*)
- If you are asked by email or telephone for your online banking credentials, credit card code or other sensitive information, do give it under any circumstances! **No bank will ever ask you for this!**
- Create a **secure password** with numbers, letters, capital letters and symbols.
- **Do not store your passwords** in a document on your PC!
- Make sure you have **account limits** for payments and transfers
- **Check your account activities regularly**; in case of irregularities, contact your bank's hotline or helpdesk immediately, change your password and, if in doubt, have the account blocked.
- **Download your bank statement and credit card statement frequently** every month and save them in folders on your PC. Account statements are only kept for up to 12 months in online banking.

Copyright: Vector Juice

Co-funded by the Erasmus+ Programme of the European Union

This project has been funded with support from the European Commission under the Erasmus+ Programme. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein. [Project Number: 2021-1-FR01-KA220-ADU-000033422]

Time for a quiz! True or False

Your bank is the only one responsible for the security of the use of online banking (False – you can also insure a safe use by keeping your ICT tools up to date, choosing a secure password etc).

If your bank asks you for your credit card password you are obliged to give it to them (False – Your bank will never ask you personal data or password by email, this is phishing).

To use online banking you need to create an account, authenticate yourself, have an ICT device and an internet connection. That's all (True)

WRAP UP – the most important points of this module.

1. Online banking is a practical and convenient way to manage your current account and savings. Its use is more and more disseminated in Europe.
2. There is a strong authentication process to connect to your online banking profile
3. You can pay bills and transfer funds rapidly, you just need the bank account number of the recipient.
4. For payments you can set-up "one-time payments", "recurrent payments" or "future payments"
5. Online banking allows you to stay informed by setting up alerts, checking your current account statement and the status of your transfers and payments sent and received.
6. It is also a safety tool as you get notified of potential fraudulent actions, you can even block your credit card in a few clicks.
7. If you follow some basic tips, online banking doesn't represent a risk, on the contrary, it is trustworthy and a tool to insure the security of your funds.

Co-funded by the Erasmus+ Programme of the European Union

This project has been funded with support from the European Commission under the Erasmus+ Programme. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein. [Project Number: 2021-1-FR01-KA220-ADU-000033422]

NETIQUETTE IN VIRTUAL MEETINGS: RULES FOR POLITE BEHAVIOUR WHEN COMMUNICATING WITH OTHER PEOPLE ON THE INTERNET

Knowledge	Skills	Attitudes
Knows what is NETIQUETTE in virtual meetings	Knows the definition of netiquette.	Willing to fact-check a piece of information and assess its accuracy, reliability and authority, while preferring primary sources over secondary sources of information where possible.
Understand the Rules of netiquette	Knows the differnt rules on netiquette in different social media	Considers the netiquette tips for general aspect and to be sure to respect the other.
Understand how to behave on social networks and through online chats	Knows about how to behave on social networks and through online chats	Takes responsibility for behaviour when you are in chats, internet, social media channels.

Co-funded by the Erasmus+ Programme of the European Union

This project has been funded with support from the European Commission under the Erasmus+ Programme. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein. [Project Number: 2021-1-FR01-KA220-ADU-000033422]

Introduction to the module

The Internet plays an enormous part in our lives, allowing us to communicate, share information with others and even run businesses. With so much of our lives dependent on the Internet, it is important for us to understand how our online behavior can impact us and others.

By nature, verbal and personal communication is impermanent. Communication on the Internet, on the other hand, is more permanent. Whether it is a video recording of a meeting or shared notes and photos, the Internet retains everything. The online mode of communication adds abstraction between participants. Because there is a barrier in the form of a screen among people, it can be easy to ignore the social etiquette that we would follow otherwise in face-to-face communication.

What are we going to learn in this module?

This modul consists of:

- Definition of the expression netiquette
- Netiquette
- Rules of netiquette
- How to behave on social networks and through online chats
- Conclusion

Why are those elements important in everyday life

Virtual meetings are becoming more and more common not only due to the events of the pandemic. Oral or in-person communication has the benefit of body language, tone of voice and facial expressions that add to the communication between sender and recipient. Written communication is devoid of this luxury, often making the writer’s intent unclear.
This is the primary reason for the presence of online etiquette—to allow us to communicate well virtually. Most websites and social media platforms have defined the rules of online behavior that users must follow.
Such codes have been put in place to ensure people interact effectively and avoid conflicts. There can even be legal implications for not following the net etiquette.

Definition of *Netiquete*

Netiquette is a made-up word from the words net and etiquette. Netiquette thus describes the rules of conduct for respectful and appropriate communication on the internet.

Time for a quiz! Select the right answer

True or False:
Netiquette is a made-up word from the words net and etiquette (TRUE)

Co-funded by the Erasmus+ Programme of the European Union

This project has been funded with support from the European Commission under the Erasmus+ Programme. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein. [Project Number: 2021-1-FR01-KA220-ADU-000033422]

This project has been funded with support from the European Commission under the Erasmus+ Programme. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein. [Project Number: 2021-1-FR01-KA220-ADU-000033422]

Netiquete

Netiquette is often referred to as etiquette for the internet. These are not legally binding rules, but recommended rules of etiquette. Netiquette is mostly used for dealing with unknown people on the internet. The rules of netiquette depend also on the platform and its participants. Generally, it is up to the operator of a website, communication app, or meeting leader to specify the type and scope of netiquette. It is also their responsibility to monitor compliance with these basic rules and to penalize violations of them.

When communicating on the internet, people should always remember that they are communicating with other people, not with computers or smartphones. As in the real world, rules of etiquette are necessary on the internet. Netiquette is therefore important to avoid adverse consequences.

Rules of netiquette

1. Be Cautious with Sarcasm

Even if you have a sarcastic personality, be very cautious using it online. People cannot read your tone of voice or facial expressions, so that sarcasm is lost when you're typing. In fact, sarcastic comments have ruined friendships and caused serious disagreements online, all when the issue at hand was not actually something worth arguing over.

2. Never Send Spam

You hate junk emails. So do your classmates. You hate spammy posts circulated on social media. So do your classmates. Before forwarding or posting something, verify the source as credible. Stop circulating the chain letters and rumors that make the Internet a time waster.

3. Use Good Grammar

Yes, it may just be a forum post, but if it's filled with typos and poor grammar, it may reflect poorly on you. Use proper language whenever possible, and avoid casual abbreviations (lol, ttyl, brb) that could be misunderstood or misinterpreted by some.

4. Consider your email address

From the address and subject line, your emails should reflect a high level of professionalism. The email address you use should be free of nicknames, slang, or strange spellings. Consider separate addresses for personal and professional use.

5. Avoid the Temptation to Over Share

Discussion forums can offer a chance to share your learning experiences, but remember these are platforms for thoughtful, academic conversations. Avoid posting personal information

6. Don't Type in ALL CAPS

In online communication, ALL CAPS is considered yelling. This is not a way to emphasize what you are saying. It is rude and can be considered offensive. If you need to emphasize something, use italics or bold typeface instead of all caps.

7. Practice the Golden Rule

When you are online, remember to "do unto others as you would have them do unto you." Treat people the way you would like to be treated, and you will avoid quite a number of potential problems. Remember, on the other side of that computer screen is a real person with thoughts and feelings just like you, so talk to them with kindness.

This project has been funded with support from the European Commission under the Erasmus+ Programme. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein. [Project Number: 2021-1-FR01-KA220-ADU-000033422]

8. Return Messages Promptly

If someone sends you an email or an online message, send them a response quickly. If you cannot send a thorough reply, at least acknowledge that you received the message. People often wonder if their messages went through when they send them online, so when you send an acknowledgment they will have peace of mind that their message did, in fact, get received.

9. Respect the Privacy and Rights of Others

If you have someone's permission to share their words, then do so, but remember that people's words are their own property. Do not forward personal emails or share statuses without the original person's permission. If you know information about someone, do not share it online without asking them first.

10. Identify Yourself

Identify yourself in online communications, like email. Let the recipient know who you are. Don't forget to sign the email at the end. Treat the email with the same professionalism you would use with a written communication.

The power of the Internet has created a world where communication takes place through a screen, rather than in person. It's critical that you practice good manners and have your netiquette in hand every time you go online and interact with people.

How to behave on social networks and through online chats:

1. **Keep the good education.** It is a basic rule that, although it seems obvious, is not always so in communication that does not occur face to face. We look at examples of how to lose shape on a daily basis on social networks like Twitter.
2. **Respect each other's bandwidth.** This implies not sending by email or instant messaging files of great weight or difficult to download.
3. **Don't send pictures or videos of other people,**especially if they're intimate.
4. Also, do not disseminate **private information** about yourself or others.
5. Take care of spelling. Unfortunately, this is one of the points to which less attention is currently paid.
6. In e-mails, it retains **the structure of traditional mail.** Includes subject, greeting, theme to develop, farewell and signature. If there are any attachments, mention them.
7. In forums, chats, social networks or WhatsApp groups, **express your opinion with respect** and never attacking others.

Time for a quiz! Select the right answer

What is condider if you write ALL CAPS in online communication?

1. Important
2. How are you?
3. Hello
4. Spam
5. Yelling

How i need to express my opinion in whatsApp groups?
1. Never express your opinon
2. Respect
3. With blue color

Time for a quiz! True or False

This project has been funded with support from the European Commission under the Erasmus+ Programme. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein. [Project Number: 2021-1-FR01-KA220-ADU-000033422]

If someone’s don´t give permission to share their words, i can do it ?

FALSE, Remember that people’s words are their own property and you cannot share without permision, if you have someone’s permission to share their words, then do so.

WRAP UP – most important points of this module

1. Netiquette in the virtual world is just as important as netiquette in the real world.
2. Although the user is in a home environment, he should behave, dress and adapt as if he were in a public place.
3. Always read the rules of use of the social network and try to comply with them
4. Few important steps to rememeber (No capital letters when you write, respect, privace in your conversation, no informtation, no pictures)

Co-funded by the Erasmus+ Programme of the European Union

This project has been funded with support from the European Commission under the Erasmus+ Programme. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein. [Project Number: 2021-1-FR01-KA220-ADU-000033422]

DATING APPS: Seniors dating online

Knowledge	Skills	Attitudes
Knows what dating apps are and what are their functionalities	Is able to use the multiple functionalities of dating apps	Is curious about online dating apps
Is aware of the advantages and challenges in the use of dating apps	Is able to identify individual needs and use online dating apps accordingly	Weights the advantages and challenges of online dating and is capable to make a decision according to its personal situation
Understands how to use online dating apps safely	Is able to safely connect from one's own device, to protect its own personal data and to avoid risk situations and scams	Trusts the online dating environment and feels confident in its usage

Introduction to the module

What are dating apps? Through this module, you will understand how dating mobile applications work and what are the advantages and challenges in using them to connect with others to seek romance, casual sex or friendship. Dating apps are gaining popularity with the senior population. Some of them target all age groups, while others target only seniors who have specific dating needs and behaviours. It is important to know what you are looking for and expecting in order to choose the most adapted app. It is also crucial to know security tips when using them to avoid the most common scams and risks and fully benefit from all they have to offer.

What are we going to learn in this module?

In this module we are going to learn:

- What are online dating apps?
- What are its advantages? What are the main challenges in its use?
- How to choose the most adapted app?
- How to use online dating apps safely and with confidence?

Why are those elements important in everyday life?

Dating at any age may be scary and often challenging. Being in the over-60 group may mean that more people your age are not interested in building new romantic relationships — but online dating can prove that the mature dating isn't limited, you can **go beyond your physical everyday life encounters**. It's quite normal to feel hesitant about making the jump to online dating as a senior. Finding a dating app that feels comfortable and natural is a challenge at any age.

Understanding online dating, its advantages and challenges

What are online dating apps?

Dating apps are software applications designed to **generate connections between people who are interested in romance, casual sex, or friendship.** They offer an online dating service presented through a mobile phone application, often taking advantage of a smartphone's GPS location capabilities, always on-hand presence and easy access to digital photo galleries to enhance the traditional nature of online dating.

Seniors' Behaviour on Dating Apps

Many studies have underlined seniors' behaviour when using dating apps. A literature review is available here. Below, you have its main conclusions:

There are significant **differences between younger seniors (aged 60–74) and older seniors (above 75),** with younger seniors being more likely to mention adventure, romance, sexual interests and seeking a soul mate, and less likely to mention health. Older seniors were more positive in their profiles and focused more on connectedness and relationships with others.

Overall, older men and women are interested in a **companion** and in someone fun, loving, kind and compassionate. Additionally, women seek a partner who is honest and engages in leisure activities with them, whereas men seek women who are physically attractive and provide emotional support. In any case, **older adults value interpersonal communication more than sex appeal.**

Copyright: PCH vector

The advantages of online dating

Many of the applications **provide personality tests** for matching or use **algorithms** to match users enhancing the possibility of finding a compatible candidate.

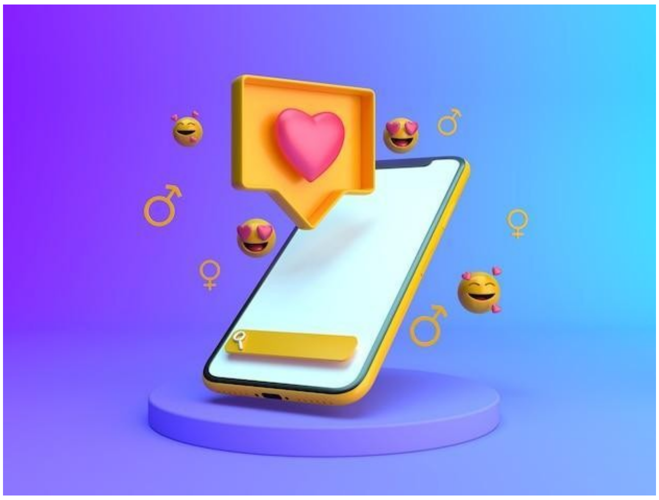
Users are **in control**; they are provided with many options in terms of matching and communication with others.

Narrowing down options is easy. Once users think they are interested, they are able to chat and get to know the potential candidate. This type of communication **saves time and money.**

This project has been funded with support from the European Commission under the Erasmus+ Programme. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein. [Project Number: 2021-1-FR01-KA220-ADU-000033422]

Online dating offers **convenience**; you can chat at any time of the day.

It can also increase **self-confidence**; even if users get rejected, they know there are other candidates that will want to match with them.



Copyright: Freepik

The challenges of online dating

Sometimes having too many options can be **overwhelming**. In addition, the algorithms and matching systems put in place may not always be as accurate as users think.

Communication online also lacks the physical chemistry aspect that is essential for choosing a potential partner. Much is **lost in translation** through texting.

After analysing a significant number of diverse mobile dating applications, researchers have concluded that most of the major dating applications are vulnerable to simple attacks, which could **reveal very sensitive personal information** such as sexual orientation, preferences, e-mails, degree of interaction between users, etc. Furthermore, online dating platforms are also becoming breeding grounds for fake profiles to steal users' private information. If you are scared after reading all that, don’t worry! **The whole section of this module is dedicated to security tips!**

Finally, an issue amplified by dating apps is a phenomenon known as **'ghosting'**, whereby one party in a relationship cuts off all communication with the other party without warning or explanation. Ghosting poses a serious problem as it can lead to users deleting the apps. Some apps have features that make it easier for users to end chat conversations more politely.

Time for a quiz, select the right answer

Dating apps allow you to meet people online

Dating apps allow you to look for specific services people might offer you

Dating apps are only relevant for romantic or sexual encounters

Co-funded by the Erasmus+ Programme of the European Union

This project has been funded with support from the European Commission under the Erasmus+ Programme. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein. [Project Number: 2021-1-FR01-KA220-ADU-000033422]

Some dating apps are not adapted to seniors

Dating apps allow you to save time and money

Dating apps can reveal your sensitive and personal information

Ghosting is a phenomenon where a person lies about his or her identity

Online dating in practice

Choosing the best app for you

Here are some elements you can consider when choosing an online dating app:

- **What kind of relationship are you looking for?** Do you want a companion to spend time with as you head into retirement? Do you want someone younger who can keep up with your fast-paced lifestyle? Maybe you just want something casual and exciting (no shame!).
- **How popular is the application?** The more popular, the better. Having many users means lots of chances to match with someone.
- **Ease of use:** Most apps are pretty straightforward — but certain ones are much clearer and easier to sign up for than others. Certain apps will give you a multi-step sign-up with endless questionnaires to better match you—but there are many apps that skip over and get straight into browsing around.
- **Social media integration**: Dating apps with social media integration are great tools to make sure you're chatting with real people and not bots or catfish. There are even apps that only match you with friends-of-friends if you're particularly concerned on that front.
- **Security:** Make sure the app you're signing into offers photo verification and the ability to block any unwanted members who might be looking for a target to take advantage of.
- **Budget:** There are lots of free apps out there — but sometimes the free version lacks in-depth features and other aspects that make meeting someone easier. You are not obliged to choose paying apps, it all depends on your wishes and expectations.
- **What others are saying:** Before you sign up for a dating app, it doesn't hurt to read a couple of user reviews.

Give examples of the most used dating apps in each country

In France some apps you can test are: Tinder, Meetic, Happn, Elite Rencontre, Disons Demain, Cupid.

