MILEAGE

RISCHIO ANALISI E BARRIERE

MILEAGE

INTRODUZIONE

L'obiettivo principale del progetto MILEAGE è quello di creare un modo nuovo e più coinvolgente per promuovere le competenze digitali degli anziani e l'alfabetizzazione mediatica e informativa (MIL) per responsabilizzarli nell'uso degli strumenti ICT nella vita di tutti i giorni sensibilizzando sui pericoli digitali e su come affrontarli.

Come?

- Con un rapporto sui rischi e le barriere affrontate dagli anziani nell'ambiente digitale
- Con lo sviluppo di scenari di rischio virtuali (role playing)
- Con la creazione di micro lezioni con spiegazioni suirischi definiti
- Con la stesura di un vademecum per educatori adulti con orientamento a supporto delle attività formative (effetto moltiplicatore).

Questo rapporto sui rischi e le barriere presenta i principali social media, strumenti di comunicazione e altre piattaforme ampiamente utilizzate al giorno d'oggi. Descriviamo specificamente i rischi e i pericoli ad essi associati: ogni problema o rischio viene analizzato e viene offerta una soluzione per superarlo, elencando anche le competenze necessarie e attivate nel farlo.

Questo documento è stato creato per fornire ai formatori, agli anziani e al pubblico in generale alcune informazioni relative all'ambiente digitale che gli individui senior affrontano nella loro vita quotidiana, offrendo alcuni suggerimenti e consigli per migliorare le competenze digitali degli anziani e la fiducia nel mondo digitale. Questo documento guiderà lo sviluppo dei nostri contenuti formativi e degli scenari di rischio creati attraverso il progetto per supportare l'alfabetizzazione mediatica e informativa per gli anziani.

MILEAGE

CONTENUTO

Nome del social media / strumento	**WHATSAPP**
Generalità	WhatsApp è un programma di comunicazione gratuito per smartphone da scaricare. WhatsApp invia messaggi, foto, audio e video su Internet. Il servizio è abbastanza simile ai servizi di messaggistica di testo; ma, poiché WhatsApp invia messaggi su Internet, èsostanzialmente meno costoso degli SMS. Puoi anche utilizzare Whatsapp sul tuo computer visitando il sito Web di Whatsapp e scaricando il programma per Mac o Windows. A causa di funzionalità come chat di gruppo, messaggi audio e condivisione della posizione, è molto popolaretra i giovani.
Rischio associato ai social media/strumento: **Privacy, accuratezza, proprietà, accessibilità, violazione delle leggi, copyright**	Privacy Furto di profili Registrazione delle chiamate (crimini informatici)
Barriere/difficoltà per gli adulti	Impostazioni sulla privacy.
Pericolo dei social media / strumento negli adulti	Hacker Backup non crittografati
Soluzioni che possiamo avere	Non fornire mai il codice di registrazione o il PIN per la verifica in due passaggi a nessun altro. Crea un codice per il tuo dispositivo. Tieni traccia di chi ha accesso al tuo telefono a livello fisico. Conoscenza delle applicazioni e delle loro impostazioni.

Nome del social media / strumento	**VIBER**
Generalità	Viber è un'app gratuita che consente agli utenti di effettuare chiamate gratuite, inviare messaggi di testo, foto e video ad altri utenti Viber. Può essere utilizzato per connettersi con persone in tutto il mondo e funziona su computer portatili e desktop. L'app di messaggistica aveva 236 milioni di utenti attivi mensili a partire da febbraio 2015. La condivisione di immagini, video e chat di gruppo sono tutte funzionalità popolari per i consumatori giovani, simili a WhatsApp.
Rischio associato ai social media/strumento: **Privacy, accuratezza, proprietà, accessibilità, violazione delle leggi, copyright**	Cyberbullismo Privacy Chiamate spam
Barriere/difficoltà per gli adulti	Impostazioni sulla privacy
Pericolo dei social media / strumento negli adulti	Hacker
Soluzioni che possiamo avere	Tieni traccia di chi ha accesso al tuo telefono a livello fisico. Conoscenza delle applicazioni e delle loro impostazioni. Blocco di un altro utente su Viber (quando si riceve un messaggio da un contatto sconosciuto.)

Nome del social media / strumento	**AZIENDE RICETTIVE**
Generalità	Per albergatore si intende chiunque fornisca alloggio dietro retribuzione o che accolga più di 5 cittadini stranieri, tranne nei casi in cui lo straniero e il fornitore possano essere considerati in stretta parentela. Esempi: Hotel, B&B, Airbnb, Booking
Rischio associato ai social media/strumento: **Privacy, accuratezza, proprietà, accessibilità, violazione delle leggi, copyright**	Truffe Disinformazione / fuorviante Frodi con carte
Barriere/difficoltà per gli adulti	Uso dellatecnologia per prenotare l'alloggio Termini e condizioni che non sono visibili
Pericolo dei social media / strumento negli adulti	Uso della tecnologia per prenotare l'alloggio Termini e condizioni che non sono visibili Non accessibile agli anziani Isolamento
Soluzioni che possiamo avere	Queste difficoltà non implicano che l'invecchiamento sul posto sia un obiettivo irraggiungibile o indesiderabile, ma piuttosto che è necessaria un'ampia pianificazione sia a livello individuale che comunitario. La primafase è quella di educare le società di alloggio sui problemi finanziari e fisici che possono affrontare se rimangono nella loro casa esistente, nonché le soluzioni disponibili per risolverli. Così come garantire che i governi locali siano consapevoli e preparati per i problemi che i loro cittadini anziani dovranno affrontare.

Nome del social media / strumento	**COMPAGNIE DI VOLO**
Generalità	Un'organizzazione che fornisce il trasporto aereo per passeggeri e merci.
Rischio associato ai social media/strumento: **Privacy, accuratezza, proprietà, accessibilità, violazione delle leggi, copyright**	Truffe Disinformazione Frodi con carte
Barriere/difficoltà per gli adulti	Uso della tecnologia per prenotare il volo
Pericolo dei social media / strumento negli adulti	Uso della tecnologia per prenotare il volo Termini e condizioni che non sono visibili Non accessibile agli anziani
Soluzioni che possiamo avere	Pianifica in anticipo Ricerca viaggi aerei senior e assistenza Gestisci il tuo parcheggio per soddisfare i problemi di mobilità Preparati per la sicurezza aeroportuale Controlla il biglietto aereo scontato per gli anziani Scegli l'orario di volo giusto