Using online dating apps with confidence

Subscribing and connecting

Step 1: Download the app on Android or IOs. If it is only available as a website, connect to the website on your computer.

Step 2: Go to the section "create an account" and complete all necessary information.

Step 3: Usually it will ask you to enter a phone number and email. It will send you a sms to verify your phone number and an email to verify your email account.

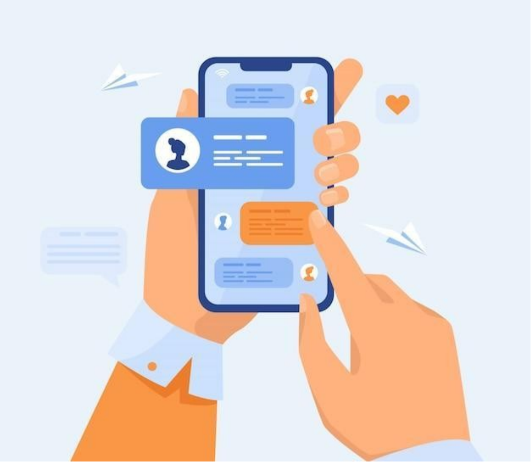
Step 4: The app can also give you the option to link it to your social media account (i.e. Facebook)_

Step 5: Set up your profile: choose a nice picture, write a description of yourself, your hobbies, expectations.

Step 6: If the application asks to have access to your GPS position, you can allow it, it facilitates matching with people around you.

Most common dating app features:

- A well-thought-out profile creator
- Effective matchmaking (i.e. swiping for Tinder, algorithms)
- Algorithms that match people according to their hobbies, geographic location and interests
- Instant chat
- Tagging and advanced search filters
- Photo and video sharing
- Relationship assistance
- Advanced security and privacy features (hide location if you want, block people, report people)
- Easy navigation



Copyright: PCH Vector

Our security tips:

When connecting online:

Avoid connecting with suspicious profiles: If the person you matched with has no bio, linked social media accounts, and has only posted one picture, it may be a fake account. It’s important to use caution if you choose to connect with someone you have so little information about.

Check your potential date on social media: If you know your match’s name or handles social media—or better yet if you have mutual friends online—look them up and make sure they aren’t “catfishing” or using a fake social media account

Block and report suspicious users. You can block and report another user if you feel their profile is suspicious or if they have acted inappropriately toward you. This can often be done anonymously before or after you've matched.

Here is a list of suspicious behaviours:

- Asks for financial assistance because of a sudden personal crisis
- Claims to be recently widowed with children
- Disappears suddenly from the app and reappears with a new name
- Gives vague answers to specific questions
- Overly compliments or is romantic too early in the conversation
- Pressures you to talk outside the dating app
- Request your home or work address to send flowers
- Tells inconsistent or grandiose stories

Here is a list of behaviours you should report:

- Requests financial assistance
- Sends harassing or offensive messages
- Attempts to threaten you or intimidate you
- Tries to sell you products or services
- You have proof it is a fake profile

Careful when sharing personal information. Never give someone you haven't met in person your personal information, including your: social security number, credit card details, bank information, or work or home address. Dating apps and websites will never send you an email asking for your username and password information, so if you receive a request for your login information, delete it and consider reporting.

Don't Respond to Requests for Financial Help. No matter how convincing and compelling someone's reason may seem, never respond to a request to send money, especially overseas or via wire transfer.

When meeting in person:

Video chat before you meet up in person. This can be a good way to help ensure your match is who they claim to be in their profile. If they strongly resist a video call, that could be a sign of suspicious activity.

Tell a friend where you're going. Take a screenshot of your date's profile and send it to a friend. Let at least one friend know where and when you plan to go on your date. If you continue your date in another place you hadn't planned on, text a friend to let them know your new location.

Meet in a public place. For your first date, avoid meeting someone you don't know well yet in your home, apartment, or workplace. It may make both you and your date feel more comfortable to meet in a coffee shop, restaurant, or bar with plenty of other people around. Avoid meeting in isolated locations for first dates.

Don’t rely on your date for transportation. It's important that you are in control of your own transportation to and from the date so that you can leave whenever you want and do not have to rely on your date in case you start feeling uncomfortable.

Make sure you have data on your phone and it’s fully charged, or consider bringing your charger or a portable battery with you.

Stick to what you’re most comfortable with. There’s nothing wrong with having a few drinks on a date. Try to keep your limits in mind and do not feel pressured to drink just because your date is drinking. It can also be a good idea to avoid taking drugs before or during a first date with someone new because drugs could alter your perception of reality or have unexpected interactions with alcohol.

Enlist the help of a bartender or waiter. If you feel uncomfortable in a situation, it can help to find help nearby. You can enlist the help of a waiter or bartender to help you create a distraction, call the police, or get a safe ride home.

Trust your instincts. If you feel uncomfortable, trust your instincts and feel free to leave a date or cut off communication with whoever is making you feel unsafe. Do not worry about feeling rude—your safety is most important.

If you felt uncomfortable or unsafe during the date, **remember you can always unmatch, block, or report your match after meeting up in person** which will keep them from being able to access your profile in the future.

Copyright: jcomp

Time for a quiz! True or False

You cannot block or report a person on the app without matching with her/him (false, you can block and report a person anytime: before matching, after matching, after meeting in person)

It is advised to check social media profiles and video chat in order to verify your match identity (true, you don’t need to stalk the person but this gives extra assurance. Also, some apps only match with people you share friends with)

Co-funded by the Erasmus+ Programme of the European Union

This project has been funded with support from the European Commission under the Erasmus+ Programme. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein. [Project Number: 2021-1-FR01-KA220-ADU-000033422]

The dating app provider can send me an email to ask for my credit card information (false, it will never send emails to ask for personal information or financial information, this is phishing)

You can help someone going through a personal crisis, even financially (false, you can exchange advice and offer emotional support but never send money)

It is ok to allow the dating app to have access to your geolocation (true, it can help in their algorithm for matching but you are not obliged to share your location).

WRAP UP – the most important points of this module.

1. Dating apps offer an online dating service presented through a mobile phone application, often taking advantage of GPS location, always on-hand presence and easy access.

2. There are significant differences between younger seniors (aged 60–74) and older seniors (above 75) behaviours and expectations.

3. Online dating apps are convenient but might be overwhelming and facilitate ghosting.

4. To choose the best app for you, know your expectations, favour ease of use, read reviews, trust the app popularity, synchronise with social media and verify safety features.

5. Main security advice includes: checking the profile of your match on social media, blocking and reporting suspicious profiles, being careful when sharing personal information or not sharing certain information, not responding to financial requests, video chatting with the person to verify their identity, meeting in a public space and letting friends know about the meeting.

Co-funded by the Erasmus+ Programme of the European Union

This project has been funded with support from the European Commission under the Erasmus+ Programme. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein. [Project Number: 2021-1-FR01-KA220-ADU-000033422]

INFORMATION AND DATA LITERACY: Risks about Booking your travel

Knowledge	Skills	Attitudes
Knows that some online content in search result may not be open access or freely available and may require a fee or signing up for a service in order to access it.	Can choose the search engine that most likely meets one’s information needs as different search engines can provide different results even for the same query.	Intentionally avoids distractions and aims to avoid information overload when accessing and navigating information, data and content
Aware that search engines, social media and content platforms often use AI algorithms to generate responses that are adapted to the individual user	Knows how to handle information overload and “infodemic” (i.e. increase of false or misleading information during a disease outbreak) by adapting personal search methods and strategies	Values tools designed to protect search privacy and other rights of users
Aware that online environments contain all types of information and content including misinformation and disinformation, and even if a topic is widely reported it does not necessarily mean it is accurate	Carefully considers the top/first search results in both text-based and audio searches, as they may reflect commercial and other interests rather than be the most appropriate results for the query	Inclined to ask critical questions in order to evaluate the quality of online information, and concerned about purposes behind spreading and amplifying disinformation.
Aware of potential information biases caused by various factors (e.g. data, algorithms, editorial choices, censorship, one’s own personal limitations).	Knows how to find the author or the source of the information, to verify whether it is credible (e.g. an expert or authority in a relevant discipline).	Willing to fact-check a piece of information and assess its accuracy, reliability and authority, while preferring primary sources over secondary sources of information where possible.
Aware that many applications on the internet and mobile phones collect and process data (personal data, behavioural data and contextual data) that the user can access or retrieve, for example, to monitor their activities online (e.g. clicks in social media, searches on Google) and offline (e.g. daily steps, bus rides on public transport).	Knows how to collect digital data using basic tools such as online forms, and present them in an accessible way (e.g. using headers in tables).	Considers transparency when manipulating and presenting data to ensure reliability, and spots data that are expressed with underlying motives (e.g. unethical, profit, manipulation) or in misleading ways.

Co-funded by the Erasmus+ Programme of the European Union

This project has been funded with support from the European Commission under the Erasmus+ Programme. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein. [Project Number: 2021-1-FR01-KA220-ADU-000033422]

Introduction to the module

Kathleen Cameron, senior director of NCOA's Center for Healthy Aging, noted that travel, visiting new places, and getting together with family and friends, both old and new, are particularly important for our mental health.

We need to travel for our mental wellness. You can reduce additional dangers by using these suggestions, regardless of whether you travel tens of thousands of miles year or only sometimes on brief trips. Avoiding frequent travel difficulties and hazards can be accomplished by planning ahead and having a backup strategy.

Let's look at some advice you can use to make your trip planning and journey to adventure as stress-free as possible.

What are we going to learn in this module?

In this module we are going to learn:

- Take measures to protect personal data while booking a travel
- Manage given personal data
- Enjoy the benefits of online environment
- Understand and identify the challenges

Why these tips are important in everyday life, using them while booking a travel?

- Follow public health guidance
- Choose a hotel that meets your needs
- Don’t publicize your trip on social media
- Stay healthy on route to, and on, the plane
- Keep important documents on hand

In order to keep ourselves and others safe from online threats, it is crucial to understand how to disclose personally identifiable information in the digital marketplace.

Co-funded by the Erasmus+ Programme of the European Union

This project has been funded with support from the European Commission under the Erasmus+ Programme. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein. [Project Number: 2021-1-FR01-KA220-ADU-000033422]

Knowing that digital services offer a "Privacy Policy" to describe how personal data is utilized and how these actions are taken in response to this data is useful.

For example: You want to buy a flight ticket to Rome online, but the platform says you must first fill out a form. You should be aware that filling out just the required fields is encouraged to reduce online dangers, such as the possibility of your personal information being stolen or abused.

Time for a quiz! Select the right answer

Question: What is data protection?

A: Data protection is the process of protecting sensitive information from damage, loss, or corruption.

B: Data protection is to give all your informations freely

Question: What we need to protect and not to give right away while pruchase something online?

A: Home address

B: Bank and card details

Understanding the advantages and risks while booking a travel

Advantages:

- ✓ Easy Access To Information for booking
- ✓ Connect with the word (Staying Connected)
- ✓ Helps you Feel Less Lonely

Risks:

- ✓ Risk of hacking into your personal details
- ✓ Phishing
- ✓ Leaking of personal information
- ✓ Fraud / Bank Fraud
- ✓ Identity theft

Co-funded by the Erasmus+ Programme of the European Union

This project has been funded with support from the European Commission under the Erasmus+ Programme. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein. [Project Number: 2021-1-FR01-KA220-ADU-000033422]

- ✓ Scams

These difficulties do not imply that aging in place is an unattainable or undesirable aim, but rather that extensive planning is required at both the individual and community levels.

The first stage is to educate accommodation companies about the financial and physical issues they may face if they stay in their existing home, as well as the solutions available to solve them. As is ensuring that local governments are aware of and prepared for the issues that their senior citizens will confront.

Time for a quiz! Select the right answer

Question: What information do you think applies when booking your travel online?

A: Public identity information (information shared publicly such as social networks, forums and websites)

B: Private identity information (information that is private such as bank details)

Co-funded by the Erasmus+ Programme of the European Union

This project has been funded with support from the European Commission under the Erasmus+ Programme. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein. [Project Number: 2021-1-FR01-KA220-ADU-000033422]

TITLE OF THE MODULE: ACCOMODATION (PLATFORMS)

Knowledge	Skills	Attitudes
The participant knows platforms and apps for boooking accomodation	The particpant is able to properly use the accomodation platform and apps	The participants is aware of the rules that accomodation platforms and apps offer
The participant is aware of the advantages and challenges in the use platforms and apps for accomodation	The participants is able to differenciate offers on accomodation platforms and apps	The participant is aware what data should be provided during the booking porcess
The participants understands how to find a safe accomodation on the platforms and application	The participant knows how to choose a good accomodation offer on the platform and app	The participant trusts official and reliable accomodation providers.

Introduction to the module

The Internet is a place where we can do a lot of everyday things, including looking for and booking various offers such as holidays, accommodation, flights or do shopping. Nowadays, we use services such as Airbnb, Trivago and Booking for this purpose. Many studies have been carried out to identify threats. ESET experts warn to be very careful when visiting sites dedicated to bookings. The experts also warn to be especially careful during the holiday season, when there is a spate of scams of all kinds.

Travelling means also looking for accommodation. You can use the offers of travel agencies, but thanks to the ever-growing popularity of websites, it is becoming increasingly common to organise holidays on one's own. When looking for rooms, flats or houses, we usually use the services offered by platforms such as Airbnb, Trivago or Booking. So what should we be particularly careful of when making bookings?

What are we going to learn in this module?

What are we going to learn in this module?

In this module we are going to learn:

- How are cybercriminals using holidays to try and scam people looking for travel deals and accomodation?
- What is the list of the most common scams you may come across when booking an accomodation?
- What should we be tempted to do if we find an extremely attractive offer?
- What is Trivago?
- Difference between Airbnb and Booking.com
- Airbnb pros and cons - how to use and what to look out for?

Co-funded by the Erasmus+ Programme of the European Union

This project has been funded with support from the European Commission under the Erasmus+ Programme. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein. [Project Number: 2021-1-FR01-KA220-ADU-000033422]

- How to make payment on Airbnb or Booking.com?
- Which data should we give during the reservation process?
- How not to get scammed on Airbnb?
- How not to get scammed on Booking.com?

How are cybercriminals using holidays to try and scam people looking for travel deals?

When using Internet platforms, we must remember to observe basic safety rules on the Internet. Otherwise, when looking for the perfect flat, hotel or room to rent, we may become victims of fraudsters.

Cybercriminals make skilful use of manipulation techniques and psychological mechanisms in their business. In their offer, they offer supposedly fantastic accommodation in a dream location at a price that is irresistible (so-called "super offer"). The combination of the desirability of the product, its bargain price and the ease of purchase makes bookers less attentive and more vulnerable to fraudsters.

Some of the most common scams that can be encountered when booking:

Payment outside the booking service

All operations related to the booking and payment process, should take place within the registration service. Any request by hosts for correspondence and payment or advances outside of Airbnb, Trivago or Booking should be a warning sign. It may herald an attempted scam.

In many places there is a statutory obligation to pay a so-called tourist tax (local hotel tax). Please note that this can be paid in person on site. In the case of most offers, the total amount of the booking is paid through the service and includes the amount of the rental and the tax. With Airbnb, it is possible to receive a discount from the host, but this must be registered through the official system.

Each of the booking platforms and apps has well-defined payment methods, which are detailed and available within the service. In the case of AirBnb, it is possible to pay with most credit cards including prepaid or using a PayPal, Apple Pay or Google Pay account. Similarly on Booking, where you can pay with a card or PayPal account. There is no option to pay by bank transfer on any of the aforementioned services. If you are asked to pre-pay your account, it is safest to abort the booking process and immediately report such an offer via the official contact form of the respective platform or the hotline. Cybersecurity experts recommend paying with payment cards when buying accommodation, as they offer a "chargeback" service. This protects buyers if there is fraud or if the service does not appear to match the offer description.

Here's a great offer, follow this link!

Cybercriminals are attempting to impersonate booking sites to conduct phishing campaigns. Their aim is to try and trick unsuspecting victims into providing them with access and personal data.

The mechanism involves sending an email that looks like a genuine email from a trusted source, advertising a great booking offer. Clicking on the included link may redirect the victim to a fake login page or a fake payment gateway, where cybercriminals aim to trick the victim into providing their bank access details. Sometimes they may also try to install malware on the victim's device.

Most email services are able to filter out this type of scam, but there are times when you will receive such an email. Always check that the messages you receive are from an official service. Do not immediately click on the links in them. To see the full URL, hover your cursor over the link. This will show you where you are being redirected to. If you are not sure whether an email with a great offer is genuine, it is safer not to click on the link, but to go to the main address of, for example, the website in question and search for the alleged opportunity. It may turn out that it never existed and that cyber criminals just used logos and added fake links

A flat offer that sounds too good to be true?

When browsing booking platforms in search of the perfect house to rent, users may come across offers that, at first glance, can be very positively surprising. These often relate to luxury residences in exclusive locations, which are available at a ridiculously low price in a very attractive location.

In this case, the very attractive price is nothing more than a decoy. In the short term, it is meant to attract as many people as possible willing to pay the rent. In practice, after paying the equivalent of hundreds or thousands of eur for rent and arriving on site, it turns out that the dream flat does not exist.

If you see an offer at a super price that is far from the average in the area, this should be a warning signal for you. In order not to be cheated, you should check the offer thoroughly. The best thing to do is to call and try to rent the flat you have booked, but as a different person. The prospect of spending time in your dream destination should not lull you into vigilance when booking accommodation. We should remember to check carefully, especially very attractive offers, not to click on links without thinking, and not to move the booking process outside of the booking platforms.

What is Trivago?

Trivago is a meta hotel search engine that compares accommodation prices and offers from different booking sites. We compare and display various offers from a number of booking sites, and they pay us for each click on their offer. We do not act as an intermediary between you and the site or accommodation where the booking is made. We do not charge you for your stay and we are not responsible for the services that booking sites and accommodation providers offer.

Trivago works with a wide range of booking sites from around the world, including online travel agencies, property chains and independent hotels.

How do I pay on Airbnb?

Requesting a reservation will not immediately take the amount from the card you have linked to your account. Once the owner confirms the booking, the amount will be blocked on the card. Usually half of the amount is taken and only then the other half. Once the booking has been made, you should receive an email from Airbnb stating when the amount will be debited from your account, e.g. within the next 3 days. If you have any doubts about payment, it is best to look for information on the Airbnb website where everything is explained in detail but you can also contact a consultant.

How not to get scammed on Airbnb?

From time to time, we may come across comments on the Internet about fraud on the Airbnb platform. Unfortunately , some users do fall victim to fraud, but not to the service itself, but to dishonest hosts who try to operate outside the platform, circumventing the terms and conditions. When making a booking, remember to NEVER transfer money outside the portal, even if the owner insists on it. If anything raises your suspicions, contact an Airbnb consultant straight away. A scammer may send an email requesting a transfer that is confusingly similar to an official message from the service:, it has the same icon, a similar address, booking details. It is therefore important to be vigilant when selecting a listing.

If the owner writes in the correspondence on Airbnb that he expects an additional fee on the spot, don't agree to that either.

Check reviews. A low price for accommodation is often because the listing/apartment/apartement has only recently been registered on Airbnb and has not yet had guests. When deciding to use such an offer, we have to expect some risk. We then have to judge for ourselves whether the landlord and the offer are convincing enough.

What do you do when an offer does not match the description?

If the listing is not as described, the property is not prepared for your arrival: it's a mess, it's dirty, and the owner is making problems, first take photos of the place showing all these things. Then contact Airbnb and inform them of the situation. Don't wait until the end of your stay or you may not get your money back. In this case, the portal should arrange alternative accommodation for you.

What should I look out for when booking my Airbnb accommodation?

Before you click the red "book" button, check the listing EXACTLY. The devil is in the detail. See if it's a private room or a whole flat. How many beds it has, whether they are single or double. Check if the guest has a private bathroom. Sometimes it's just a washbasin in the room, but it's always a plus. Read the description of the accommodation and what the owner writes about it. This is important because sometimes you can overlook important details that will backfire on you later.

Check the description of the offer, whether it is fully available in the same language or whether there are any annotations in the language of the country you are going to.

If you have any doubts about an offer, contact the owner and ask.

How do I recognise a scam on Booking?

The first warning of a suspicious listing, may be the lack of reviews. Perhaps this is due to the fact that the facility was only added this year. This means that no one has yet used the offer and seen what it is like on site.

A second warning is the very attractive prices. Much lower than the others in the location. This is one of the ways of the scammers. A very attractive price in as short a time as possible allows you to find a lot of people willing to pay. There is also a message - the price is currently no longer displayed.

The third warning - there are photos posted by the supposed owners. Pay attention to the quality of the photos and such lemmings as e.g. electrical sockets. Compatibility of the photos with the description.

Another warning is the information about contacting the owner without going through booking.com. The most common aim of fraudsters is to convince you to transfer money behind the intermediary's back. No intermediary does this. It is possible to contact the owners of properties, but through the website of the intermediary in question.

Completing the transaction on WhatsApp.

Booking.com never offers to complete the transaction through the use of WhatsApp messenger. This is a new scam method on booking.com to defraud the payer's details - name, account number and security code.

This project has been funded with support from the European Commission under the Erasmus+ Programme. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein. [Project Number: 2021-1-FR01-KA220-ADU-000033422]

If you are redirected to continue your booking on WhatsApp immediately abort the transaction.

What card details do I need to provide when making a booking?

At the time of booking you provide your card number, the name of the cardholder and the security code. Correctly entered data will redirect you to the payment secured by your bank. You will then need to confirm the payment, either by entering the sms code from your bank or by confirming the payment in your bank's mobile app.

Remember never to enter your PESEL number, ID or passport number . Asking booking.com to send you card details in the form of a scan of the front and back of your card is not recommended by the bank. If you are asked to do so, please stop the payment process immediately and report the offer on the portal by filling in the appropriate form or by contacting the customer service line.

Difference between Airbnb and Booking.com

The difference between booking.com and Airbnb is who makes the accommodation available on these services. In the case of booking.com, it is mostly all kinds of establishments designed for this kind of activity - hotels, hostels, guesthouses, etc. Airbnb, on the other hand, was created for private individuals who want to make their flats or rooms available to visitors for a fee. Today, booking.com also offers private accommodation and Airbnb also offers hotels. Undoubtedly, however, there are far more of the former on Airbnb. Often accommodations listings on both booking.com and Airbnb. It is then worth comparing the price and choosing the more favourable option. The differences are usually small, but it can also happen that one portal has clearly better conditions than the other. What are its advantages? What are the main challenges in its use?

Set limits with your bank before you start shopping online.

If you decide to use your payment card to book accommodation, it is a good idea to set appropriate limits for card payments on the Internet in advance. This will ensure that even if someone (e.g. a hotel, a shop or a scammer claiming to be such) wants to take a higher amount of money from the card than expected, they will not be able to exceed the limit we set.

There is no one-size-fits-all instruction on how to set limits for your card (this is done differently in each bank). Limits can be set not only for card payments, but also for the number and amount of transfers made online. Card payments are adequately insured and, in the event of fraud, we can apply for a so-called chargeback, i.e. a refund of the payment to the card. In addition, more and more banks are introducing a security feature - 3D Secure. This service ensures that even if someone gets to know your card details, they cannot make a payment from it if they do not have access to your phone. When making an online payment, you will be redirected to the bank's website, where you have to enter a code received by SMS or confirm the transaction in the mobile app.

Apps and modern technology used to reserve accomodation.

Use large and well-known accommodation search engines.

The best and at the same time easiest way to increase the security of our rental transaction is to use large and well-known search engines such as booking.com or airbnb.com. We can treat them as an intermediary between us and the hotel through which the payment will be made, and in case something goes wrong, we are able to assert our rights through them. It is worth

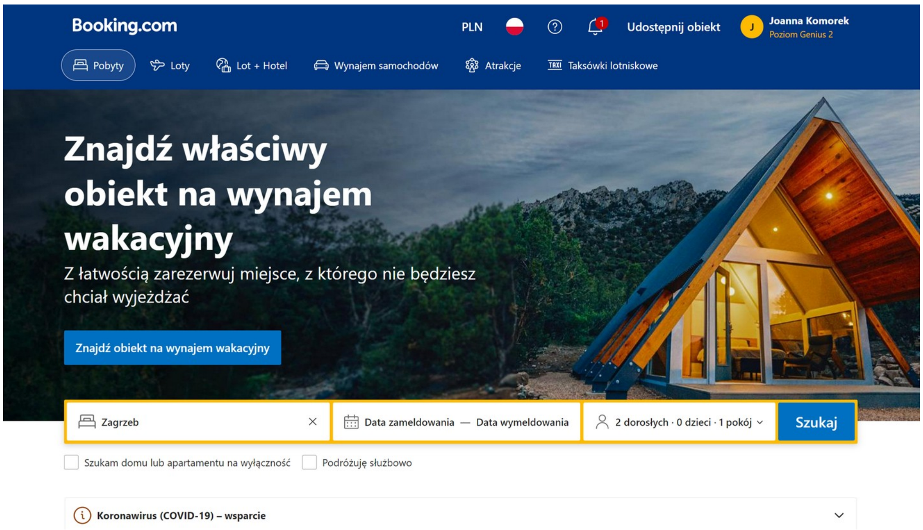
Co-funded by the Erasmus+ Programme of the European Union

This project has been funded with support from the European Commission under the Erasmus+ Programme. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein. [Project Number: 2021-1-FR01-KA220-ADU-000033422]

noting that from a technical point of view, these companies provide us above all with the security of both our personal data and the payment process itself.

Verify that the website of the hotel or guesthouse where you enter sensitive data uses an encrypted connection.

If the offer you want to use is not available on intermediaries' websites and you book directly on the hotel's website, it is worth verifying that the website on which you enter your data (including personal and payment card data) uses an encrypted connection - the address bar should start with https and there should be a closed padlock next to the website address. Remember that a closed padlock does not solve all security issues, but it does ensure that the communication between you and the hotel is encrypted and not eavesdropped on by a potential offender.

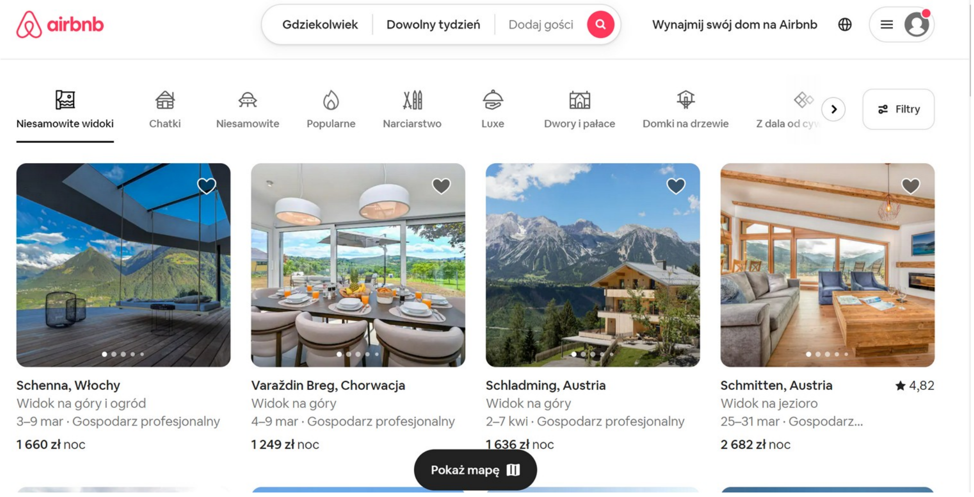

Booking.com
PLN
Udostępnij obiekt
Joanna Komorek
Poziom Genius 2
Pobyty
Loty
Lot + Hotel
Wynajem samochodów
Atrakcje
Taksówki lotniskowe
Znajdź obiekt na wynajem wakacyjny
Zagrzeb
Data zameldowania — Data wymeldowania
2 dorosłych · 0 dzieci · 1 pokój
Szukaj
□ Szukam domu lub apartamentu na wyłączność
□ Podróżuję służbowo
Koronawirus (COVID-19) – wsparcie

Znajdź właściwy obiekt na wynajem wakacyjny

Z łatwością zarezerwuj miejsce, z którego nie będziesz chciał wyjeżdżać

Booking.com

Best hotel app overall



Schenna, Włochy
Widok na góry i ogród
3–9 mar · Gospodarz profesjonalny
1 660 zł noc

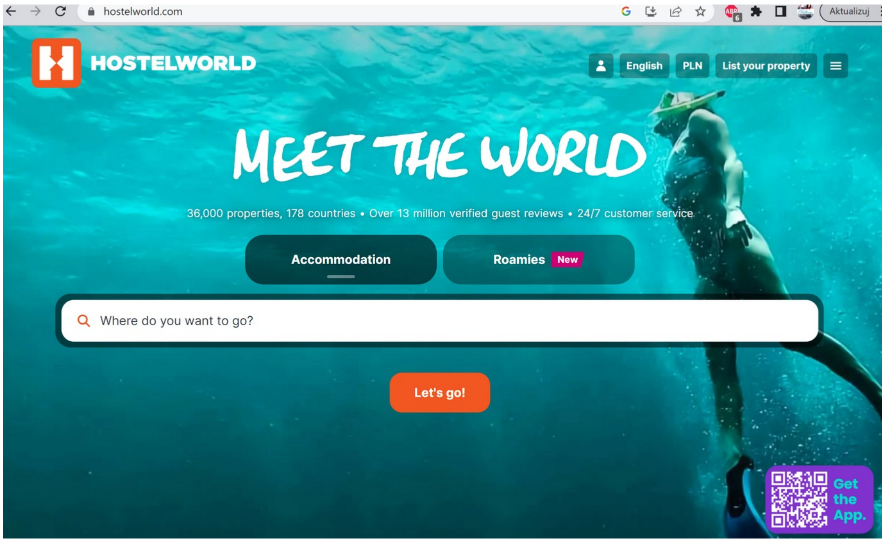
Varaždin Breg, Chorwacja
Widok na góry
4–9 mar · Gospodarz profesjonalny
1 249 zł noc

Schladming, Austria
Widok na góry
2–7 kwi · Gospodarz profesjonalny
1 636 zł noc

Schmitten, Austria ★ 4,82
Widok na jezioro
25–31 mar · Gospodarz...
2 682 zł noc

Airbnb

Best hotel app for private stays

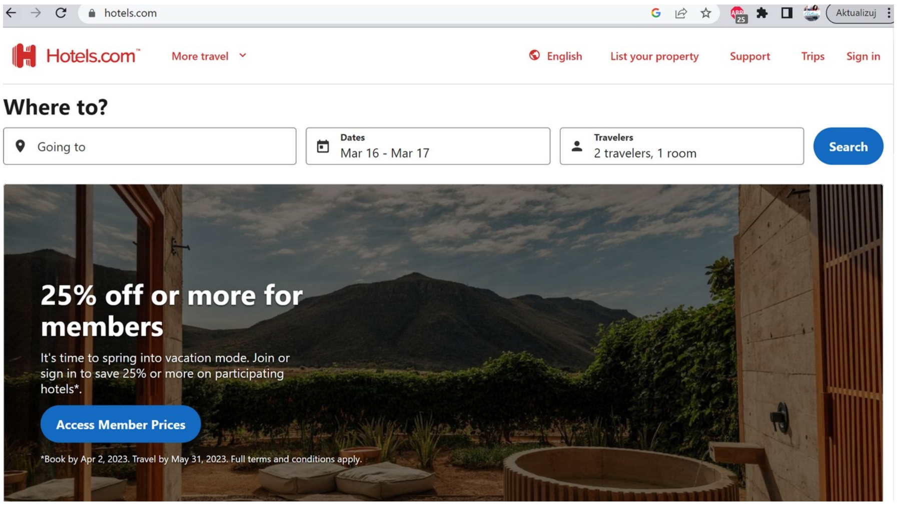


36,000 properties, 178 countries • Over 13 million verified guest reviews • 24/7 customer service

Where do you want to go?

Hostelworld

Best hotel app for hostels



Where to?

Going to

Dates
Mar 16 - Mar 17

Travelers
2 travelers, 1 room

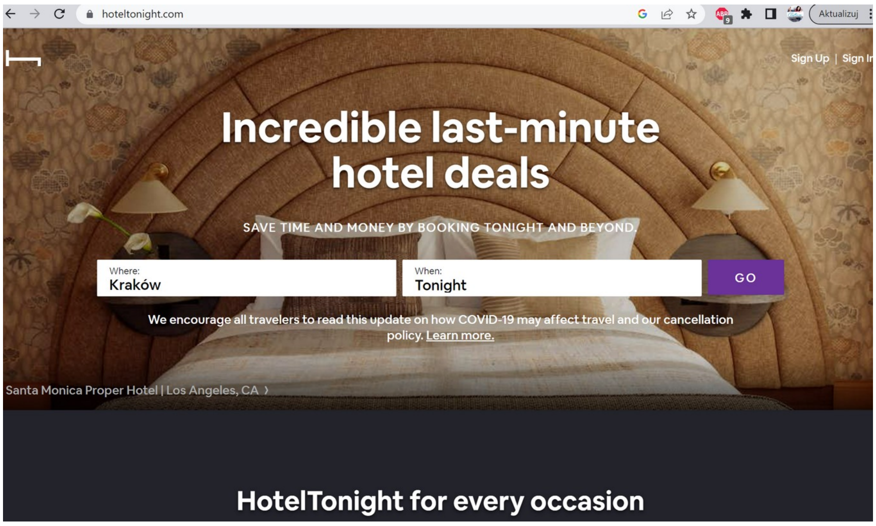
25% off or more for members

It's time to spring into vacation mode. Join or sign in to save 25% or more on participating hotels*.

*Book by Apr 2, 2023. Travel by May 31, 2023. Full terms and conditions apply.

Hotels.com

Best hotel app for cheap hotels



hoteltonight.com

Incredible last-minute hotel deals

SAVE TIME AND MONEY BY BOOKING TONIGHT AND BEYOND.

Where: Kraków

When: Tonight

We encourage all travelers to read this update on how COVID-19 may affect travel and our cancellation policy. Learn more.