Nome del social media / strumento	**PIATTAFORME DI INCONTRI**
Generalità	Le piattaforme di incontri sono siti Web o app che consentono alle persone di contattare e comunicare per sviluppare una relazione. L'accesso a questi siti richiede spesso agli utenti di fornire informazioni personali come età, sesso e posizione geografica. Esistono centinaia di piattaforme di incontri diverse. Può essere generalista o specializzato per un tipo di relazione (amore, erotico, amicizia) o un tipo di membri (appartenenza religiosa o etnica, orientamento sessuale e fascia d'età). Alcune delle piattaforme più conosciute sono: Meetic, Tinder, Bumble, eDarling, Badoo, OkCupid, ecc. Sebbene la maggior parte delle piattaforme di incontri siano gratuite, alcune richiedono una quota di abbonamento mensile o il pagamento di funzionalità aggiuntive a pagamento.
Rischio associato ai social media/strumento:	Privacy Pesce gatto
Barriere/difficoltà per gli adulti	La principale difficoltà per gli anziani con piattaforme di incontri è l'uso pratico di questi strumenti. Per essere in grado di utilizzare tali piattaforme, gli anziani hanno bisogno di una conoscenza abbastanza avanzata delle TIC. Ad esempio, devono utilizzare un indirizzo e-mail per accedere, il che implica che devono sapere come creare un indirizzo e-mail e utilizzarlo. La piattaforma richiede anche il caricamento di immagini, ma gli anziani non sanno necessariamente come farlo.
Pericolo dei social media / strumento negli adulti	**Privacy** Gli utenti condividono informazioni personalisu piattaforme di incontri, sperando di trovare le migliori corrispondenze. Le informazioni che condividono includono foto di se stessi, orientamento sessuale, età, religione, sesso, hobby, se hanno figli, altezza, ecc. Inoltre, le piattaforme di incontri offrono spesso l'opzione di collegare i loro profili ai loro account di social media come Facebook o Instagram, consentendo all'app di appuntamenti di essere sincronizzata con i social media e visualizzando informazioni personali come le immagini da caricare automaticamente sul loro profilo di appuntamenti. Diverse piattaforme di incontri hanno subito una violazione della sicurezza, che può essere particolarmente dannosa per gli utenti poiché i dati sensibili sono condivisi su tali piattaforme. **Pesce gatto**

	Gli anziani che si registrano sulle piattaforme di incontri sono spesso soli (divorziati, vedovi) e quindi ripongono grandi speranze neltrovare un potenziale partner. Tuttavia, molti profili falsi e truffe si verificano su queste piattaforme. Le persone fingono di essere qualcosa che non sono e si investono in una relazione sentimentale per stabilire un legame e usarlo per estrarre denaro.
Soluzioni che possiamo avere	Prima di creare un account, gli utenti devono rivedere l'informativa sulla privacy e i termini di servizio della piattaforma. È importante fermarsi a leggere e comprendere questi termini il più possibile per poter dare il consenso informato. La pesca al gatto può causare danni reali. Per evitarlo, gli utenti possono chiedere una videochiamata con la persona con cui stanno parlando per verificare che corrispondano alle immagini sul sito web. Gli utenti possono anche utilizzare strumenti come Google Reverse Photo Search per verificare se la foto è originale o se proviene da qualcun altro. Ancora più importante, è importante che gli utenti si fidino del loro istinto se sentono di essere stati pescati e quindi rimangono cauti nel condividere molti dettagli.

Nome del social media / strumento	**SERVIZI BANCARI ONLINE**
Generalità	L'online banking è anche conosciuto come Internet Banking, net banking o e-banking. Si tratta di un sistema di pagamento elettronico che consente al cliente di una banca o di un istituto finanziario di effettuaretransazioni finanziarie o non finanziarie online via Internet. Questo servizio offre accesso online a quasi tutti i servizi bancari, tradizionalmente disponibili attraverso una filiale locale, inclusi trasferimenti di fondi, depositi e pagamenti di fatture online ai clienti. È possibile accedervi da qualsiasi individuo che si sia registrato per l'online banking presso la banca, abbia un conto bancario attivo o qualsiasi istituto finanziario. Online Banking offre accesso 24 ore su 24 ai conti degli utenti ogni giorno. È veloce e conveniente consentireg di eseguire transazioni ovunque, in qualsiasi momento, su qualsiasi dispositivo (computer, smartphone, tablet) con accesso a Internet Alcune banche online sono banche tradizionali che offrono anche servizi bancari online, mentre altre sono solo online e non hanno presenza fisica.

	Secondo Eurostat, nel 2020 la media della popolazione che utilizza l'online banking nell'UE era del 60%. NellaRepubblica ceca ha raggiunto il 70%, ma in Polonia solo il 49%. In Italia, l'86,8% delle persone che utilizzano Internet utilizza anche un sito Web o un'app bancaria. Nell'ultimo World Retail Banking Report, il 57% dei consumatori afferma di preferire l'internet (online) banking al tradizionale branch banking. E il 55% dei consumatori ora preferisce utilizzare app di mobile banking per rimanere sotto controllo delle proprie finanze, rispetto al 47% nell'era pre-pandemia.
Rischio associato ai social media/strumento: **Privacy, accuratezza, proprietà, accessibilità, violazione delle leggi, copyright**	Privacy Cyber-crimes: furto di dati e frodi.
Barriere/difficoltà per gli adulti	Le difficoltà per gli adulti anziani riguardano la questione della paura e della fiducia, nonché la mancanza di conoscenza e guida su come utilizzare il sistema bancario online della loro banca.
Pericolo dei social media / strumento negli adulti	**Mancanza di fiducia** I dati raccolti da Casalo et al (2007) hanno dimostrato che la sicurezza e la privacy del sito web, l'usabilità e la reputazione hanno un effetto diretto e significativo sulla fiducia dei consumatori nel sito web dei servizi finanziari. Si osserva che la fiducia è un fattore chiave di mediazione nello sviluppo del finanziamento online. **Frodi e furti di dati** Questo rischio è più una paura comune che un problema frequente. Infatti, secondo un sondaggio condotto nel 2020 dall'Agenzia europea per i diritti fondamentali, un quarto degli europei (24%) è molto preoccupato che i dati del proprio conto bancario online o della carta di pagamento vengano utilizzati in modo improprio. Ma nel complesso, meno di 1 su 10 (8%) ha subito frodi bancarie online o con carta nei cinque anni precedenti il sondaggio. Le persone nel Regno Unito (24%), Francia (19%) e Danimarca (15%) hanno maggiori probabilità di avere un'esperienza del genere. **Sicurezza** Il rischio per la sicurezza è collegato al crescente numero di siti Web bancari fraudolenti, con e-mail false che pretendono di essere inviate dalle banche, con l'uso di programmi cavallo di per acquisire ID utente e password. Esistono anche rischi di hacking (un hacker che entra in un conto bancario e ruba i fondi) anche se sono molto rari.