Sign Up | Sign In
GO
Santa Monica Proper Hotel | Los Angeles, CA ›
HotelTonight for every occasion

HotelTonight

Best hotel app for last-minute stays

Using platforms and apps to search for accommodation pay attention to....

- Description of the offer and pictures of it.
- Data that are required to make a reservation.
- Payment method.
- Pay attention to unknown links.
- Never continue reservation on WhatsApp or any other communicator.
- Check if the apartment/building, hotel exists on the maps (google maps offers to look on the street view)
- If there is a contact to the owner of apartment or to the hotel.
- Don't send your credit card number by email and don't give it to a consultant during a phone call.
- Do not share your online banking login and password, or provide it on any site other than the bank's website.
-
- Do not provide scans of your documents.
- Do not brag about photos of your tickets on social media
- Enable disk encryption on your laptop
- Enable automatic screen locking.
- Make sure you have all your devices and documents in sight.
- Have limited trust in open Wi-Fi networks.

Time for a quiz! True or False

This project has been funded with support from the European Commission under the Erasmus+ Programme. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein. [Project Number: 2021-1-FR01-KA220-ADU-000033422]

1. When making booking on the BOOKING.COM portal we have to complete the reservation through WhatsApp (FALSE – BOOKING.COM never asks to use this communicator or any other to complete the reservation)
2. One of the information given during the reservation process is my PERSONAL ID (FALSE – tbooking platforms never ask for personal ID).
3. It is not allowed to pay outside the service I use for booking (TRUE – the payment is always done on the providers platforms or apps. Payment outside the platform means the scam)
4. To make the payment on Airbnb it is possible to use most of credit cards including prepaid or using a PayPal, Apple Pay or Google Pay account (TRUE - Each of the booking platforms and apps has well-defined payment methods, which are detailed and available within the service).
5. To reservation on Booking.com can be done with a card or PayPal account. (TRUE - Each of the booking platforms and apps has well-defined payment methods, which are detailed and available within the service).
6. Offers with low prices are the best one to choose (FALSE - If you see an offer at a super price that is far from the average in the area, this should be a warning signal for you. In order not to be cheated, you should check the offer thoroughly).

WRAP UP – most important points of this module

1. When making a booking, remember to NEVER transfer money outside the portal, even if the owner insists on it. If anything raises your suspicions, contact an Airbnb consultant straight away or Booking.com consultunt.
2. Cybercriminals use of manipulation techniques and psychological mechanisms in their business. In their offer, they offer supposedly fantastic accommodation in a dream location at a price that is irresistible.
3. Always pay attention to strange links when starting the payment.
4. Read the description of the accommodation and what the owner writes about it. This is important because sometimes you can overlook important details that will backfire on you later.
5. Check the description of the offer, whether it is fully available in the same language or whether there are any annotations in the language of the country you are going to.
6. Never complete payment or provide your data on the WhatsApp account.

Co-funded by the Erasmus+ Programme of the European Union

This project has been funded with support from the European Commission under the Erasmus+ Programme. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein. [Project Number: 2021-1-FR01-KA220-ADU-000033422]

STAYING SAFE ON THE INTERNET: PHISHING SCAMS

Knowledge	Skills	Attitudes
Learn about phishing	Recognise "phishing" communication	The participants will be more active when seeing suspicions communication
Learn about the different type of phishing	Be protective of personal data and information	The participant will make conscious decisions about the content they see on line or in their mail box
Learn how to protect themselves against those attack	Assess options before taking decisions	Consider plausibility of situation calmy before taking decisions

Introduction to the module

All frauds that are perpetrated online with digital devices (e.g. computer, tablet, smartphones) resulting in the victim's loss of money, personal information or passwords can happen in many unpredictable ways. More often than not, the defrauder's ultimate goal is to benefit financially from the victim's ignorance or gullibility.

This approach earned its unusual name because it uses attractive "bait" to lure people to websites and solicit their data under false pretences. Phishing is not the same as spam. While spam is just another term for junk mail and unwanted ads, phishing attacks are deliberate attempts to steal your information and use it in harmful ways.

In this module, we are going to learn more about different ways criminals can steal personal information, such as financial details or account passwords, and we will learn to defend ourselves and prevent those risks.

What we will learn

- What is phishing?
- How does phishing work?
- Types of Phishing You Need to Know to Stay Safe[1]
- How will I know if I've been phished?
- How can you protect yourself from phishing?[2]

[1] https://mypage.webroot.com/types-of-phishing.html

[2] https://www.webroot.com/us/en/resources/tips-articles/computer-security-threats-

Co-funded by the Erasmus+ Programme of the European Union

This project has been funded with support from the European Commission under the Erasmus+ Programme. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein. [Project Number: 2021-1-FR01-KA220-ADU-000033422]

Why these are important in our daily lives

While many frauds are attempted each day, it is still possible to use and benefit securely from the many possibilities that the internet offer to us. Having the basic knowledge on what kind of threats await us virtually could help in increasing our awareness to be more careful. Often, scammers would corner you into making a rash decision by creating a sense of urgency, or with attractive limited opportunity, by creating an imaginary situation relating to your current circumstances to make it look real. Being sceptical while surfing the internet is an important trait, especially when we are dealing with financial transactions.

What is Phishing?

The fraudulent attempt to obtain sensitive and important information and data.

The term phishing was coined to attract 'bait' that is able to lure people to websites and solicit their data under false pretences.

Phishing is one of the internet hoaxes in which scammers steal your personal information. They may use email or text messages to try to steal your passwords, account numbers, or Social Security numbers. If they get that information, they could get access to your email, bank, or other accounts. Or they could sell your information to other scammers. Scammers launch thousands of phishing attacks like these every day — and they're often successful.

It is important not to confuse Phishing (an attempt to steal from you) with Spam.

Phishing vs Spam

Phishing Attacks	Spam Attacks
Fake websites/ emails/ instant messages that look almost identical as the real website	Junk mails, unwanted advertisements
Aiming to get your personal data, tries to trick users in divulging sensitive information	Aiming to hawk goods and services by sending unsolicited emails to bulk lists. Not as dangerous as phishing

Signs of Phishing Email

- Misspelt words
- Discrepancies between the language of links and the website address they direct to.
- Requests for personal information
- Forms within emails
- Highly emotional or charged language

phishing

Co-funded by the Erasmus+ Programme of the European Union

This project has been funded with support from the European Commission under the Erasmus+ Programme. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein. [Project Number: 2021-1-FR01-KA220-ADU-000033422]

How does phishing work

The three main components of phishing scams are:

1. **Malicious web links**

   Web links/ address/ URLs are common in emails. Malicious links take users to impostor websites or sites infected with malicious software a.k.a malware. It can be disguised as trusted links with logos and other images in an email.

2. **Malicious attachments**

   An attachment in an email may look like a legitimate file, but it is infected with malware that can compromise computers and their files. For example, a ransomware (a type of malware) when it has infected a computer, all the files in the computer will become locked and inaccessible. Sometimes, they will automatically install a keystroke logger to track everything a computer user types, including passwords.

   Malware and ransomware infections can spread from one computer to other connected/ same network devices (ie: External hard drives, servers, clouds systems)

3. **Fraudulent data-entry forms**

   These types of emails will prompt users to fill in sensitive information such as user IDs, passwords, credit card data, and phone numbers. Once users submit that information, they can be used by cyber criminals for personal gain.

Some examples of phishing attacks

- **A plea for help:** These scammers will try to tug at your heartstrings by pretending to be a good friend or close relative. claiming to be in a financially dire situation that requires immediate assistance.
- **“You’re the Grand Prize WINNER”**: Receiving a congratulatory text message on you being the big prize winner, of an irresistible travel package or free tickets to an event of the year. You will be asked to provide personal details to claim your prize.
- **“ATTENTION: Your Bank Account Has Been Compromised”**: You get an “urgent” notice that appears to be from your bank, alerting you of suspicious activity on your account. You're then asked to click a link that takes you to a website, where you'll be prompted to confirm your bank account information.
- **“The Government is after you”**: An email that has a threatening tone and mentions big, scary penalties- unless you provide the payment or personal data they demand.

Co-funded by the Erasmus+ Programme of the European Union

This project has been funded with support from the European Commission under the Erasmus+ Programme. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein. [Project Number: 2021-1-FR01-KA220-ADU-000033422]

Types of Phishing You Need to Know to Stay Safe

- Standard Phishing
  Attempt to steal confidential information by pretending to be an authorised person or organisation.
- Email Phishing/ Spam Phishing
  Attempt to steal confidential information by pretending to be an authorised person or organisation. It lets the cybercriminal get access to a large number of customers registered on a site.
- Malware Phishing
  Introduces nasty bugs(virtual bug that could infect your computer) by convincing a user to click a link or download an attachment. Currently the most widely used form of phishing.
- Spear Phishing
  Similar to malware phishing, but this one cyber criminals will target a specific individual or group rather than a generic user base and it often succeeds precisely because it is more personalised. The perpetrator customises emails with the recipient’s name, company, phone number, and similar information, making the target believe that they share some form of connection.
- Search Engine Phishing
  Careful What You Choose - In this type of attack, cyber criminals wait for you to come to them. Search engine phishing injects fraudulent sites, often in the form of paid ads, into results for popular search terms.
- Vishing
  Voice-phishing involves a fraudulent actor calling a victim pretending to be from a reputable organisation and trying to extract personal information, such as banking or credit card information. Most often, the “caller” on the other line obviously sounds like a robot, but as technology advances, this tactic has become more difficult to identify.
- Pharming - Poisoning the Waterhole/ DNS poisoning
  A technically sophisticated form of phishing involving the internet’s domain name system (DNS). Pharming reroutes legitimate web traffic to a spoofed page without the user’s knowledge, often to steal valuable information.
- Clone Phishing
  A shady actor makes changes to an existing email, resulting in a nearly identical (cloned) email but with a legitimate link, attachment, or other element swapped for a malicious one.
- Man-in-the-middle/ Evil Twin
  The *Public WiFi Phisherman*; A man-in-the-middle attack involves an eavesdropper monitoring correspondence between two unsuspecting parties. When this is done to steal credentials or other sensitive information, it becomes a man-in-the-middle phishing attack. These attacks are often carried out by creating phony public WiFi networks at coffee shops, shopping malls, and other public locations. Once joined, the man in the middle can phish for info or push malware onto devices
- Malvertising

Co-funded by the Erasmus+ Programme of the European Union

This project has been funded with support from the European Commission under the Erasmus+ Programme. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein. [Project Number: 2021-1-FR01-KA220-ADU-000033422]

Takes advantage of exploits within advertising or animation software to steal information from targeted users. Usually embedded in otherwise normal-looking ads—and placed on legitimate websites like Yahoo.com or movies-streaming websites —but with malicious code implanted within.

- Domain Spoofing

  Perpetrator spoofs a notable organisation's domain name. This technique makes it appear as if you are receiving an email from a legitimate company. Email addresses are unique, so the phisher can only mimic the organisation's address. They do so by using character substitution like 'r' and 'n' together for 'rn' instead of 'm.'

How will I know if I've been phished?

Phishing scams often lure you with spam email and instant messages requesting you to "verify your account" or "confirm your billing address" through what is actually a malicious Web site. Be very cautious. Phishers can only find you if you respond.

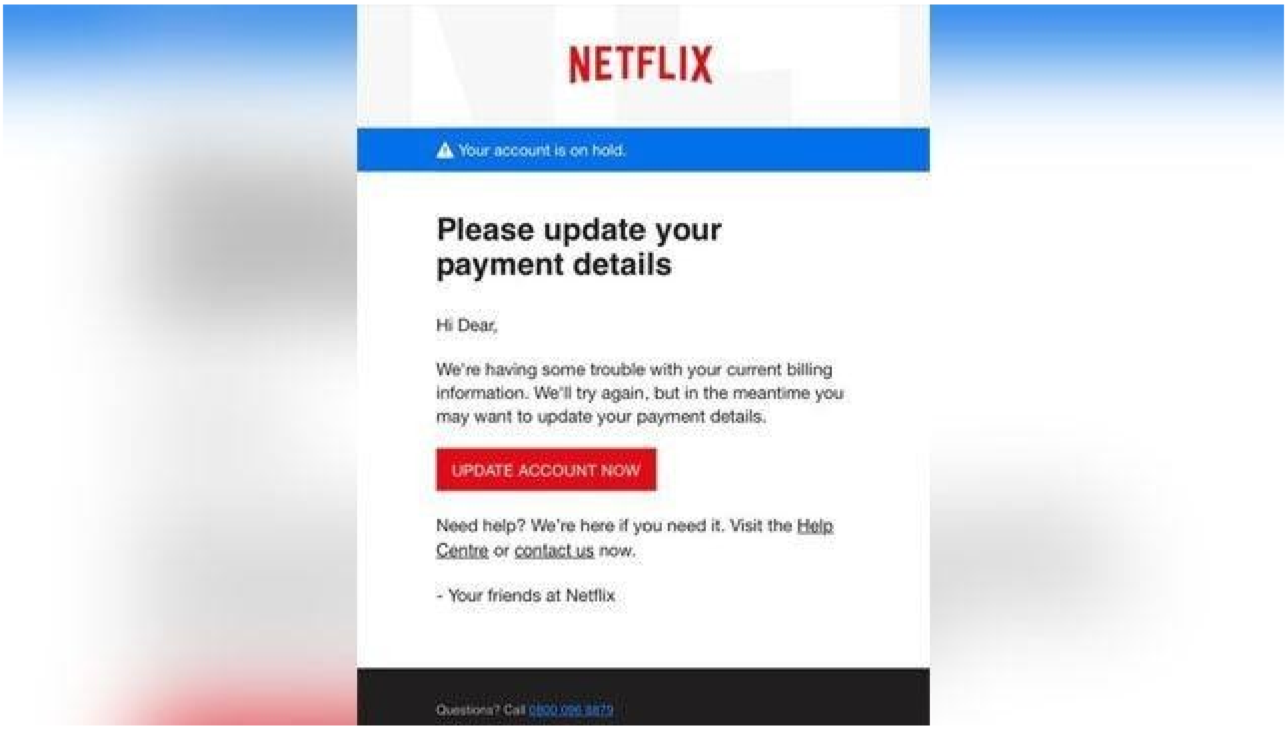
Phishing Through Email - Some examples

1. Subject Line: A subject that ‘calls’ you for an urgent matter
2. The “From” field: Appears to come from a legitimate entity within a recognised company, i.e. customer support, however some words in the field will be misspelt.
3. The “To” field: instead of addressing you by name, it addresses you as “user” or “customer”
4. Body copy: Typically employs urgent language, riddled with both grammar and punctuation mistakes.
5. Malicious link: a suspicious link that is shortened (ie: bit.ly), however, rolling over the link shows a malicious address that doesn’t take you to the stated web address.
6. Scare tactics: the email urges you to click the link to “update” your information that requires a payment made within a certain period.
7. Email Sign-off: often impersonal — typically a generic customer service title, rather than a person’s name and corresponding contact information.
8. Footer: Incorrect copyright date or a location that doesn’t correspond with that of the company.
9. Attachment(s): malicious downloadable files, often compressed .zip files, which can infect your computer.
10. Malicious landing page: ie: website address with misspelling, or suspicious logo on the header or footer of the website.

Co-funded by the Erasmus+ Programme of the European Union

This project has been funded with support from the European Commission under the Erasmus+ Programme. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein. [Project Number: 2021-1-FR01-KA220-ADU-000033422]

Here’s a real-world example of a phishing email:



NETFLIX

⚠ Your account is on hold.

Please update your payment details

Hi Dear,

We're having some trouble with your current billing information. We'll try again, but in the meantime you may want to update your payment details.

UPDATE ACCOUNT NOW

Need help? We're here if you need it. Visit the Help Centre or contact us now.

- Your friends at Netflix

Questions? Call 0800 096 8879

Netflix phishing scam screenshot

Imagine you saw this in your inbox. At first glance, this email looks real, but it’s not. Scammers who send emails like this one are hoping you won’t notice it’s a fake.

Here are signs that this email is a scam, even though it looks like it comes from a company you know — and even uses the company’s logo in the header:

- The email has a generic greeting.
- The email says your account is on hold because of a billing problem.
- The email invites you to click on a link to update your payment details.

While real companies might communicate with you by email, legitimate companies won’t email or text with a link to update your payment information. Phishing emails can often have real consequences for people who give scammers their information, including identity theft. And they might harm the reputation of the companies they’re spoofing.

How can you protect yourself from phishing?

- **DON'T CLICK** on links in emails from unfamiliar senders.
- **BE WARY** of unexpected or strange-looking messages from people you know.
- **ALWAYS CHECK** with the original resource, for example the company that is the subject of the email to check whether the email is legitimate or not.
- **DON'T OPEN** any attachments that show a different than usual type of file, unless you have been informed by the sender specifically regarding the file type. (ie: .exe/ .doc)
- **USE COMPLEX** and varied passwords for all your accounts, do not put generic passwords or the ones that are easy to be guessed.
- **DON'T RESPOND** to or click on pop-up windows on your phone or computer.
- **CHECK** the URL: "https" in the web address or one that has the 'lock' icon are two important signs you need to check upon providing personal informations. If the web address does not have both, it can be signs of phishing.
- **IGNORE** unsolicited phone calls or "robocalls" that may claim to be from "tech support" and tell you, falsely, that your computer is infected with a virus that needed immediate repair, and then they will ask for remote access.

TAKEAWAYS

It is better to be safe than sorry. Cyber criminals hide behind the anonymity of the internet. What you have put up on the internet is visible to others, and it is not erasable. Always be vigilant on what you are putting on the internet by not revealing any personal information to strangers online.

Look before you leap. Do not fall for lucrative rewards from random contests, or from signing up on certain websites, unless you really know the legitimacy of it. Most organisations - banks, charities, universities, do not ask for your personal information over an email.

It is just the tip of an iceberg. Your personal information is more precious than you think it is. These cyber criminals can put together the pieces available from your social networks to steal your identities, money or credit.

A chain is as strong as its weakest link. If we all realise the importance of having a cybersecurity awareness, it can make a big difference as it could also be our nation's first line of defence against people who might want to do harm. No matter young or old, it is important to encourage everyone to be cyber smart and savvy.

Co-funded by the Erasmus+ Programme of the European Union

This project has been funded with support from the European Commission under the Erasmus+ Programme. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein. [Project Number: 2021-1-FR01-KA220-ADU-000033422]

SOCIAL MEDIA PROFILES: HOW TO RECOGNIZE A FAKE PROFILE

Knowledge	Skills	Attitudes
Aware about the reasons for creating a fake social profile	Knows about the different fake social profiles Know the definition fake profile	Carefully considers the fake profiles before clicking. Concerned about the purposes behind the fake profile.
Knows how to recognize a fake profile	Know how to recognize the fake profiles in simple way. Can differentiate between different types fake profiles	Inclined to ask critical questions in order to evaluate the fake profiles Willing to check the facts of a piece of information and assess its accuracy, reliability and authority,
Understand how to stop a fake profile	To know basic tips to avoid fake profiles	Caution and verify information from multiple sources

Co-funded by the Erasmus+ Programme of the European Union

This project has been funded with support from the European Commission under the Erasmus+ Programme. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein. [Project Number: 2021-1-FR01-KA220-ADU-000033422]

Introduction to the module

Nowadays, social media is a part of everyday life. People use social media profiles to keep in touch with their friends and family, to tackle boredom or read the news. Other main uses of social media are finding content, seeing what is being talked about and finding inspiration for things to do and buy.

Social media platforms allow users to have conversations, share information and create web content. There are many forms of social media, including blogs, micro-blogs, wikis, social networking sites, photo-sharing sites, instant messaging, video-sharing sites, podcasts, widgets, virtual worlds, and more.

Everyone who wants to use social media creates their own profile - a description of individuals' social characteristics that identify them on social media sites. However, people create fake profiles for various reasons.

What are we going to learn in this module?

This modul consists of:

- What a social profile is.
- What a fake social profile is.
- Reasons for creating a fake profile.
- How to recognize a fake profile.
- How common fake profiles are.
- How to prevent fake profiles.

Why are those elements important in everyday life

As digitalization and our web presence grow, it is important to know how to recognize the official profiles of companies, brands and people on social media. Scammers can use social networks to gain trust by passing for official profiles. By pretending to be from customer service or sharing a fake deal, they can reach groups all at once or target individuals to swindle them.

Definition of a social profile

Social profiles are a description of individuals' social characteristics (such as interests, expertise, professional affiliations, status, recent activity and geographic location) that identify them on social media sites such as LinkedIn and Facebook. Profiles are the digital DNA of a person and display information that helps to understand the type and strength of an individual's relationships with others; for example, their level of participation and contribution in different initiatives, projects, communities, or conversations; their reputation among other participants, and so on. Creating a robust social profile allows individuals to be discovered by people who could benefit from an association with them.

Time for a quiz! Select the right answer

What is “social profile”??
a. Platform

b. Description of individuals
c. Name of country

True or False.
Profiles are the digital DNA of a person (TRUE)

A fake social profile

A fake profile is the representation of a person, organization or company that does not truly exist or is created without their knowledge, on social media. Often these accounts use names and identities that not only look real but are designed to get closer access to specific people and their target audience. These accounts are usually called imposter accounts or sock puppet accounts.

Reasons for creating a fake social profile

People create fake profiles for several different reasons, such as:

- Showing an unreal identity: users create an unreal “happy life” online.
- Stalking someone. people stalk somebody they are interested in without getting caught or recognized.
- Getting in touch with other people: users initiate talks with others in order to avoid embarrassment.
- Testing: especially programmers create fake accounts to do certain tests.
- For own benefits: some users support their own opinions, get votes or even criticize others without getting their real self involved.
- Spam: users use the accounts to spam.
- Second “me”: acting without involving the real profile.
- Bullying: cyber bullies bully others without getting caught.

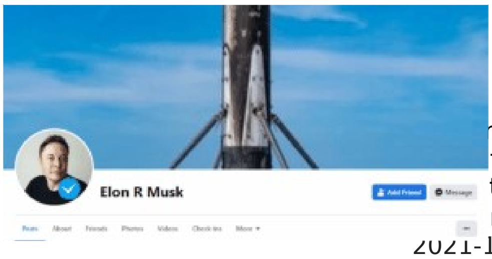
How to recognize a fake profile

Fake profiles can look very trustworthy, so it is essential to pay maximum attention to anything that might indicate that it is not a real profile.
Here are some facts that could help you:

Fake accounts often use avatars and symbols as their profile images, instead of photos. And when they do use actual human photos, they are usually low resolution. Low-res pictures can be a red flag when the account purportedly belongs to a public figure or celebrity.

To be sure whether the account is fake or not, run the profile picture through search engines like Google Image Search to see if the image is linked to another account or has appeared somewhere else on the internet.

Scammers often change their Facebook or Twitter usernames after signing up on the platform. This can give you a clue as to whether an account is real or fake.



Take this Facebook account as an example. It’s supposedly owned by Elon Musk.

roject has been funded with support from the European Commission
the Erasmus+ Programme. This publication reflects the views only of
thor, and the Commission cannot be held responsible for any use
may be made of the information contained therein. [Project Number:
2021-1-FR01-KA220-ADU-000033422]

The first red flag in this profile is the use of Elon's middle initial 'R'. The account is registered at this URL (web.facebook.com/profile.php?id=100083227784922), which shows no vanity name was set for this account, making it unlikely to be Elon Musk's actual Facebook page.

To further verify the authenticity of an account like this, check if the said person is registered on other social media networks with the same name. Also check if the profile image, bios, location, and contact details match up.

If there is significant overlap, then the account is likely genuine. If not, you're probably dealing with a fake account.

Using the fake Elon Musk example from above, that account has 236 followers—which is weird for somebody as popular and controversial as Elon Musk.

To check if this is Musk's real account or not, search for Musk's verified Twitter account and compare it to this Facebook account. On Twitter, Elon Musk has 104 million followers, which is a far cry from 236 Facebook followers.

When you spot a huge discrepancy in a person's follower count across different social media platforms, there's a good chance the account with the lower number is fake.

Another way to confirm if a public figure's account is real or not is to check if other verified accounts follow or interact with it. If yes, it's most likely real. If not, you're dealing with a fake account.

Pay attention to the kinds of posts published on the social media account. Check if it matches the person or seems out of character.

Fake accounts often spread false information and extreme views, and their feeds are usually filled with memes, stock photos, and recycled images. No published posts is also a sign of a fake account.

Also, check the kinds of comments the account leaves on other people's posts. If they leave the same (or similar) comments asking people to invest money or subscribe to a sketchy channel, it's likely a fake account. This can also indicate that the account is actually a bot.

The use of slurs, curse words, or weird slang can also give away the illegitimacy of a fake account.

Verified accounts have a blue icon (it's green on WhatsApp) at the end of the profile handle and may even have "Verified account" written on them. Only companies that request that icon and can give documentary proof that an official channel is theirs can receive it. In fact, Twitter and other sites prohibit handles with emojis that look like the verified account icon to avoid misleading users. We can often find links to a company's official profile on its corporate website. It is advisable to visit an official website where there is a link to the official social media profiles.

Official profiles can receive numerous tags and messages by the day, hour or even minute depending on their type. Check out how a profile engages with followers and be suspicious of profiles that post spam or only showcase deals that seem too good to be true. On customer service profiles, you will likely find direct engagement with followers. Remember to send a private message and not to post personal or particular details on a message wall.

It is common that there is some account history. On Twitter and other social media platforms, you can see how long a profile has been active. Be careful when interacting with profiles that haven't been open for long, since you can't know their purpose. If a profile has been open for a long time but has few posts or messages, it may no longer be in use.

How common fake profiles are

There are many sources that report the percentage of fake profiles and their figures vary widely. According to the latest data, it is likely that every user of social media meets a fake profile. Meta, which owns competitor platforms Facebook and Instagram, estimates that fake accounts represent about 5 per cent of monthly active Facebook users. In the second quarter of 2022, Facebook took action on 1.4 billion fake accounts, down from 1.6 billion in the previous quarter. (Meta considers fake accounts to be those that are created with malicious intent, or created to represent a business, organization, or non-human entity.) As Facebook is the most used social media platform worldwide it is not surprising that the service is a target for inauthentic activity and potentially harmful content. One third of US social media users creates fake accounts.

How to stop fake profiles

We cannot completely prevent fake social media accounts from popping up on social media platforms. Social networking platforms monitor the situation and delete suspicious accounts regularly, but it is up to each user to find out all available information about the profile and assess whether the profile can be trusted. Nowadays, when profiles are created also by robots and artificial intelligence is used, it is necessary to exercise caution and verify information from multiple sources.

If the user suspects a fake profile, or even if his own profile has been duplicated and misused, he has the option to report this fact to the administrators of the social network.

Time for a quiz! Select the right answer

Time for a quiz! True or False

What is the percentage of fake accounts on Facebook?

1. 25%

2. 5%

3. 40%

TRUE OR FALSE:

Official accounts should have messages, tags and interactions. (TRUE, Official profiles receive numerous tags and messages by the day, hour or even minute depending on their type)

How to make sure that an account is not Fake?

1. Caution and verify information from multiple sources.
2. Ask a friend

WRAP UP – most important points of this module

1. Fake social media profiles are common and it is very likely that every user will come across them.
2. Fake profiles are created for personal gain or to harm someone else.

Co-funded by the Erasmus+ Programme of the European Union

This project has been funded with support from the European Commission under the Erasmus+ Programme. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein. [Project Number: 2021-1-FR01-KA220-ADU-000033422]

3. When in doubt, we should verify information from multiple sources and not share sensitive information.
4. When we are sure that the profile is fake, we should report it to the administrators of the social network and block the contact.

Co-funded by the Erasmus+ Programme of the European Union

This project has been funded with support from the European Commission under the Erasmus+ Programme. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein. [Project Number: 2021-1-FR01-KA220-ADU-000033422]

STAYING SAFE ON THE INTERNET: DEBUNKING FAKE NEWS

Knowledge	Skills	Attitudes
Know what fake news are	Able to recognise fake news	Be aware and avoid fake news
Learn about fake news and why it exists.	Reflect on the reasons behind what we read	Be aware of other's intent
Know why fake news are dangerous	Assess the impact of wrong information on our decision making	Be aware of the risks connected with disinformation
Learn how to verify information found online	Using criteria for evaluating information you find online.	Be more careful before sharing with others

Introduction

We have all been there - reading something on Facebook or Whatsapp that makes us feel bad or angry. Why are people so easily fooled by fake news? How can we learn to recognize it?

The Internet is an incredible resource for news and information, but unfortunately not everything online is trustworthy. Fake news is any article or video containing untrue

This project has been funded with support from the European Commission under the Erasmus+ Programme. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein. [Project Number: 2021-1-FR01-KA220-ADU-000033422]

information disguised as a credible news source. While fake news is not unique to the Internet, it has recently become a big problem in today’s digital world.

Fake news typically comes from sites that specialise in made-up or exaggerated stories. It tends to use provocative headlines, like "Celebrity endorses not brushing teeth '' or "Politician selling toxic waste on the black market". These headlines can seem suspicious or even unbelievable to the point of being silly, making it tempting to think of fake news as harmless.

In recent years, however, fake news has been responsible for a great deal of misinformation because more and more people have begun consuming and believing these articles without bothering to fact check or even read beyond the headlines. This acceptance of incorrect information has led to confusion, panic, and an inability to discuss the actual facts surrounding current events.

The aim of the module is to understand what fake news is, how to identify news that is fake and more importantly how to prevent such news from spreading.

In this module we will:

- Learn about fake news and why it exists.
- Reflect on how our own opinions impact the way we evaluate information.
- Discuss and practice using criteria for evaluating information you find online.
- Learn how to verify information found online before sharing it with others.

Co-funded by the Erasmus+ Programme of the European Union

This project has been funded with support from the European Commission under the Erasmus+ Programme. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein. [Project Number: 2021-1-FR01-KA220-ADU-000033422]

What Is Fake News?

There are two kinds of fake news:

1)Stories that aren't true. These are entirely invented stories designed to make people believe something false, to buy a certain product, or to visit a certain website.

2)Stories that have some truth, but aren't 100 percent accurate. For example, a journalist quotes only part of what a politician says, giving a false impression of their meaning. Again, this can be deliberate, to convince readers of a certain viewpoint, or it can be the result of an innocent mistake. Either way, it quickly attracts an audience and can become entrenched as an "urban myth."

Why is it important to combat fake news?

While manipulating and distorting information has been part of recorded history, the weaponisation of information in the 21st century has risen at an unprecedented rate, which requires urgent and effective responses.

Today, news can travel in seconds from London to Tokyo through Whatsapp Application, they are inevitably a part of our everyday life. We read news based on our preference of platforms, either through the physical newspaper & magazines, or through online platforms such as Facebook, Twitter or Mass Media websites. We will then process the news and reflect upon it with our peers, each of us having our own set of opinions on the topics mentioned.

However, how do we know if the news we are consuming is real? How do we know which platform brings out the truth, fake or incomplete?

Fake news has the potential to undermine the legitimate opinions of experts, authoritative and legitimate institutions which could prevent society from getting a clear picture of the real situation, and end up having a distorted vision of reality and the limited ability of engaging in rational discourse.

There are three important points we need to focus on in combating fake news; first being the increasing fragmentation and politicisation of news; second, the promotion of “safe news” at the expense of difficult news stories; third, the need for credible sources to debunking inaccurate information, which poses both financial and reputation costs.[1]

False Information v Fake News

[1] Fighting Fake News Workshop Report hosted by The Information Society Project The Floyd Abrams Institute for Freedom of Expression On March 7, 2017, the Information Society Project at Yale Law School and the Floyd Abrams Institute for Freedom of Expression hosted a workshop intended to explore the ongoing efforts to define fake news and discuss the viability and desirability of possible solutions.

Experts now recommend avoiding the term ‘fake news’, or at least limit its use, as the term ‘fake news’ is closely associated with politics, and this association can unhelpfully narrow the focus of the issue. The term ‘false information’ is preferable as it can refer to a diverse range of misinformation and disinformation covering topics such as health, environmental and economics across all platforms and genres, while ‘fake news’ is more narrowly understood as political news stories.

What are the different types of false information?

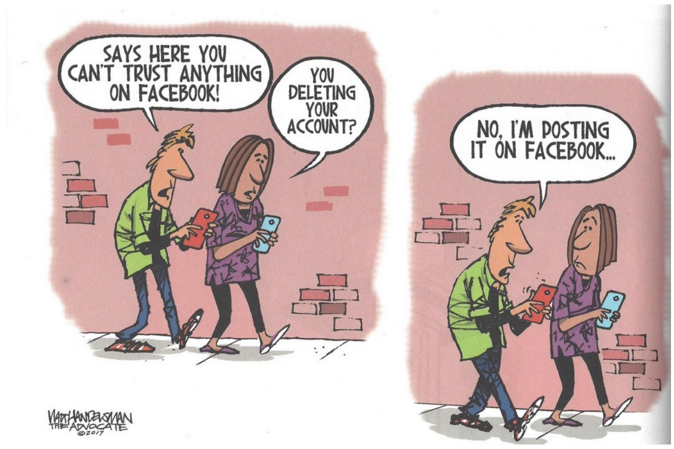
False information can be categorised in three ways:

1) Misinformation is the spread of false or mistaken information that wasn’t necessarily created to harm you. By sharing and spreading information that is incorrect you make it credible.

2) Fake News lies or fabricated information/news that is non-verifiable through sources, facts or quotes. This includes: hoaxes, conspiracy theories, fake websites, clickbait pages posing as legitimate websites, memes, Youtube channels posing as official channels, and “zombie claims” (photos or posts that have been manipulated or edited to look real that keep popping up all over social media).

3) Disinformation is information that was created to deceive, lie or support either an individual or a social/political group’s agenda. It's biased information like propaganda used for “brainwashing” created with the intent to harm you.

Mis- and disinformation is designed to trigger a reaction, an emotional response that spurs you to share the content. It’s easy to spread misinformation without even thinking about it when something triggers strong feelings in us.


SAYS HERE YOU CAN'T TRUST ANYTHING ON FACEBOOK!
YOU DELETING YOUR ACCOUNT?
NO, I'M POSTING IT ON FACEBOOK...
WALT HANDELSMAN THE ADVOCATE ©2017

How can you verify that news is legitimate or FAKE?