	Privacy Secondo uno studio del 2020 pubblicato da KPMG, l'87% dei consumatori afferma che la privacy dei dati è un diritto umano fondamentale. Eppure il 68% afferma di non fidarsi delle aziende per vendere eticamente i propri dati personali. **Violazione dei dati e phishing** Nel 2020, gli specialisti hanno scoperto un problema di sicurezza con una banca, la 5a banca più grande d'Europa e la 16a più grande del mondo. La filiale belga della banca ha avuto una configurazione errata nel dominio del suo sito web, consentendo il download dei suoi file. Questifile contenevano informazioni sensibili (nome, e-mail, telefono) che potevano essere utilizzate dagli hacker per i potenziali clienti della banca. Il phishing è un tipo di attacco spesso utilizzato per rubare i dati di un utente, comprese le credenziali di accesso e i numeri di carta di credito. Si verifica quando un utente malintenzionato, fingendo di essere un'entità attendibile, inganna una vittima nell'apertura di un'e-mail, un messaggio istantaneo o un messaggio di testo e ruba le sue informazioni.
Soluzioni che possiamo avere	**Imparare a utilizzare l'online banking – tutorial** Per guidarvinell'utilizzo del vostro strumento di online banking, chiedete al vostro banchiere il tutorial della banca. Ogni banca ne ha prodotto uno. **Sicurezza e Online Banking** I portali bancari online sono protetti da ID utente/cliente e password univoci. Alcuni di essi hanno bisogno di una chiave sicura (dispositivo) che genera un codice univoco ad ogni connessione). **Previsione delle frodi** Nel contesto dell'online banking, la previsione delle frodi consiste nelcreare profili di clienti basati su informazioni storiche raccolte durante le attività bancarie online (terminali utilizzati, ora e luogo abituali di connessione, viaggi di connessione e attività, ecc.) e quindi prevedere il grado di frode dell'operazione corrente, confrontando il comportamento attuale del cliente con il suo profilo. Se il grado di frode è considerato elevato, l'operazione viene bloccata. **Reazione alla frode** Le banche offrono anche una linea diretta (telefonica o online) per denunciare le frodi eper prevenire le frodi. **Consigli pratici**

	• Utilizzare password sicure e aggiornarle regolarmente • Scegli password univoche per ogni conto bancario digitale, non utilizzare la stessa password per più account • Utilizzare un gestore di password sicuro per memorizzare le password • Evita di utilizzareun Wi-Fi pubblico non protetto quando accedi ai conti finanziari online • Sapere come riconoscere le truffe di phishing via email o testo • Visita solo siti Web sicuri • Installa protezioni antispyware e malware sui tuoi dispositivi • Imposta avvisi per tracciare i tuoi account e monitorarel'attività di tr ansaction • Abilita l'autenticazione a più fattori

Nome del social media / strumento	**PAGAMENTI ONLINE**
Generalità	I pagamenti online vengono effettuati su siti di e-commerce tramite carte di credito ma anche tramite e-wallet. Bonifici bancari, carte virtuali e voucher sono anche altri metodi di pagamento digitale. Secondo Statista, nel 2019 , un europeo su cinque ha preferito utilizzare le applicazioni di pagamento Fintech per i propri acquisti online nel 2019. Le carte di debito si sono classificate come il metodo di pagamento online più popolare, con Apple Pay e Google Pay utilizzati da circa il tre percento degli intervistati. Per quanto riguarda gli e-wallet, i dati non sono ancora disponibili ma è un mercato in costante crescita. Piattaforme di pagamento online e portafogli elettronici: • PayPal • Google Pay • Apple Pay • Ali Paga • Samsung Pay • Mobikwik • Paytm • Amazon Pay

	• Portafoglio Microsoft • Stipe • Klarna
Rischio associato ai social media/strumento: **Privacy, accuratezza, proprietà, accessibilità, violazione delle leggi, copyright**	Privacy Cyber-crime: furto di dati e frodi online.
Barriere/difficoltà per gli adulti	Le difficoltà presentate per gli adulti anziani riguardano la questione della paura e della fiducia in quanto i casi di frode nei pagamenti sono molto mediatizzati. L'altra difficoltà riguarda l'uso pratico di questo strumento. I diversi tipi di pagamento online possono essere difficili da capire e i numerosi passaggi necessari per concluderlo potrebbero essere tecnicamente impegnativi.
Pericolo dei social media / strumento negli adulti	**Privacy** Mentre oggi il contante consente pagamenti anonimi - e quindi nessuna tracciabilità degli acquisti effettuati e nessun rischio per la privacy - non è il caso dei pagamenti online altamente tracciabili (indirizzo IP, nome, cognome, indirizzo, numero di carta ecc.). **Dati ilft** La quantità di dati condivisi durante le transazioni di pagamento online solleva la questione del furto di dati. Secondo il Norton Global Cyber Safety Report 2019, più della metà degli intervistati ha subito un crimine informatico, mentre 1 su 3 è stato vittima negli ultimi 12 mesi. 4,1 miliardi di record sono stati esposti a livello internazionale e c'è stato un aumento del 54% del numero di violazioni segnalate. **Frodi online** Secondo la Banca centrale europea, il valore totale delle transazioni fraudolente utilizzando carte emesse in tutto il mondo ammontava a 1,80 miliardi di euro nel 2018. Per quanto riguarda le carte emesse solo nell'area dell'euro, il valore totale delle operazioni fraudolente con carta ammontava a 0,94 miliardi di euro nel 2018.
Soluzioni che possiamo avere	**Multi Factor Authentication (MFA) o Two Factor Authentication (2FA)** Si tratta di un metodo di autenticazione elettronica in cui a un utente viene concesso l'accesso a un servizio solo dopo aver presentato con successo due o più elementi di prova (o fattori) a un meccanismo di autenticazione: **Conoscenza**: qualcosa che solo l'utente conosce, normalmente presentato come risposta a una domanda come il nome di un animale domestico

	Possesso: qualcosa che solo l'utente ha come uno smartphone o un token. Nel caso dello smartphone, verrà inviato un sms al tuo telefonocon un codice da digitare. **Inerenza**: qualcosa che solo l'utente comprende l'uso del riconoscimento oculare e facciale o delle impronte digitali. **Richiedi il CVV** Sono i tre numeri dietro la carta di credito e ti vengono chiesti durante una transazione di pagamento online per assicurarti di essere in possesso della tua carta di credito. **Elaborazione sicura dei pagamenti** Avviene attraverso portali di pagamento online certificati PCI, SSAE-16 e HIPAA. Clienti e fornitori non devono preoccuparsi che i loro dati sensibili vengano trapelati e rubati dagli hacker.

Nome del social media / strumento	**INSTAGRAM**
Generalità	Instagram è un servizio di social networking americano per la condivisione di foto e video. L'app consente agli utenti di caricare media che possono essere modificati con filtri e organizzati per hashtag e tag geografici. I post possono essere condivisi pubblicamente o con follower pre-approvati. Gli utenti possono sfogliare i contenuti di altri utenti per tag e posizioni e visualizzarei contenuti di tendenza. Gli utenti possono mettere "Mi piace" alle foto e seguire altri utenti per aggiungere i loro contenuti a un feed personale. Il servizio ha anche aggiunto funzionalità di messaggistica, la possibilità di includere più immagini o video in un singolo post e una funzione "storie" che consente agli utenti diinserire foto e video in un feed sequenziale, con ogni post accessibile da altri per 24 ore ciascuno. Alla fine del 2021, c'erano 2,9 milioni di utenti nella Repubblica Ceca. Questa è la rete in più rapida crescita. È più popolare tra gli utenti di età compresa tra 15 e 29 anni.
Risk associato al social media / strumento:	Privacy Furto di profili

Privacy, accuratezza, proprietà, accessibilità, violazione delle leggi, copyright	Impatto sulla salute mentale (sintomi deprimenti, ansia, stress, dipendenza, soddisfazione per l'aspetto, falsa interpretazione di sé,immagine corporea, solitudine, esclusione sociale, soddisfazione di vita, ecc.)
Barriere/difficoltà per gli adulti	Difficoltà a trovare coetanei (il 71% degli utenti di Instagram ha meno di 35 anni). Richiesta di dati personali (come la data di nascita). Impostazioni sulla privacy.
Danger dei social media/strumento negli adulti	Privacy - l'utente della rete dovrebbe prestare attenzione a chi segue e da chi viene seguito, o chi può vedere le informazioni personali e le foto / video. Furto del profilo: l'account potrebbe essere "rubato", lefoto dell'utente potrebbero essere utilizzate da qualche altra parte o gli hacker potrebbero agire a suo nome.
Soluzioni che possiamo avere	Conoscenza delle applicazioni e delle sue impostazioni, regole su come comportarsi su Instagram. Utilizzando una password complessa e la sua modifica regolare. Autenticazione a due fattori (in un computer e sul telefono). Account privato per profilo personale. Utilizzando solo applicazioni autorizzate.

Nome del social media / strumento	**SKYPE**
Generalità	Skype è un'applicazione di telecomunicazioni proprietaria gestita da Skype Technologies, una divisione di Microsoft, meglio conosciuta per la videotelefonia basata su VoIP, la videoconferenza e le chiamate vocali. Ha anche messaggistica istantanea, trasferimento di file, chiamate basate su debito verso telefoni fissi e mobili (su reti telefoniche tradizionali) e altre funzionalità. Skype è disponibile su varie piattaforme desktop, mobili e console per videogiochi. La popolarità di Skype è aumentata significativamente durante la pandemia.
Rischio associato ai social media/strumento: **Privacy, accuratezza, proprietà, accessibilità, violazione delle leggi, copyright**	Privacy Furto di profili Registrazione delle chiamate (crimini informatici)

Barriere/difficoltà per gli adulti	Impostazioni sulla privacy.
Pericolo dei social media / strumento negli adulti	Chiamate non richieste. Diffidenza verso gli altri utenti.
Soluzioni che possiamo avere	Conoscenza delle applicazioni e delle loro impostazioni. Sfondo ben scelto - dove la fotocamera è puntata (non per mostrare l'attrezzaturadell'appartamento, ecc.). Spegnere la fotocamera quando non serve. Silenzio durante una chiamata (non accendere la TV, ad esempio), disattivare l'audio del microfono quando non è necessario. Uso delle cuffie. Non tollerare l'ingresso di partecipanti indesiderati, non fare clic su link sospetti.

Nome del social media / strumento	**NOTIZIE FALSE**
Generalità	Le notizie false, o comunemente intese come disinformazione, sono definite come "articoli di notizie che sono intenzionalmente e verificabilmente falsi e potrebbero fuorviare i lettori" (Allcott e Gentzkow, 2017, p.213) Il termine "notizie false" non è nuovo. Wardle e Derakhshan (2017) hanno suddiviso il termine fake news in tre diversi tipi. Hanno definito la disinformazione come "false informazioni condivise senza intento dannoso", la disinformazione come "falsa informazione condivisa con intento dannoso" e, infine, la disinformazione è definita come "informazioni autentichecondivise per causare danni" (p.5). Dove altro, i ricercatori Lazer et al. (2018, p.2) hanno definito le notizie false come "informazioni fabbricate che imitano il contenuto

	dei media di notizie nella forma ma non nel processo o nell'intento organizzativo". Pertanto, Fake-News si riferisce spesso a notizie false, ma che sembrano essere notizie legittime. Internet è una fonte comune di notizie false, con notizie false frequentemente promosse e diffuse sui social media. Le notizie false possono riguardare qualsiasi argomento. Ad esempio, è stata prodotta una notevole quantità di notizie false sul coronavirus e sui vaccini.
Rischio associato ai social media/strumento: **Privacy, accuratezza, proprietà, accessibilità, violazione delle leggi, copyright**	Le persone in tutto il mondo stanno assistendo a un drammatico aumento dell'accesso alle informazioni e alla comunicazione. Mentre alcune persone sono affamate di informazioni, altre sono inondate di stampa, trasmissione e contenuti digitali. Recenti studi condotti a livello globale tra le persone hanno dimostrato che hannodifficoltà a pensare criticamente ai media e a giudicarne la credibilità, specialmente online. Tra le molte questioni, lo studio ha suggerito che la maggior parte delle persone - non hanno una buona comprensione di ciò che costituisce "fake news" rispetto alle notizie reali. Non riuscivo a capire la differenzatra articoli sponsorizzati e notizie reali. non si è preoccupato di verificare da dove provenisse la provenienza delle foto online e ha accettato ciecamente i contesti dichiarati delle foto. Non riuscivo a capire la differenza tra un vero articolo di notizie e un articolo di notizie false dall'aspetto reale sui social media. non è stato in grado di identificare i contenuti di parte provenienti da fonti di notizie indipendenti supportate da gruppi come società di lobbying come meno affidabili di una fonte di notizie mainstream Di fronte a molteplici problemi di incitamento all'odio, o cyberbullismo, o contenuti hackerati di YouTu,o notizie false ecc., Stiamo assistendo a richieste urgenti per gestire meglio l'ambiente dei media - in particolare, per regolare Internet. Ma di fronte a scontri tra diritti positivi e negativi, difficoltà normative, potenti aziende globali e convenienza politica a breve termine, questo appello a sua volta si trasforma rapidamente in un appello per la soluzione apparentemente "più morbida" di educare il pubblico che utilizza Internet.
Barriere/difficoltà per gli adulti	Ciò che preoccupa gli studiosi è l'effetto delle notizie false sullapercezione pubblica che li induce a prendere decisioni ragionevoli basate sulla disinformazione (Tandoc et al., 2018). Ciò è ancora più vero quando gli utenti hanno maggiori probabilità di condividere notizie negative e, con la recente pandemia, ci sono molte notizie relative al Covid-19 che sono negative (Nyilasy, n.d.). 374 Di conseguenza, Chen et al. (2011) hanno sottolineato la necessità che gli individui siano alfabetizzati sui nuovi media per impegnarsi con competenza in questo nuovo ambiente.