Identifying fake news can be challenging, as it can be designed to look like legitimate news and often contains misleading or false information. However, there are some ways to identify fake news:

Check the source: One of the easiest ways to identify fake news is to check the source of the information. Is the source reputable and trustworthy, or is it an unknown or suspicious website? A simple search can often reveal if the source is credible.

Verify the information: Check if the information in the news article can be verified by other reputable sources. If the story is only reported by one source or if it contains information that is not supported by other sources, it could be fake news.

Look for bias: Fake news often has a bias or agenda behind it, which can be reflected in the language used or the tone of the article. If the article seems to have a clear bias or is trying to push a particular agenda, it could be fake news.

Check the date: Fake news stories can be old stories that are recycled and presented as new information. Check the date of the article to make sure it is current.

Check your emotions: Fake news often plays on people's emotions to get them to share or believe the story. If the story seems designed to provoke a strong emotional response, be cautious and fact-check before sharing or believing it.

Overall, identifying fake news requires critical thinking, scepticism, and the willingness to verify information from multiple sources.

Why is it important NOT to share fake news?

With so many sources of information online, it has become difficult to make sense of what content is based on fact, half-truths or lies. The use of digital platforms to share things we believe to be true when they are not, can have a powerful ripple effect, influencing others to see them as facts.

It is important to not share fake news for several reasons:

Misleading information: Fake news often contains misleading information that can cause confusion and mislead people into believing things that are not true. This can lead to incorrect decisions being made based on false information.

Social unrest: Sharing fake news can create social unrest and panic. In extreme cases, it can even incite violence or riots. For example, fake news about religious or ethnic conflicts can escalate tensions and lead to violence.

Harmful consequences: Fake news can have harmful consequences, especially when it relates to public health issues or medical advice. False information about health issues can lead people to make poor health choices, endangering their lives and those around them.

Trust in media: When people share fake news, it undermines trust in the media and can make it harder for people to distinguish between real and fake news in the future. This can have a long-term impact on society and the functioning of democracy.

Personal reputation: Sharing fake news can also harm your personal reputation. When people share fake news, it can be seen as a sign of poor judgement, lack of critical thinking skills, and lack of credibility. It's important to be responsible and verify the accuracy of information before sharing it with others.

TIME FOR A QUIZ

Co-funded by the Erasmus+ Programme of the European Union

This project has been funded with support from the European Commission under the Erasmus+ Programme. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein. [Project Number: 2021-1-FR01-KA220-ADU-000033422]

Any article or video containing untrue information disguised as a credible news source

- Clickbait
- Wikileaks
- Fake News
- All of the above

Choose the options that best describe the characteristics of Fake News

- are bogus, sensationalised stories
- asks viewers to click a link
- have provocative headlines
- show secret government documents

What is Propaganda?

- found on all online news sources
- Information used to promote a particular point of view, often biased or misleading.😀
- information on a website that is credible
- none of the above

TRUE OR FALSE

People generate fake news to fulfil a social agenda.

TRUE

WRAPPING UP FAKE NEWS

1. It risks concealing the truth and quality of good and ethical journalism. Having fake news crawling around us daily is not new but rather have become increasingly more powerful as they are fueled by new technologies and rapid online dissemination.
2. Each of us has the ability to contribute to improving the nature of our online discourse. You can pass along the idea that people are often distracted from accuracy, and that it is important to stop and think about whether something is true before you share it.
3. Fake news doesn't want you to think. It is almost always sensationalised, bringing simple narratives that are grand into the extremes with exaggerated language and misinformation.
4. It mostly relies on the biases that are in all of us. Readers unconsciously made snap judgements as to what to believe and what to discard.
5. The only defence to fake news is vigilance. Taking the time to check sources before you share and learning how to spot fake news in the wild are two important steps.

STAYING SAFE ON THE INTERNET: EMAILS SCAMS

Knowledge	Skills	Attitudes
What are email scams	Learn to recognise good and fake emails	Be aware of the risks associated with scams
How to protect yourself against them	Increase assessment capacity to judge an email by its objective only	Be able to select and trash emails that are dangerous.

Introduction to the module

Email is one of the most common ways to communicate with anyone from anywhere across the globe. However, it is also a primary tool used by cyber criminals to steal money, account credentials, and sensitive information.

For this reason, it is important to recognise a fraudulent email, or an unsecure website. In this module we will review the main types of scams, analyse them and learn how to recognise the fake and dangerous ones.

Much like any other kind of fraud, the perpetrator can cause a significant amount of damage, especially when the threat persists for an extended period. Email fraud has a list of negative effects, including loss of money, loss of intellectual property, damage to reputation, sometimes with irreparable repercussions.

What are we going to learn in this module?

- What are email scams
- The most popular types of scams
- How to protect yourself from scams
- Real examples of email scams

Why is it important to learn about scams?

These days, the scam's perpetrators attempt to run from old-fashioned bait-and-switch operations to phishing schemes using a combination of email and bogus web sites to trick us into divulging sensitive information. Most scams follow the same pattern and by understanding this pattern, we could spot them easier. They often try to create a sense of urgency and use high-pressure sales tactics.

A successful scam can have a devastating impact. An attack that targets a company could affect the individuals who work for that company, or customers and partners of that company.

Scammers target people of all backgrounds, ages and income levels. All of us may be vulnerable to a scam at some time. More often than not, they look like the real thing and would catch you off guard when you are not expecting it.

Co-funded by the Erasmus+ Programme of the European Union

This project has been funded with support from the European Commission under the Erasmus+ Programme. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein. [Project Number: 2021-1-FR01-KA220-ADU-000033422]

What are scams and email scams?

Scams are fraudulent actions that can be used to cheat someone out of money or confidential information.[1]

Scams can happen in many ways, either through emails, social media messages, phone calls or even online dating apps. An email scam is an unsolicited commercial email; a starting point for scam activities. The convenience and anonymity of email, along with the capability it provides to easily connect with thousands of people at once, enables scammers to work in volume.[2] Scammers only need to fool a small percentage of the tens of thousands of people they email for their ruse to pay off.

The most popular types of scams

- ### Financial scams
  - Includes tax, charity, inheritance, lottery, donation, loan, e-commerce and other payment scams.
  - Someone would claim to be from a financial institution or a government agency and asking you to pay some "outstanding payment"
  - They may say that if you don't pay immediately, they will take legal action against you.
- ### Identity or Medical information theft
  - Scammers might use your personal information to get drugs, prescription, diagnostic tests and even a medical procedure or operation.
  - They might ask for your insurance statement.
- ### Catfishing
  - Is when a scammer creates a fake account or identity to trick people into believing they are talking to a real person.
  - Often happens in online dating apps.
  - They would want to leave the app immediately and ask for your personal email or messaging app to continue chatting.
  - Asks you to wire money claiming something bad happened to them.
  - Claims to be in love very quickly to persuade you to speak with them.
- ### Tech-support scams that can include access token theft
  - Someone claiming to be tech support from a real company may say your computer has been infected by a certain virus.
  - They may ask you to follow instructions to "save your data" which will allow them to install malicious software on your computer.
  - This malicious software could potentially steal your personal information by gaining access on your computer.

[1] https://wethinkdigital.fb.com/wp-content/uploads/2021/09/Avoiding-Scams-Presentation-1.pdf

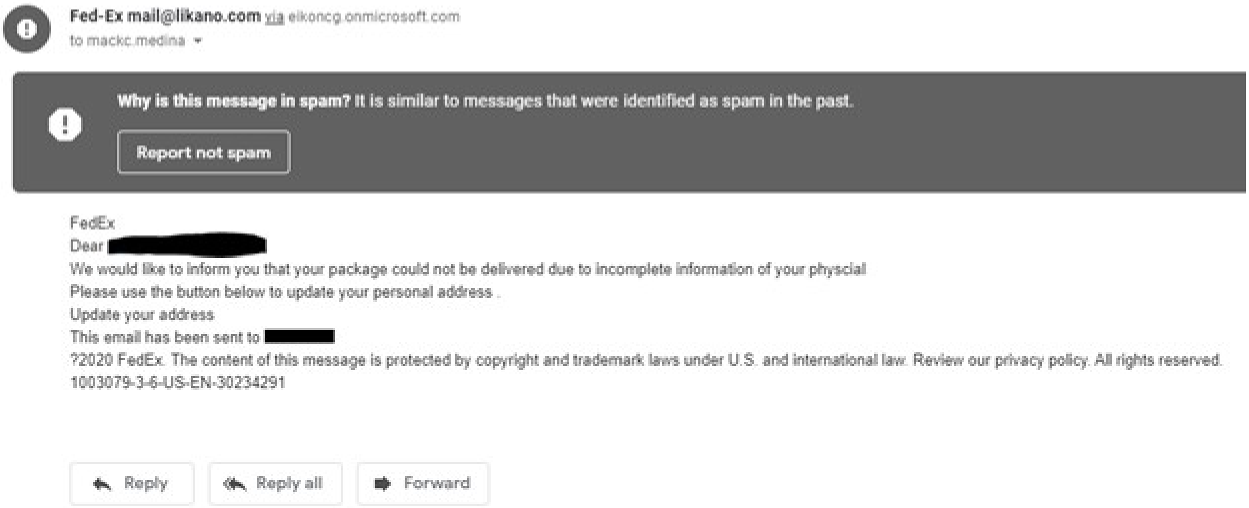
[2] https://www.cisa.gov/uscert/sites/default/files/publications/emailscams_0905.pdf

How to protect yourself from these kinds of scams

- **Filter Spam:** Most email applications have in-built spam-filtering features, or suggestions that would automatically recognise if the email is a scam or not. Utilise this feature and you will keep a great deal of spam email from reaching your mailbox.
- **Regard unsolicited email with suspicion.** Don't trust any email quickly in just a glimpse. Never open an attachment to unsolicited email, and never click on a link sent in the email.
- **Treat email attachments with caution.** Email attachments are commonly used by cyber criminals to sneak a virus onto your computer. These viruses have the ability to help scammers in stealing the data and information available from your computer.
- **Install Antivirus Software and Keep it up-to-date.** If possible, install antivirus software that has an automated update feature on it to ensure you have the most up-to-date protection against any unforeseeable viruses.
- **Install a Personal Firewall and Keep it up-to-date.** It may not prevent scam emails, but it can protect you from opening a virus-bearing attachment. It will also help to prevent outbound traffic from your computer to the attacker.
- **Choose your passwords carefully.** A strong password should not have any relations from your obvious personal details (ie: name, birth of date), and it includes a mix of upper and lower case letters, numbers and symbols. DO NOT use the same password for every other account on the internet.
- **Review your privacy and security settings on social media.** Be careful who you connect with on social media, and learn how to use your privacy settings.

Examples of email scams

1. Email from "FedEx" - A prominent courier company commonly used by everyone



Fed-Ex mail@likano.com via eikoncg.onmicrosoft.com
to mackc.medina

Why is this message in spam? It is similar to messages that were identified as spam in the past.

FedEx
Dear [redacted]
We would like to inform you that your package could not be delivered due to incomplete information of your physcial
Please use the button below to update your personal address .
Update your address
This email has been sent to [redacted]
?2020 FedEx. The content of this message is protected by copyright and trademark laws under U.S. and international law. Review our privacy policy. All rights reserved.
1003079-3-6-US-EN-30234291

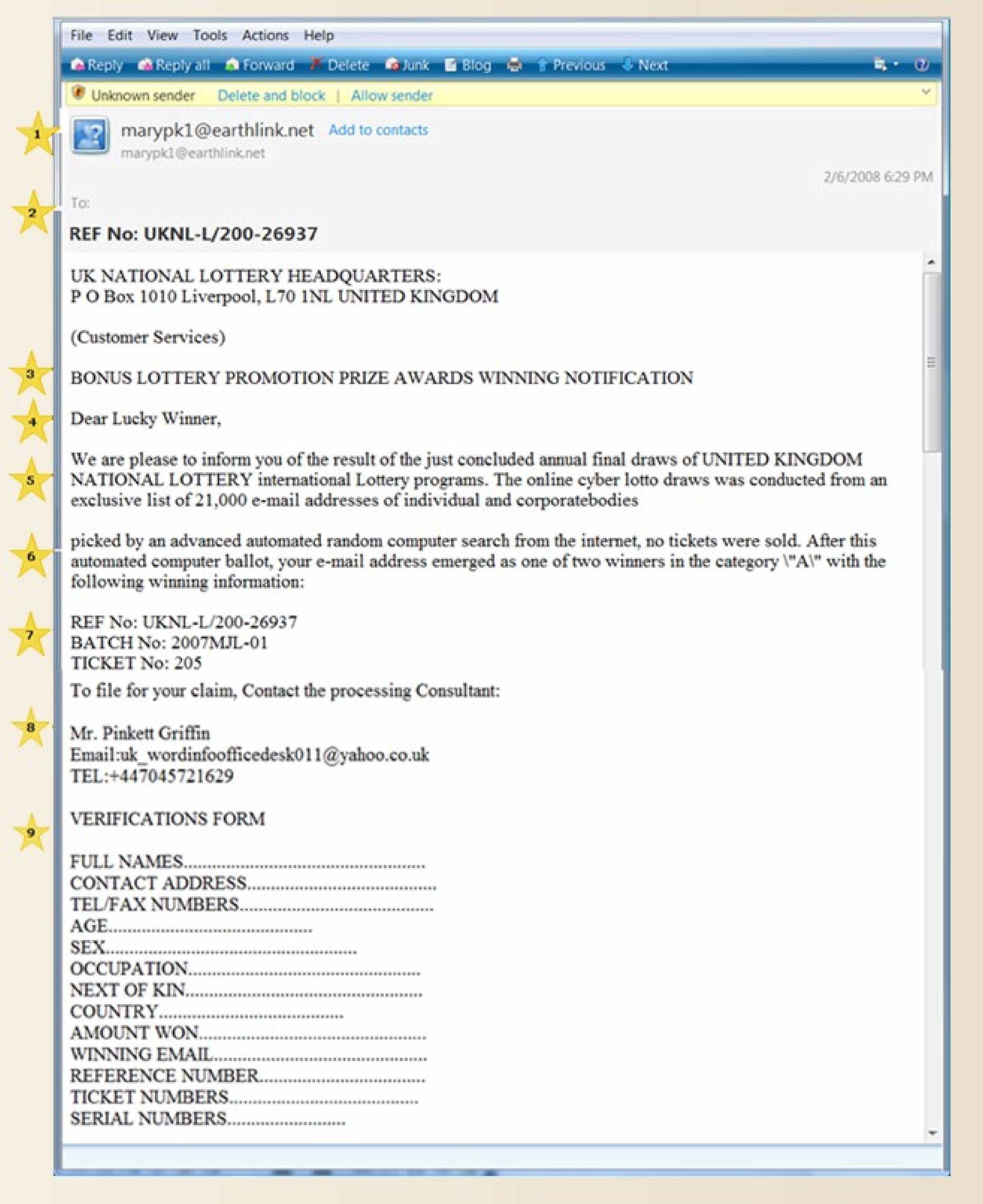
Attackers use this type of message because it is common for us to expect a package from FedEx. If the message is sent to thousands of recipients, it can trick many of them.

NOTE

- The sender's email address in the above image is from a public domain is NOT associated with FedEx.

- The email gives no contact number, but has a single link that directs you to a malicious web page.
- The email does not address the recipient by name or have any personal information that an account vendor would have. The email is generic with only the recipient's email address used in the greeting (the email address is blacked out).

2. The Lottery Email



marypk1@earthlink.net
marypk1@earthlink.net

2/6/2008 6:29 PM

To:

REF No: UKNL-L/200-26937

UK NATIONAL LOTTERY HEADQUARTERS:
P O Box 1010 Liverpool, L70 1NL UNITED KINGDOM

(Customer Services)

BONUS LOTTERY PROMOTION PRIZE AWARDS WINNING NOTIFICATION

Dear Lucky Winner,

We are please to inform you of the result of the just concluded annual final draws of UNITED KINGDOM NATIONAL LOTTERY international Lottery programs. The online cyber lotto draws was conducted from an exclusive list of 21,000 e-mail addresses of individual and corporatebodies

picked by an advanced automated random computer search from the internet, no tickets were sold. After this automated computer ballot, your e-mail address emerged as one of two winners in the category \"A\" with the following winning information:

REF No: UKNL-L/200-26937
BATCH No: 2007MJL-01
TICKET No: 205
To file for your claim, Contact the processing Consultant:

Mr. Pinkett Griffin
Email:uk_wordinfoofficedesk011@yahoo.co.uk
TEL:+447045721629

VERIFICATIONS FORM

FULL NAMES...
CONTACT ADDRESS...
TEL/FAX NUMBERS...
AGE...
SEX..
OCCUPATION..
NEXT OF KIN...
COUNTRY..
AMOUNT WON...
WINNING EMAIL..
REFERENCE NUMBER..
TICKET NUMBERS...
SERIAL NUMBERS..........................

Foreign lottery scams are rampant.

It should be obvious but is important to state: If you did not enter a lottery, you did not win a lottery.

If you did enter the lottery, you still are very unlikely to win, and **you would not be notified via email.** This is a straightforward scam to get your information.