	Il pericolo più saliente associato alle "fake news" è il fatto che svalutano e delegittimano le voci di competenza, le istituzioni autorevoli e il concetto di dati oggettivi, che minano la capacità della società di impegnarsi in un discorso razionale basato su fatti condivisi. Sono stati rilevati tre danni corollari: in primo luogo, il problema della crescente frammentazione e politicizzazione; in secondo luogo, la promozione di "notizie sicure" a scapito di notizie difficili o impegnative; In terzo luogo, la necessità di fonti credibiliper allocare risorse sempre minori per smascherare informazioni inesatte (che comportano costi sia finanziari che di reputazione).
Pericolo dei social media / strumento negli adulti	Il numero crescente di anziani che stanno rapidamente adottando i social media e diventandovulnerabili alla disinformazione è motivo di particolare preoccupazione. Gli utenti più anziani possono essere particolarmente vulnerabili ai problemi di assorbimento di informazioni false, ma ci sono fattori che hanno un impatto universale su tutte le fasce di età e sulla capacità delle persone di distinguere gliatti dalla finzione. L'età di una persona e la fonte di un contenuto sono importanti quando si analizza la diffusione della disinformazione, ma questi fattori non spiegano perché alcune persone credono ancora alle informazioni false molto tempo dopo essere state presentate con le prove che le correggono. Un'organizzazione di verifica dei fatti ha affermato che ci sono tre fattori che modellano la capacità di tutti di cadere in informazioni false. Il primo è la ripetizione: se un'affermazione errata viene ripetuta più e più volte, diventa più credibile. Il secondo è come appaiono le informazioni. Il rapporto ha rilevato che le dimensioni dei caratteri, la complessità delle parole, il contrasto e la grammatica influiscono su quanto è probabile che qualcuno creda a una falsa affermazione fatta online. Le immagini tendono ad essere più facilmente credute come reali perché creanoun'illusione di prove fattuali di un evento e sono facilmente elaborabili. Il rapporto evidenzia anche i pregiudizi che le persone hanno già prima di consumare informazioni. Le opinioni delle persone influenzeranno il modo in cui le nuove informazioni vengono accettate, anche quando il presidentesa il contrario. Le convinzioni politiche o sociali possono impedire alle persone di accettare informazioni, nonostante i loro livelli di istruzione o alfabetizzazione mediatica. La maggior parte degli anziani ha sentito il termine fake news e sono consapevoli che la diffusione della disinformazione online è un problema. Mentre le persone di tutte le età cadono vittime di notizie false, gli studi hanno dimostrato che gli anziani sono più vulnerabili alle notizie false e alla disinformazione digitale. Uno studio ha dimostrato che gli utenti di Facebook

	di età pari o superiore a 65 anni hanno pubblicato sette volte più articoli da falsi siti Web rispetto agli adulti di età pari o inferiore a 29 anni.1 Gli adulti più anziani hanno anche meno probabilità di essere in grado di individuare la differenza tra annunci pubblicitari progettati per sembrare notizie reali e articoli che sono notizie reali. Furto di profilo: l'account potrebbe essere "rubato", le foto dell'utente potrebbero essere utilizzate altrove o gli hacker potrebbero agire a suo nome.
Soluzioni che possiamo avere	A causa dei problemi sopra citati, un'ampia ricerca tra gli anziani condotta tra il 2009-2019 da Päivi Rasi, Hanna Vuojärvi e Susanna Rivinen ha rivelato che gli interventi dovrebbero essere offerti agli anziani con problemi di salute (Xie, 2011b), agli anziani di età superiore ai 76 anni, agli anziani con meno esperienza con la tecnologia e alle popolazioni minoritarie con bassa h ealth competenze di alfabetizzazione che vivono in diversi paesi (Bertera, 2014; Lee & Kim, 2018; Vaportzis et al., 2017). Inoltre, interventi e servizi dovrebbero essere forniti anche per gli anziani costretti a casa che sono a grande rischio di isolamento sociale (Lee & Kim, 2018). Besides che offre formazione per le persone anziane nell'uso delle tecnologie e dei media digitali (ad esempio, González et al., 2015; Taha et al., 2016; Xie & Bugg, 2009), c'è anche un grande bisogno di sviluppare più strategie per migliorare la fiducia e l'autoefficacia delle persone anzianenel padroneggiare le attività di Internet (Chu & Chu, 2010). Per quanto riguarda la dimensione dell'alfabetizzazione mediatica del "comprendere", gli interventi di alfabetizzazione mediatica dovrebbero mirare all'alfabetizzazione mediatica sanitaria e all'alfabetizzazione sanitaria elettronica delle persone anziane (Manafò & Wong, 2013; Xie, 2012; Young et al., 2012). Le implicazioni pratiche della capacità delle persone anziane di creare contenuti multimediali, in particolare la necessità di prestare attenzione alla capacità delle persone anziane di raccontare storie personali e pubbliche sulla loro vita per sfidare la rappresentazione principaledella loro demografia (Manchester & Facer, 2015). La legge sui servizi digitali della Commissione europea intende affrontare e rendere più sicura la superficie dei fornitori. Tuttavia, ogni cittadino deve fare del suo meglio per sviluppare competenze appropriate perproteggersi dai danni. Thierry Breton, Commissario per il Mercato interno, ha dichiarato: "Dobbiamo tenere a freno l'infodemia e la diffusione di informazioni false che mettono in pericolo la vita delle persone. La disinformazione non può rimanere una fonte di entrate. Abbiamo bisogno di un impegno più forte da parte dellepiattaforme online, dell'intero ecosistema pubblicitario e delle reti di verificatori di fatti. La legge sui servizi digitali ci fornirà ulteriori e potenti strumenti per affrontare la disinformazione". L'alfabetizzazione digitale è qualcosa che può essere insegnata ed è un'abilità che può essere sviluppata. È diventato più importante per gli anziani imparare a distinguere tra disinformazione e notizie reali. Se credi all'argomento secondo cui gli anziani

	hanno più difficoltà a individuare le notizie false rispetto ai gruppi più giovani a causa dell'analfabetismo digitale, neconsegue che questo è un problema che può essere affrontato attraverso l'educazione digitale. L'alfabetizzazione digitale è qualcosa che può essere appreso e migliorato. Un modo per migliorare la tua alfabetizzazione digitale è seguire un corso o partecipare a un webinar sull'alfabetizzazione digitale. Queste organizzazioniinsegnano agli anziani come verificare i fatti e forniscono strumenti e tecniche per valutare i contenuti online. **Quali misure possono adottare gli anziani per evitare di cadere preda di notizie false?** Un anziano ha affermato che "ora mi rendo conto che le notizie false sono molto più complicate e insidiose di quanto pensassi". Le notizie false non sono nuove, però; Finché le parole potevano essere pronunciate o messe su carta con la penna, la disinformazione è stata in circolazione intenzionalmente o erroneamente. Come ha scritto un articolo del Guardian: "L'era della post-verità, in effetti, per quantoti preoccupi di guardare, non c'è mai stata un'età dell'oro della trasparenza". Indipendentemente dal fatto che il concetto di fake news sia nuovo o meno, consumare informazioni soprattutto ora richiede di avere una cassetta degli attrezzi di competenze. Può essere particolarmente utile utilizzare una serie di domande che possono aiutare a valutare nuove informazioni. Quando lavori per determinare se qualcosa è reale, chiediti: Chi ha scritto le informazioni? Quali credenziali ha l'autore dell'articolo? Le informazioni sono aggiornate? Il websitè affidabile? Stanno cercando di venderti un prodotto? Un'azienda o un'organizzazione sponsorizza il sito web? Il sito web supporta punti di vista alternativi o diversi sull'argomento trattato? **Altre strategie pratiche** **Controllare l'origine e il contesto** I siti web sono fonti affidabili o attendibili? "La disinformazione può provenire da più luoghi: non è sufficiente evitare dove pensi che sarà. È meglio avere un filtro attraverso il quale passano tutte le informazioni", controlla i siti web suffixes, ad esempio, per vedere se terminano con .gov o .edu e sono quindi siti web ufficiali del governo o istituzioni educative, rispettivamente. Senior Planet enfatizza anche la comprensione del contesto, come riconoscere la

	satira. È facile confondere un mago divertenteo un articolo scherzoso come reale. **Sii attento anche all'immagine** Cerca angoli sconnessi e / o illuminazione dispari per rilevare se le immagini sono state modificate. Ancora una volta, nota la fonte e il contesto. **Opinioni contro fatti** Comprendi la distinzione tra opinione e fatti, soprattutto perché chiunque può pubblicare contenuti online. "Lettura laterale" - o controllo di altre fonti affidabili per verificare le informazioni mentre leggi - è un termine usato per la prima volta dallo Stanford History Education Group. Domande chiave da porsi mentre lo fai: "Chi c'è dietro le informazioni? Quali sono le prove? Cosa dicono le altre fonti?" Anche le biblioteche possono fornire risorse utili. Le biblioteche potrebbero offrire eventi per conoscere l'alfabetizzazione mediatica – e i bibliotecari sono addestrati a "analizzare le informazioni e tutto il noise ogni giorno", Metti in pausa prima di condividere o reagire online "Metti in pausa, considera e fai più pressione sui clic." Fare in modo che qualcuno si impegni di più con i contenuti click-bait attraverso Mi piace o commenti può essere un modo per i siti Web di generare entrate. Se amici o familiari condividono disinformazione online, offri risorse di verifica dei fatti. Attenzione a bot e troll I bot sono falsi account automatizzati. Identificali individuando nuovi account con pochi follower, nessuna foto, nomi utente strani con molti numeri e commenti senza senso o infiammatori. Bot e troll sono spesso piantagrane online. Che si tratti di bot o meno, pensaci due volte prima di interagire online con qualcuno che non conosci. È necessario o costruttivo farlo?

Nome del social media / strumento	**TRUFFE VIA E-MAIL**
Generalità	L'e-mail è uno dei modi più vantaggiosi per comunicare con chiunque. Ma è anche uno strumento primario utilizzato dagli aggressori per rubare denaro, credenziali di account e informazioni sensibili. Se gli utenti interagiscono con il truffatore di posta elettronica e forniscono informazioni sensibili, ciò può causare problemi a lungo termine, tra cui furto di identità, perdita finanziaria e corruzione dei dati. La frode via e-mail (o truffa via e-mail) è un inganno intenzionale per guadagno personale o per danneggiare un altro individuo tramite e-mail. Non appena l'e-

	mail è diventata ampiamente utilizzata, ha iniziato a essere utilizzata per frodare le persone. La frode via e-mail può assumere la forma di un "gioco della truffa" o truffa. I trucchi di fiducia tendono a sfruttare l'avidità e la disonestà intrinseche delle sue vittime. La prospettiva di un "affare" o di "qualcosa in cambio di niente" può essere moltoallettante. Le frodi via email, come con altri "schemi bunco", di solito prendono di mira individui ingenui che ripongono la loro fiducia in schemi per arricchirsi rapidamente. Questi includono investimenti "troppo belli per essere veri" o offerte per vendere articoli popolari a prezzi "incredibilmente bassi". Molte persone hanno perso i risparmi di una vita a causa di frodi.
Rischio associato ai social media/strumento: **Privacy, accuratezza, proprietà, accessibilità, violazione delle leggi, copyright**	Molte truffe via email esistono da molto tempo. In realtà, alcuni di loro sono semplicemente truffe "riciclate" che precedono l'uso della posta elettronica. **Truffe della LOTTERIA** Ricevi un'e-mail che afferma di aver vinto una lotteria poco conosciuta e sempre con una vincita enorme. Potrebbe anche esserti chiesto di pagare una piccola somma per "liberare" le tue vincite. Ti viene chiestodi inviare tutti i dettagli personali come verifica e improvvisamente sei vittima di una frode di identità e il denaro che hai inviato è sparito. **Offerte di lavoro e false opportunità di business** Queste truffe promettono l'opportunità di fare un sacco di soldi con pochissimo sforzo. Sono normalmentepieni di lusinghe come "Lavora solo ore alla settimana", "Sii il tuo capo", "Imposta le tue ore" e "Lavora da casa". I messaggi di posta elettronica che offrono queste "opportunità" hanno spesso un oggetto simile al seguente:Fare un reddito regolare conOnline; Metti il tuo computer al lavoro per te!: Aste ; Usa Internet per fare soldi; Rivelati i segreti di eBay Insider 6228; Ottieni un clic avanzato Ricevi un'e-mail non richiesta che offre un lavoro, in genere non nella tua area di competenza, spesso per un mystery shopper ouna posizione simile. Quando accetti, vieni pagato tramite assegno o vaglia postale, per un importo superiore a quello offerto dal tuo "datore di lavoro". Ti viene quindi chiesto di restituire la differenza, solo per scoprire che l'assegno originale o l'ordine di pagamento era falso, e sei fuori dai soldi che hai inviato al tuo falso datore di lavoro. Nella maggior parte dei casi, l'e-mail fornisce pochissimi dettagli sulla natura dell'opportunità di business. La maggior parte fornisce un indirizzo o un sito web da cui è possibile, a pagamento, ottenere un "kit informativo" sull'opportunità. Leopportunità se, tuttavia, di solito ammontano a nient'altro che schemi piramidali in cui l'"opportunità" implica la tua capacità di reclutare più persone ignare per acquistare la truffa. Alla fine, la truffa viene scoperta o il pool di nuove reclute si esaurisce e fallisce. **Truffe di frode di beneficenza**

	Dopo disastri naturali su larga scala o tragedie pubbliche di alto profilo, i truffatori cercano di capitalizzare il sentimento pubblico. Hanno creato siti e account di donazione falsi e quindi creano un'e-mail emotiva per sollecitare fondi che non raggiungono mai le vittime. Questetruffe possono avere successo perché giocano sulla simpatia e la buona volontà delle persone! **Truffe sui beneficiari** Ricevi un'e-mail da qualcuno che sta cercando di spostare rapidamente dei soldi. Queste e-mail a volte provengono da persone che affermano di essere un importante imprenditoreo funzionario che dice di avere milioni per trasferirsi fuori dal paese e vuole il tuo aiuto in cambio di un taglio dei profitti. **L'imitatore** Molte truffe imitano le aziende legittime nel tentativo di ingannare i consumatori. Il modo più semplice per evitare questi falsi è quello di non fare mai clic su un link inviato in un'e-mail non richiesta. Trova il link dell'azienda da solo utilizzando un motore di ricerca o, se conosci l'indirizzo dell'annuncio aziendale, digitalo tu stesso. **Truffe di riparazione PC** Una truffa che inizia nel mondo reale e si sposta rapidamente in quello online, si riceve una telefonata da qualcuno che afferma di lavorare per "Microsoft" o un'altra grande società di software che afferma di poter riparare i PC issues come la bassa velocità di Internet. Sembra utile, e così quando l'e-mail arriva nella tua casella di posta, scarichi un programma di accesso remoto, che consente ai truffatori di assumere il controllo del tuo computer. **La "comunicazione ufficiale"** Queste truffe tentano di ingannare i consumatori nel credere diaver ricevuto un'e-mail che richiede loro di intraprendere alcune azioni. Spesso pretendendo di provenire da agenzie governative, queste e-mail ti avvisano di un problema. Questo esempio è stato inviato a maggio, un momento in cui le persone sono più propense a credere che un annuncio provenga dall'IRS. Qui dovresti essere sollevato dal fatto che l'IRS stia riconoscendo di aver ricevuto il tuo pagamento, e quindi essere ansioso che ci sia un problema e fare clic senza pensare. **L'indagine** Queste truffe si basano sul desiderio delle persone di pesare sui problemi ed essere ascoltati sui problemi del giorno. In un anno elettorale un sapore è il sondaggio elettorale, ma qualsiasi argomento caldo andrà bene: riscaldamento globale, atteggiamenti nei confronti della guerra, gestione dell'ultimo disastro naturale e così via. **Truffe sulla salute e sulla dieta**