1. The sender is a person. No organisation is going to send a notice from a personal email, and they will use their organisation's e-mail, not a free email service.
2. No one is listed as the recipient. If your name isn't on the To: line, it's a scam. Also, no legitimate company will send you an email with an incomprehensible subject line.
3. The message is illiterate.
4. The sender does not know your name.
5. There is no such lottery. A simple Web search on the lottery name shows that it does not exist – and several results that say it is a scam. In addition, the idea that you are on an 'exclusive list of 21,000 email addresses' is absurd.
6. If no tickets were sold, how does the lottery make money?
7. Random jumbles of numbers designed to look impressive.
8. You will never be asked to respond to an individual. If the organisation is legitimate it will have its own email address and you will be directed to customer support or another department, not a person.
9. The information request. Collecting your information to sell to other criminals is the first goal. But if you respond with this information you will surely be asked for bank account and bank routing numbers as well so they can 'deposit' the money.

WRAPPING UP EMAIL SCAMS

- Scammers do not discriminate when it comes to who they try and get money out of: rich, poor, black, white, 65 and healthy, 85 and ailing. They'll try to take money from anyone.
- We should stay vigilant and keep ourselves informed on ways these scammers could scam us.
- Keep an eye on our bank accounts whenever we need to perform any online transactions.
- If faced with a "good deal" on a dream holiday package, discuss it with your loved ones first and ask the company for more information to check if it's valid.
- Do not fall for seasonal sales on the e-commerce website easily. This would trigger you to make an impulse buy for a product that you don't necessarily have a need for.
- Know when and how to report scams to the authorities.

Co-funded by the Erasmus+ Programme of the European Union

This project has been funded with support from the European Commission under the Erasmus+ Programme. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein. [Project Number: 2021-1-FR01-KA220-ADU-000033422]

MILEAGE I03 - AN INTRODUCTION

The internet is full of possibilities and opportunities to learn, make new friends and even find love. However, it's also the perfect place for people to take advantage of the anonymity a computer screen offers. Most know that young people are the ideal target for predators, but few think about online safety for older people.

Older adults are the fastest growing population among computer and internet users (Friemel, 2016), and use technology for a number of reasons; from convenience activities such as banking, shopping, maintaining communication , through to facilitating self-care and health management . Older adults recognize the benefits that technology provides for staying independent for longer, and many are keen to continue using technology well into older age.

As with all users, older adults are at risk of cyber-attacks; however, they are specifically sought out by cyber criminals (Munanga, 2019). While much of the existing technology research surrounding older adults has focused on adoption and attitudes toward technology, a growing literature base has started to focus on older adults' cyber-security vulnerability and online behavior.

This project tackles the digital divide and addresses the urgent necessity for seniors' citizens to develop digital skills, while fostering their participation in civic and cultural EU life. The project, by adding a digital perspective to the procedure of 'active aging' also provides seniors with the essential skills to respond to the 21st century's challenges and demands, helping them become more independent and autonomous.

Loneliness is one of the biggest issues the elderly face, and the internet can offer individuals a social life, but it also increases their vulnerability. Social media usage is steadily increasing amongst the elderly as it is becoming a significant platform that allows people to connect and share their experiences.

But, if something or someone seems too good to be true, it usually is, so staying safe online should be a top priority for everyone.

What is digital literacy and digital competence?

Digital literacy refers to the skills required to achieve digital competence, the confident and critical use of information and communication technology for learning, leisure, communication and work. Digital competence, however, has a dual nature. First of all, it is the technical ability to operate programs, pages, and equipment. Secondly, it is the ability to use digital media safely.

Co-funded by the Erasmus+ Programme of the European Union

This project has been funded with support from the European Commission under the Erasmus+ Programme. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein. [Project Number: 2021-1-FR01-KA220-ADU-000033422]

What are some of the reasons for seniors to go online?

The reasons seniors go online include:

- Participating in social and cultural activities
- Keeping in touch with loved ones
- Meeting new friends or romantic partners
- Online banking, shopping and investing
- Making travel arrangements
- Getting medical advice and information including doctor reports and test results
- Sharing and viewing pictures
- Exploring and sharing political views
- And much more

However, like all powerful tools, the Internet and mobile technologies come with some risks, with our devices being exposed to hackers every single day without us even knowing that we are in danger.

What is cyber safety?

Cyber safety is all about staying safe online and protecting yourself against potential risks on the internet. This involves being able to analyse, compare and critically evaluate the credibility and reliability of sources of data, information and digital content as well as having the skills and knowledge to avoid these threats. This includes knowing how to keep personal information private and secure online, protecting devices from malware, avoiding harmful or illegal content, and managing online relationships safely.

Factors that contribute to increased risk for seniors

When it comes to safely navigating the internet, every age group has unique vulnerabilities in addition to general Internet risks, and seniors are no exception. Few entirely new types of scams are created to target seniors; the issue lies in how existing scams are tailored specifically to exploit older Internet users.

For example, while an online scam targeting minors is going to promise trips to Disneyland or cool toys, scams aimed at seniors are more likely to offer discount drugs and low-cost insurance. Phishing scams frequently target seniors with ‘bank notices’ or official looking ‘government documents’.

In addition to being targeted for different types of crime, seniors may share characteristics that make them vulnerable online. Here are some of the major factors that make seniors vulnerable to online scams.

Lack of computer skills

Though many seniors are very computer savvy, many more are not. Often their computers are not properly secured. Even when you have installed security software, it is critical that you set up automatic updates, turn on a firewall, use secure passwords, and so on.

Lack of Internet skills

Though many seniors are cutting edge users of internet services, many are beginners when it comes to computer technology.

Another important thing to note is that even people who are computer savvy, perhaps because they worked with computers before retiring, are sometimes more at risk online because they believe that being computer savvy means they are Internet savvy – but in reality navigating the Internet safely is more a matter of understanding human behavior than understanding technology.

More importantly, understanding the reach of content posted online, how criminals try to deceive you, or the trustworthiness of a site for example, has nothing to do with how well you can use a computer.

Senior users are more trusting

Many seniors are more trusting and respectful of official looking material than younger generations, so are more likely to fall for scams. And seniors tend to be more worried about notices that claim there is a problem with your information that might somehow sully your good name.

In the online world, unless you know for sure with whom you are dealing, you must assume that you could have landed on a ‘look-a-like’ site trying to scam you.

No one can build a fake bank or store on some street corner for a few days, so you never have to worry about whether the bank or store is real. When you enter, you quickly get a sense of whether it is a reputable place or not. If you have a problem with a purchase you can march right back through the door and demand service.

On the Web, those physical attributes and clues are all gone. Anyone can build a website that looks as official and legitimate as any other site for very little money. They can scam search engines to make their websites show up as one of the first results when someone runs a search. Anyone can copy the exact look and content of any other website. This means that the fakes are sometimes very, very hard to identify no matter what your age.

One of the difficulties of online safety is that the threats are constantly changing, getting ever-more sophisticated. However, there are some basic concepts that, when mastered, can help prevent against a wide variety of threats. These include:

Securing Personal Information

The first basic of online safety is protecting personal information. This means being careful about sharing information such as:

- Full name
- Address
- Social security number
- Account usernames and passwords

Protecting Against Malware

Most malware attempt to gain access to a computer or to steal personal information to use for nefarious purposes. They may compromise not only personal security, but can also wreak havoc on software, files, and operating systems. There are a wide variety of attacks at differing levels of sophistication, which can make them difficult to detect or avoid. However, some basic online safety skills can help prevent these attacks:

- Don’t click links or open attachments in emails from people you don’t know.
- Be wary of contests, “freebies,” or awards stating you’ve won something or have “money” or some other award waiting for you.
- Avoid downloading software or files from unknown sources–this includes being wary of pop-up windows that ask you to download something.
- Be wary of error message pop-ups that you don’t understand.

Manage Relationships Safely

Finally, online safety should also include discussing communication students may have with other individuals online and how to manage these relationships safely. This means understanding the risks associated with engaging with others online, including:

- Knowing that some people may not be who they say they are.
- Never meeting someone they’ve met online in real life unless it is thoroughly evaluated, approved and overseen by a parent.
- Telling an adult if someone says something that makes them uncomfortable.

In this modern world, internet safety is a lifelong concern. As technology changes and evolves, learning how to avoid identity theft online will be an ongoing process, so staying abreast of new trends and findings will be important for the young and old alike.

https://www.learning.com/blog/online-safety-definition-basics/

Co-funded by the Erasmus+ Programme of the European Union

This project has been funded with support from the European Commission under the Erasmus+ Programme. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein. [Project Number: 2021-1-FR01-KA220-ADU-000033422]

https://www.atg.wa.gov/internet-safety-seniors

https://www.snbsd.com/about/online-safety-guide

https://www.safetydetectives.com/blog/the-ultimate-internet-safety-guide-for-seniors

Co-funded by the Erasmus+ Programme of the European Union

This project has been funded with support from the European Commission under the Erasmus+ Programme. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein. [Project Number: 2021-1-FR01-KA220-ADU-000033422]

TITLE OF THE MODULE: INSTANT MESSAGING SOCIAL PLATFORMS

Knowledge	Skills	Attitudes
The participant knows of instant messaging social platforms and their functionalities.	The participant knows the functionalities of messaging social platforms	The participants are curious about the subject
The participant is aware of the pros and cons in the use of instant messaging social platforms	The participants is able to identify pros and cons of messaging social platforms	The participants will be more active while also be more aware of using apps
The participant understands how to use instant messaging social platforms safely	The participants is able to avoid risk situations, while using apps	The participant will make conscious decisions about the content he sends and receives.

Introduction to the module

The Internet and social media have come a long way in the last few years. There are now apps which allow you to connect with two or more people at the same time. One of the most important features of these messaging apps is that they allow large groups to talk, chat and send files at the same time. Seniors, the social group most at risk of digital exclusion, can enrich their social life by using social networking platforms for instant messaging. Given the competitive nature of the industry, there are many applications that perform a similar function and all are free and fairly easy to use.

What are we going to learn in this module?

In this module we are going to learn:

- What is instant messaging?
- What are its advantages? What are the main challenges in using it?
- How to choose the most suitable instant messaging application.
- How to use instant messaging safely and securely.

This project has been funded with support from the European Commission under the Erasmus+ Programme. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein. [Project Number: 2021-1-FR01-KA220-ADU-000033422]

Why are those elements important in everyday life

Making new friends and maintaining old ones is time-consuming and demanding and can be a challenge in the 21st century. The digital revolution has rendered old methods of communication obsolete and ineffective. People have not used the telegraph for decades and yet fewer use the postal service to send letters. Seniors often find themselves on the margins of the digital world and nobody seems to remember them. The blessings of the digital world are by no means just reserved for the young. With basic training, anyone of any age can communicate online with ease.

What are instant messaging platforms?

Messaging platforms

A messaging app is an application used to communicate with other users using the Internet. The most popular messaging applications are Discord, WhatsApp, Facebook Messenger, WeChat, Viber and Line and others. These apps allow users to send text messages, images, videos and audio messages to each other and conduct teleconferences. Messaging apps differ from traditional social media apps such as Twitter or Instagram, which are designed to broadcast public messages to a large audience. Messaging apps, on the other hand, are designed for private conversations between two or more people. In general, messaging apps are a convenient and inexpensive way to communicate with others.

The most popular messaging platforms

DISCORD

Discord is an instant messaging social platform. Users have the ability to communicate with voice calls, video calls, text messaging, media and files in private chats or as part of communities called "servers”. A server is a collection of persistent chat rooms and voice channels which can be accessed via invite links. Discord runs on Windows, macOS, Android, iOS, iPadOS, Linux, and in web browsers. As of 2021, the service has over 350 million registered users and over 150 million monthly active users.

WhatsApp

WhatsApp - a mobile application for smartphones that serves as an instant messenger. The app is available for various platforms: iOS, Android and KaiOS. With this app you can send messages and media files between two mobile phones connected to the internet. Installation of the app on the phone is required. It is possible to create group chats, send your own position thanks to Google Maps and share the contacts of your own column. The application also allows video and VoIP calls.

This project has been funded with support from the European Commission under the Erasmus+ Programme. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein. [Project Number: 2021-1-FR01-KA220-ADU-000033422]

FACEBOOK MESSENGER

Facebook Messenger is an instant messaging service created by Meta. It is used to send messages, photos, videos, stickers and other files, and allows you to respond to friends' messages and interact with bots. The service also allows voice calls (including group calls) and video calls. The app offers the ability to encrypt messages and access mini-games.

In April 2017, Facebook Messenger was used by 1.2 billion users.

VIBER

Viber - instant messaging and voice over IP (VoIP) phone call application for smartphones and computers, developed by Viber Media. In addition, users can send photos, videos and audio files. The programme is available for many platforms, including Mac OS, Android, BlackBerry OS, iOS, Series 40, Symbian, Bada, Windows Phone, and Microsoft Windows. Viber uses both 3G/4G and Wi-Fi mobile operator networks. Viber has more than 100 million monthly active users with more than 280 million users registered globally.

Telegram Messenger

Telegram is an app available for both mobile phones and desktops, allowing senders to send free and secure messages. Like WhatsApp, the app encrypts messages and allows them to be destroyed if necessary.

Co-funded by the Erasmus+ Programme of the European Union

This project has been funded with support from the European Commission under the Erasmus+ Programme. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein. [Project Number: 2021-1-FR01-KA220-ADU-000033422]

Signal

It is a free, open source messenger for Android and iOS. Signal uses end-to-end encryption, so app developers, as well as third parties, are unable to read your messages or eavesdrop on your phone calls.

Signal uses standard cellular telephone numbers as identifiers and secures all communications to other Signal users with end-to-end encryption. The client software includes mechanisms by which users can independently verify the identity of their contacts and the integrity of the data channel.

Title: Pros and cons of messaging social platforms

What are the advantages of messaging social platforms?

One of the most important advantages of these messaging apps is that they allow users to chat in real time. Once a message is sent, the recipient is immediately informed of its receipt and can respond instantly. In this way, the correspondence becomes a dynamic dialogue.

This is in contrast to email, which is asynchronous, meaning that messages are not delivered in real time.

Another advantage of messaging apps is that they are often free for app users. This is in contrast to traditional SMS messaging, which can be expensive depending on the tariff plan.

Finally, messaging apps tend to be more private and secure than traditional forms of communication such as email and SMS. This is because messages are often end-to-end encrypted, meaning that only the sender and recipient can read them.

This is extremely important if personal, sensitive data or secrets of any kind are being transmitted.

What are the main challenges in using Instant Messaging Platforms?

Talking to strangers

Meeting and chatting online with strangers poses a risk to seniors, who may be vulnerable to scams and online (and offline) forms of exploiting their ignorance.

Sending inappropriate content

With the physical barrier of a screen, some people feel more empowered to pressure others to send messages, often of a sexual, violent or derogatory nature.

Location sharing

Many apps operate on the basis of identity or phone number information. In many cases, the apps do not always indicate that this information is being used, which means that children may be sharing personal information. As with social networks themselves, privacy and security settings are available on most devices.

Sharing information

Many apps operate on the basis of identity or phone number information. In many cases, apps do not always inform you that this information is being used, which means that they may share personal information. In addition to the social networks themselves, privacy and security settings are available on most devices.

Cyberbullying

Smartphones allow people to take photos and share them instantly on social networks or post information about someone online in seconds. Sometimes this can mean that people of all ages are vulnerable to episodes of cyberbullying.

Distorted image of life

With the rise in popularity of photo-sharing apps such as Snapchat and Instagram, people are increasingly feeling overwhelmed by the vision of successful celebrities posting images of fabulous lives. These are creations of the marketing machine and aim to benefit the publishers financially but become opinionated channels and can lead to low self-esteem in viewers.