	Le truffe sulla salute e sulla dieta sfruttano le insicurezze che alcune persone hanno sullo stato del loro benessere. Queste insicurezze rendono alcune persone particolarmente suscettibili alle truffe perché possono essere riluttanti o imbarazzate a discutere i loro problemi con un medico, o non possono afford per acquistare farmaci o trattamenti legittimi. Le truffe tentano di attirare i consumatori con promesse di soluzioni rapide e risultati sorprendenti, prezzi scontati, consegna rapida, requisiti di prescrizione rinunciati, privacy e imballaggio discreto. L'e-mail che offre questi ems avràrighe dell'oggetto simili al seguente:Aumenta drasticamente le tue prestazioni sessuali; CONTROLLA IL TUO PESO!!; Hai bisogno di perdere peso per l'estate?; Rimedio naturale per la salute che funziona!; Ridurre il grasso corporeo e costruire massa muscolare magra senza esercizio; Giovane a qualsiasi età; Toglie anni al tuo aspetto; Dona energia e brucia i grassi; **Email cavallo di** L'e-mail del cavallo di offre la promessa di qualcosa che potrebbe interessarti: un allegato contenente uno scherzo, una fotografia o una patch per una vulnerabilità del software. Una volta aperto, tuttavia, l'allegato può eseguire una o tutte le operazioni seguenti: creare una vulnerabilità di sicurezza sul computer; aprire una "backdoor" segreta per consentire a un utente malintenzionato di accedere illecitamente al tuo computer; installare software che registri le sequenze di tasti e le invii a un utente malintenzionato, consentendo all'utente malintenzionato di scovare le password e altre informazioni importanti; installare software che monitori le transazioni e le attività online; fornire a un utente malintenzionato l'accesso ai file; trasformare il computer in un "bot" che un utente malintenzionato può utilizzare per inviare spam, lanciare attacchi denial-of-service, o diffondere il virus ad altri computer. Le e-mail cavallo di sono arrivate in una varietà di pacchetti nel corso degli anni. Uno dei più noti era il virus "Love Bug", allegato a un'e-mail con oggetto "Ti amo" e che chiedeva al destinatario di visualizzare la "lettera d'amore" allegata. Altre e-mail del cavallo di hanno incluso quanto segue: e-mail che si presentano come cartoline virtuali; Ema; Il mascherato da bollettino sulla sicurezza da un software ve ndor che richiede al destinatario di applicare una "patch" allegata; e-mail con oggetto "divertente" che incoraggia il destinatario a visualizzare lo "scherzo" allegato; e-mail che afferma di provenire da un fornitore di antivirus che incoraggia il destinatario a installare gratuitamente il "virus sweep er" allegato. **E-mail generate da virus** Si noti che, in alcuni casi, un indirizzo "da" familiare non garantisce la sicurezza: molti virus si diffondono cercando prima tutti gli indirizzi e-mail su un computer infetto e poi inviandosi a questi indirizzi. Quindi, se il computer del tuo amico è statoinfettato da un tale virus, potresti ricevere un'e-mail che potrebbe, in effetti, provenire dal computer del tuo amico ma che non è stata effettivamente

	creata dal tuo amico. Se hai dei dubbi, verifica il messaggio con la persona che ritieni essere il mittente prima di aprire qualsiasiallegato di posta elettronica. Si prega di trovare un ampio elenco di diversi tipi di truffe via e-mail al suo link - https://en.wikipedia.org/wiki/Email_fraud
Barriere/difficoltà per gli adulti	Proprio come qualsiasi altro tipo di frode, l'autore può causare un significativoaumento dei danni, specialmente quando la minaccia persiste per un periodo prolungato. La frode via e-mail ha un elenco di effetti negativi , tra cui perdita di denaro, perdita di proprietà intellettuale, danni alla reputazione, a volte con ripercussioni irreparabili. Sebbenele persone anziane raramente riferiscano di essere vittime di crimini informatici finanziari, ci sono prove che gli utenti online più anziani sono a maggior rischio. Una ricerca approfondita ha indagato come, perché e in quali circostanze gli anziani diventano vittime di crimini informatici e ha estrapolato questoper prendere in considerazione strategie di intervento razionali. Secondo la ricerca, isolamento sociale, problemi cognitivi, fisici e di salute mentale; Lo status patrimoniale, le limitate competenze o consapevolezza in materia di cibersicurezza, gli atteggiamenti sociali e il contenuto delle truffe hanno portato alla vittimizzazione. Ha scoperto che la maggior parte degli interventi per migliorare la consapevolezza e le competenze degli utenti di Internet più anziani sono stati tentati fino ad oggi. Altri interventi teoricamente plausibili comprendono: programmi di gestione dei delinquenti, misure di sicurezza su misura, riduzione dello stigma a livello socialee sensibilizzazione dei gruppi che sostengono gli anziani.
Pericolo dei social media / strumento negli adulti	L'atto di truffare gli anziani è un problema enorme in tutto il mondo. Le truffe che iniziano su Internet stanno diventando sempre più frequentianche tra questa popolazione, soprattutto quando le persone esperte di Internet iniziano a invecchiare. I truffatori non discriminano quando si tratta di chi cercano di ottenere denaro: ricchi, poveri, neri, bianchi, 65 e sani, 85 e malati. Cercheranno di prendere soldi da chiunque. La ricerca stima che circa il 5% della popolazione anziana (che equivale a circa due o tre milioni di persone) soffre di una sorta di truffa ogni anno. "Quel che è peggio, è molto probabile che sia una sottostima", Questo è molto probabilmente perché si prevede che unagrande percentuale di truffe su Internet non venga segnalata. Truffare le persone anziane è un business gigantesco che drena gli anziani dei loro fondi pensione e benefici governativi. Sottolinea che le persone anziane perdono circa $ 3 miliardi a causa dei truffatori ognianno.

Stime meno prudenti prevedono che gli anziani perdano fino a $ 36 miliardi ogni anno. È stato anche riferito che l'importo mediano che qualcuno sopra gli 80 anni ha perso era superiore a $ 1.000 e l'importo mediano che qualcuno tra 70 e 79 ha perso era superiore a $ 600.