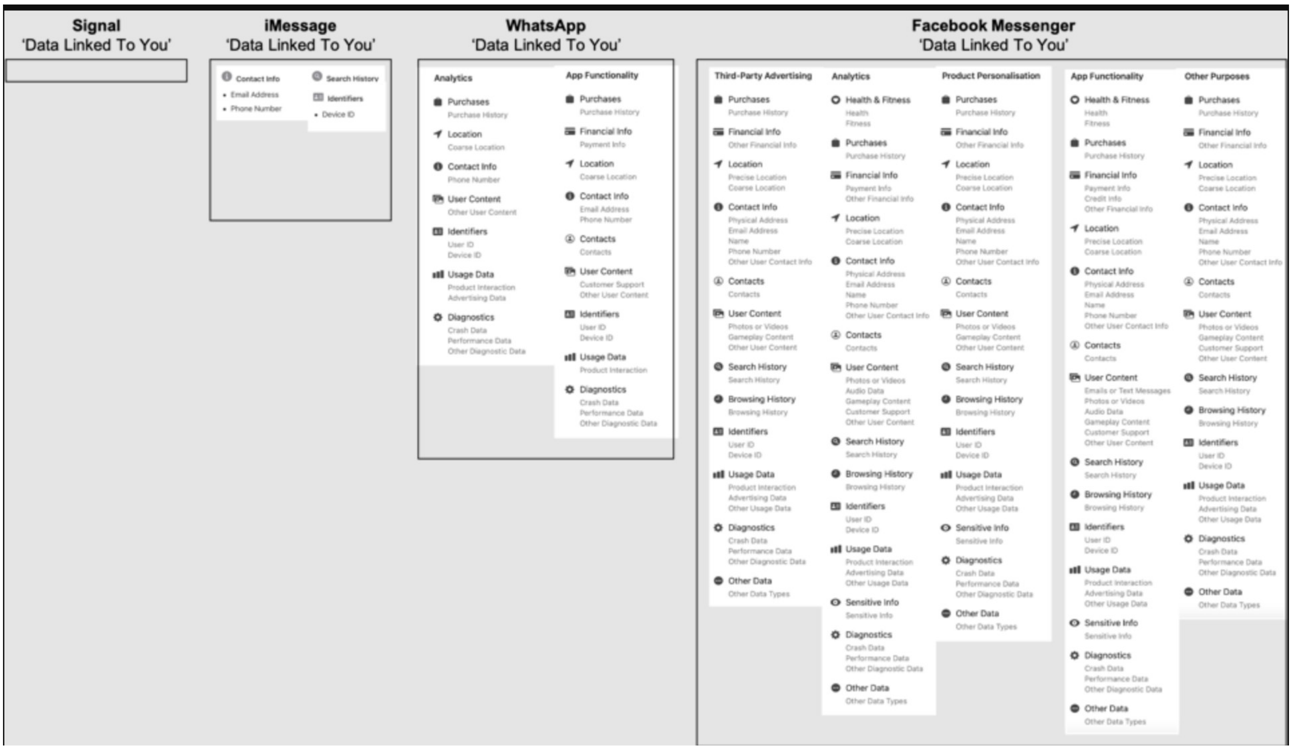
Title: How to choose the most suitable instant messenger?

One of the most important advantages of these messaging apps is that they allow users to chat in real time. Once a message is sent, the recipient is immediately informed of its receipt and can respond instantly. In this way, the correspondence becomes a dynamic dialogue.

Choosing an instant messenger that suits your needs is, despite appearances, a difficult task: you should not only consider functionality and security, but also the availability of friends on a particular platform or the possibility of convincing them to use it. However, this is an individual matter.

Co-funded by the
Erasmus+ Programme
of the European Union

This project has been funded with support from the European Commission under the Erasmus+ Programme. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein. [Project Number: 2021-1-FR01-KA220-ADU-000033422]



Signal
'Data Linked To You'

iMessage
'Data Linked To You'

Contact Info
- Email Address
- Phone Number

Search History

Identifiers
- Device ID

WhatsApp
'Data Linked To You'

Analytics

Purchases
Purchase History

Location
Coarse Location

Contact Info
Phone Number

User Content
Other User Content

Identifiers
User ID
Device ID

Usage Data
Product Interaction
Advertising Data

Diagnostics
Crash Data
Performance Data
Other Diagnostic Data

App Functionality

Purchases
Purchase History

Financial Info
Payment Info

Location
Coarse Location

Contact Info
Email Address
Phone Number

Contacts
Contacts

User Content
Customer Support
Other User Content

Identifiers
User ID
Device ID

Usage Data
Product Interaction

Diagnostics
Crash Data
Performance Data
Other Diagnostic Data

Facebook Messenger
'Data Linked To You'

Third-Party Advertising

Purchases
Purchase History

Financial Info
Other Financial Info

Location
Precise Location
Coarse Location

Contact Info
Physical Address
Email Address
Name
Phone Number
Other User Contact Info

Contacts
Contacts

User Content
Photos or Videos
Gameplay Content
Other User Content

Search History
Search History

Browsing History
Browsing History

Identifiers
User ID
Device ID

Usage Data
Product Interaction
Advertising Data
Other Usage Data

Diagnostics
Crash Data
Performance Data
Other Diagnostic Data

Other Data
Other Data Types

Analytics

Health & Fitness
Health
Fitness

Purchases
Purchase History

Financial Info
Payment Info
Other Financial Info

Location
Precise Location
Coarse Location

Contact Info
Physical Address
Email Address
Name
Phone Number
Other User Contact Info

Contacts
Contacts

User Content
Photos or Videos
Audio Data
Gameplay Content
Customer Support
Other User Content

Search History
Search History

Browsing History
Browsing History

Identifiers
User ID
Device ID

Usage Data
Product Interaction
Advertising Data
Other Usage Data

Sensitive Info
Sensitive Info

Diagnostics
Crash Data
Performance Data
Other Diagnostic Data

Other Data
Other Data Types

Product Personalisation

Purchases
Purchase History

Financial Info
Other Financial Info

Location
Precise Location
Coarse Location

Contact Info
Physical Address
Email Address
Name
Phone Number
Other User Contact Info

Contacts
Contacts

User Content
Photos or Videos
Gameplay Content
Other User Content

Search History
Search History

Browsing History
Browsing History

Identifiers
User ID
Device ID

Usage Data
Product Interaction
Advertising Data
Other Usage Data

Sensitive Info
Sensitive Info

Diagnostics
Crash Data
Performance Data
Other Diagnostic Data

Other Data
Other Data Types

App Functionality

Health & Fitness
Health
Fitness

Purchases
Purchase History

Financial Info
Payment Info
Credit Info
Other Financial Info

Location
Precise Location
Coarse Location

Contact Info
Physical Address
Email Address
Name
Phone Number
Other User Contact Info

Contacts
Contacts

User Content
Emails or Text Messages
Photos or Videos
Audio Data
Gameplay Content
Customer Support
Other User Content

Search History
Search History

Browsing History
Browsing History

Identifiers
User ID
Device ID

Usage Data
Product Interaction
Advertising Data
Other Usage Data

Sensitive Info
Sensitive Info

Diagnostics
Crash Data
Performance Data
Other Diagnostic Data

Other Data
Other Data Types

Other Purposes

Purchases
Purchase History

Financial Info
Other Financial Info

Location
Precise Location
Coarse Location

Contact Info
Physical Address
Email Address
Name
Phone Number
Other User Contact Info

Contacts
Contacts

User Content
Photos or Videos
Gameplay Content
Customer Support
Other User Content

Search History
Search History

Browsing History
Browsing History

Identifiers
User ID
Device ID

Usage Data
Product Interaction
Advertising Data
Other Usage Data

Diagnostics
Crash Data
Performance Data
Other Diagnostic Data

Other Data
Other Data Types

Source: Forbes: “WhatsApp Beaten By Apple’s New iMessage Privacy Update”

https://www.forbes.com/sites/zakdoffman/2021/01/03/whatsapp-beaten-by-apples-new-imessage-update-for-iphone-users/?sh=2a1ca08c3623

Which instant messenger should I choose? I have prepared a short download that may help you to make a decision:

- ✔ If you are looking for a universal instant messenger and want security, but without sacrifices: choose Telegram or Viber
- ✔ If you are looking for an instant messenger with the highest level of security and privacy: choose Signal
- ✔ If you're looking for the simple instant messaging possible and you're smartphone, tablet device user: choose WhatsApp
- ✔ If you are looking for a social communicator, mainly for group discussions: choose Discord or possibly Viber

How to use instant messaging safely and securely

Instant messaging allows you to send messages quickly between users. It is now a very popular form of online conversation. Cybercriminals are well aware of this. That is why they are increasingly using instant messaging for a completely different purpose than we would like.

What should you watch out for?

Here are some of the most common indications that you may be dealing with an attack:

You receive a message that forces you to act immediately.

Example: a) I need an urgent loan, I'll pay it back tomorrow, help!

b) You haven't paid your bill, settle it as soon as possible!

In the message you find a request/request for your personal data, password or other sensitive information that strangers should not have access to. The message you receive makes no sense, e.g. it relates to an event in which you were not involved.

Example: If you didn't take part in the lottery, you can't win anything right?

The message comes from a close friend, family member, colleague, but its style or choice of words does not match it at all. These are just a few examples. However, they all usually have one goal - to force you to act quickly, to arouse strong emotions in you and... to rob you - of your data or money in your account.

And here's the first tip - don't let the pressure get to you. If you receive such a message (it could also be an e-mail) - wait a moment, don't do anything on impulse. Think it over and, if possible, verify.

Think before you click!!!

Attacks based on instant messaging text messages are more dangerous than others because they seem more personal. And this makes us trust them. That's why it's so important that when we receive such a message, which seems suspicious or simply strange, we react accordingly, says Minister Marek Zagórski, the government's plenipotentiary for cyber security. - In such a situation, it is worth starting by asking ourselves: is this message really true, does it make sense, why did we receive it? - he adds.

What else is worth bearing in mind?

- ✔ Never click on links in messages that seem suspicious to you.
- ✔ If you receive a message from a friend that you think is unusual or questionable, call your friend and ask if they really sent you such a message (your friend's account may have been compromised).
- ✔ Do not disclose any confidential data in messages, e.g. passwords, login details.
- ✔ Do not reply to suspicious messages, especially from strangers.
- ✔ Be suspicious/suspicious of all messages, especially those that require you to act immediately. For example, if you get a message about a problem with your bank account, with your credit card - contact your bank directly.

Our vigilance and logical thinking are the best protection against any cyberattacks and fraud on the internet.

It is also worth taking care of the security of the very communicator we use. Unencrypted text messages can be intercepted by almost anyone. That's why it's a good idea to use communicators that use end-to-end encryption.

If you care about privacy - use communicators that make minimal use of and save your data.

Time for a quiz! True or False

1. Instant messaging allows you to send messages quickly between users. (true, Once a message is sent, the recipient is immediately informed of its receipt and can respond instantly.)
2. The most universal instant messenger and want security, but without sacrifices are Telegram and Messenger (false, universal instant messenger and want security, but without sacrifices are Telegram or Viber)
3. Meeting and chatting online with strangers poses a risk to seniors (true, they are vulnerable to scams and online (and offline) forms of exploiting their ignorance.)

Co-funded by the Erasmus+ Programme of the European Union

This project has been funded with support from the European Commission under the Erasmus+ Programme. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein. [Project Number: 2021-1-FR01-KA220-ADU-000033422]

4. SMS messaging is the most private and secure way of communication/form of communication (false, no, only instant messaging allows you to send fully secured messages).
5. Many apps operate on the basis of identity or phone number information (true, to register you must provide either your email or phone number)
6. Do not disclose any confidential data in messages, e.g. passwords, login details. (true, messaging platforms never asks for this data)

WRAP UP – the most important points of this module.

1. A messaging app is an application used to communicate with other users using the Internet. These apps allow users to send text messages, images, videos and audio messages to each other and conduct teleconferences

2. The highest level of security and privacy provides a Signal application.

3. One of the most important advantages of these messaging apps is that they allow users to chat in real time. Once a message is sent, the recipient is immediately informed of its receipt and can respond instantly. In this way, the correspondence becomes a dynamic dialogue.

4. Never click on links in messages that seem suspicious to you.

This project has been funded with support from the European Commission under the Erasmus+ Programme. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein. [Project Number: 2021-1-FR01-KA220-ADU-000033422]

INFORMATION AND DATA LITERACY: Whatsapp + phone related risks (messages, calls)

Knowledge	**Skills**	**Attitudes**
Knows that some online content in search results may not be open access or freely available and may require a fee or signing up for a service in order to access it.	Can choose the search engine that most likely meets one's information needs as different search engines can provide different results even for the same query.	Intentionally avoids distractions and aims to avoid information overload when accessing and navigating information, data and content
Aware that search engines, social media and content platforms often use AI algorithms to generate responses that are adapted to the individual user	Knows how to handle information overload and "infodemic" (i.e. increase of false or misleading information during a disease outbreak) by adapting personal search methods and strategies	Values tools designed to protect search privacy and other rights of users
Aware that online environments contain all types of information and content including misinformation and disinformation, and even if a topic is widely reported it does not necessarily mean it is accurate	Carefully considers the top/first search results in both text-based and audio searches, as they may reflect commercial and other interests rather than be the most appropriate results for the query	Inclined to ask critical questions in order to evaluate the quality of online information, and concerned about purposes behind spreading and amplifying disinformation.
Aware of potential information biases caused by various factors (e.g. data, algorithms, editorial choices, censorship, one's own personal limitations).	Knows how to find the author or the source of the information, to verify whether it is credible (e.g. an expert or authority in a relevant discipline).	Willing to fact-check a piece of information and assess its accuracy, reliability and authority, while preferring primary sources over secondary sources of information where possible.
Aware that many applications on the internet and mobile phones collect and process data (personal data, behavioural data and contextual data) that the user can access or retrieve, for example, to monitor their activities online (e.g. clicks in social media, searches on Google) and offline (e.g. daily steps, bus rides on public transport).	Knows how to collect digital data using basic tools such as online forms, and present them in an accessible way (e.g. using headers in tables).	Considers transparency when manipulating and presenting data to ensure reliability, and spots data that are expressed with underlying motives (e.g. unethical, profit, manipulation) or in misleading ways.

Co-funded by the Erasmus+ Programme of the European Union

This project has been funded with support from the European Commission under the Erasmus+ Programme. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein. [Project Number: 2021-1-FR01-KA220-ADU-000033422]

Introduction to the module

Social media has completely changed the way we interact with one another. For instance, we can use these platforms to communicate with our distant friends and relatives. For the younger age, it is a common form of communication. Let's discuss the benefits and challenges of social media for seniors. WhatsApp, the Meta-owned messaging platform, is one of the world's most popular messaging apps. It is estimated that over one billion people use the app, sending over 65 billion messages per day. WhatsApp is a free smartphone communication program to download. WhatsApp sends messages, photos, audio, and video over the internet. The service is quite similar to text messaging services; but, because WhatsApp sends messages over the internet, it is substantially less expensive than texting.

Viber is a fully encrypted texting app that has applications for your smartphone, tablet and computer. One differentiator with Viber is that it allows public accounts, which are usually set up by brands or celebrities, to engage with an audience. Viber is a free app that allows users to make free calls, send text messages, photos, and videos to other Viber users. It may be used to connect with individuals all around the world and works on both mobile and desktop computers.

Telegram is a cloud-based messaging service that touts itself to be, "the fastest and most secure mass-market messaging system in the world." Telegram's Secret Chat feature allows the user to program messages to delete automatically from both devices after two seconds or up to one week.https://www.makeuseof.com/tag/4-security-threats-whatsapp-users-need-know/

What are we going to learn in this module?

In this module we are going to learn:

- ✔ Recognize how social media works.
- ✔ Engage in responsible behaviour in online communities
- ✔ Use social media to positively impact the world

Why are those elements important in everyday life?

Co-funded by the Erasmus+ Programme of the European Union

This project has been funded with support from the European Commission under the Erasmus+ Programme. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein. [Project Number: 2021-1-FR01-KA220-ADU-000033422]

Social networking websites are frequently used by seniors as a communication tool.

Social media has become an everyday factor in our lives. More and more people want to stay connected and seniors jump on that train! We need to ensure the benefits but also the risk that this contains.

Time for a quiz! Select the right answer

Question: What are social media applications such as whatsapp and viber?

A: A way to stay connect

B: Just devices

Understanding the benefits and risks of online platforms

Social media has a number of significant **benefits** for seniors, including:

- **Keeping in touch with loved ones:** Social media is obviously a fantastic method to remain in touch with loved ones. This applies particularly to those who reside far away. Seniors can see and communicate with their friends and family whenever they want.
- **Reduces their feeling of being alone:** Social media connections can make seniors feel less isolated in this big world. They provide companionship for elderly people who are isolated or lonely. It gives them a sense of belonging and community, which can help them combat isolation. Additionally, it might lead to better physical and mental wellness.
- **Easy information access:** Almost anything you want to know may now be found online. Seniors may also instantly obtain knowledge on a wide range of topics thanks to social media! On these sites, you may get everything from news sources to cooking instructions and medical advice. This can be beneficial, especially if they're seeking specific information or assistance.
- **Make new friends:** Social media is a great way to meet new people and develop friendships. It can be incredibly great to make even one new friend in a world where people are more estranged than ever!

On the other hand, social media contains some **risks** for seniors, including:

This project has been funded with support from the European Commission under the Erasmus+ Programme. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein. [Project Number: 2021-1-FR01-KA220-ADU-000033422]

- **Negative impact for their health:** Technology has been generally useful, but spending too much time in front of a screen has its own set of dangers. Social media use too much can be harmful to your health. That covers bad dietary practices, inactivity, and sleep deprivation. Anxiety and despair may also worsen if you spend too much time on social media.
- **Addictive:** Social media has the potential to become addicting. And it might not be the greatest idea for your loved one to use social media if they already experience loneliness or sadness.
- Risk of online fraud: Senior citizens are frequently simple online fraud targets. They might not be as careful as the younger generation, which causes this. Social networks can therefore be a doorway for con artists who will do everything in their power to get your personal information or money. Therefore, it's crucial to use social media with caution and to always be on the lookout for any scams.

Time for a quiz! Select the right answer

Question: You just received a message on Viber from an unknown number saying is your daughter and this is her new number and she is in trouble asking for some money immediately. What do you do?

A: Answer the message and send the money

B: Ignore and block the number

Co-funded by the Erasmus+ Programme of the European Union

This project has been funded with support from the European Commission under the Erasmus+ Programme. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein. [Project Number: 2021-1-FR01-KA220-ADU-000033422]