Perchéi senatori sono vittime di truffe via e-mail? I temi principali

Troppi anziani cadono vittima di truffe, ma non è colpa loro. Questa popolazione è in gran parte affidabile e composta da persone finanziariamente fruttuose la cui cognizione può essere diminuita a causa di vari disturbi. Approfondiamo le caratteristiche e le ragioniper cui gli anziani diventano vulnerabili ai truffatori.

A parte il motivo per cui gli anziani possono essere presi di mira, queste truffe si presentano in varie forme che sfruttano le loro vulnerabilità.

Isolamento

La solitudine può erodere molti aspetti della vita di un anziano, inclusoil fatto che diventi estremamente suscettibile alle truffe. Prima di tutto, quando sono isolati, non c'è nessuno che fornisca un check-in sulle loro finanze. Potrebbe essere troppo tardi per fare qualsiasi cosa se una persona cara lo scopre anni dopo. Gli anziani isolati possono anche essere più vulnerabili all'interazione sociale, che può impostarli per un truffatore desideroso che usa una "relazione" per iniziare il loro schema.

Situazione monetaria

La situazione finanziaria di una persona anziana è una delle ragioni principali per cui diventano bersagli di truffe. Da un lato, una persona anziana potrebbe avere milioni di dollari a portata di mano dopo aver risparmiato per la pensione e aver ottenuto assegni pensionistici mensili e benefici governativi. Ciò può rendere la persona un po 'meno severa con i propri soldi, il che a sua volta rende un'e-mail o un messaggio da un "nipote" che richiede denaro un gioco da ragazzi. D'altra parte, un anziano potrebbe essere finanziariamente insicuro e ha bisogno di una fonte di reddito per arricchirsi rapidamente, rendendo attraente uno schema piramidale senza sapere che non riavranno mai indietro i loro soldi.

Fiducioso

Uncaccordo con le persone di ricerca che sono cresciute negli anni 1920, '30 e '40, a.k.a. Quelli spesso presi di mira per le truffe sono generalmente più fiduciosi delle altre generazioni, il che li rende suscettibili ai truffatori che vogliono trovare le personalità più vulnerabili.

Insicurezza

A volte, gli anziani vengono semplicemente vittime di bullismo nel consegnare denaro ai truffatori. Sia di persona che al telefono, un truffatore potrebbe incessantemente premere una persona anziana per soldi fino a quando non si

	rompono. Inoltre, un truffatore può prendere di mira le insicurezze di una persona anziana come la sua salute o il suo stato sociale, dicendo che devono pagare una certa fattura medica altrimenti non saranno più in grado di ricevere un'assicurazione sanitaria finanziata dal governo. **Cognizione abbassata con l'età** Con l'avanzare dell'età, abbiamo maggiori probabilità di avere qualchetipo di condizione cognitiva del cervello come la demenza, che colpisce la memoria e la funzione cognitiva generale. Queste condizioni cognitive possono influenzare la tua memoria in una miriade di modi, incluso chi è la tua famiglia e quanti soldi hai e cosa è vero o falso. I truffatoriattaccheranno queste debolezze. Ad esempio, un truffatore può chiamare qualcuno di 80 anni fingendo di essere il loro nipote. La persona anziana può ricordare di avere un nipote, ma potrebbe non ricordare i loro veri nomi o come suonano, quindi seguirannoqualsiasi cosa stia dicendo il truffatore. **Imbarazzo** Gli anziani possono semplicemente imbarazzarsi per essere truffati, portandoli a non denunciarlo alle autorità. Questo li rende obiettivi attraenti perché i truffatori sanno che c'è un'alta possibilità che non vengano scoperti per aver cercato (o riuscendoci) a ingannare qualcuno. Inoltre, molte persone anziane non hanno idea di dove segnalare le truffe, il che è purtroppo tanto meglio per i truffatori. Stime meno prudenti prevedono che gli anziani perdano fino a $ 36 miliardiogni anno. È stato anche riferito che l'importo mediano che qualcuno sopra gli 80 anni ha perso era superiore a $ 1.000 e l'importo mediano che qualcuno tra 70 e 79 ha perso era superiore a $ 600.
Soluzioni che possiamo avere	L'e-mail ci fornisce uno strumento di comunicazione comodo e potente. Sfortunatamente, fornisce anche ai truffatori e ad altri individui malintenzionati un mezzo semplice per attirare potenziali vittime. Le truffe che tentano vanno dalle operazioni di esca e interruttore vecchio stile aschemi di phishing che utilizzano una combinazione di e-mail e siti Web fasulli per indurre le vittime a divulgare informazioni sensibili. Per proteggerti da queste truffe, dovresti capire cosa sono, che aspetto hanno, come funzionano e cosa puoi fare per evitarle. I seguenti consigli di base possono ridurre al minimo le possibilità di cadere vittima di una truffa via email: Filtra lo spam. Non fidarti delle email indesiderate. Trattare gli allegati di posta elettronica con cautela. Non fare clic sui collegamenti nei messaggi di posta elettronica. Installa il software antivirus e tienilo aggiornato.

	Installa un firewall personale e tienilo aggiornato. Configurare il client di posta elettronica per la sicurezza. **Cosa puoi fare per evitare di diventare una vittima** **Filtro Spam** Poiché la maggior parte delle truffe via e-mail inizia con e-mail commerciali non richieste, è necessarioadottare misure per impedire allo spam di entrare nella tua casella di posta. La maggior parte delle applicazioni di posta elettronica e dei servizi di posta elettronica Web include funzionalità di filtro della posta indesiderata o modi in cui è possibile configurare le applicazioni di posta elettronica per filtrare la posta indesiderata. Consulta il file di aiuto della tuaapplicazione o servizio ema il per scoprire cosa devi fare per filtrare lo spam. Potresti non essere in grado di eliminare tutto lo spam, ma il filtraggio impedirà a gran parte di esso di raggiungere la tua casella di posta. È necessario essere consapevoli del fatto che gli spammer monitorano gli strumenti di filtraggio dello spam e software e adottano misure per eluderli. Ad esempio, gli spammer possono utilizzare sottili errori di ortografia per sovvertire i filtri antispam, cambiando "Pillole di potenza" in "Pillole di potenza". **Considera le e-mail indesiderate con sospetto** Non fidarti automaticamente delle e-mail che ti vengono inviate da un individuo o un'organizzazione sconosciuti. Non aprire mai un allegato a e-mail indesiderate. Ancora più importante, non fare mai clic su un link inviato in un'e-mail. I collegamenti abilmente realizzati possono portarti a siti Web contraffatticreati per indurti a divulgare informazioni private o scaricare virus, spyware e altri software dannosi. Gli spammer possono anche utilizzare una tecnica in cui inviano link univoci in ogni singola e-mail di spam. La vittima 1 può ricevere un'e-mail con il link <http://dfnasdunf.example.org/> e la vittima 2 può ricevere la stessa e-mail di spam con il link <http://vnbnnasd.exaple.org/>. Osservando quali link sono richiesti sui loro server web, gli spammer possono capire quali indirizzi e-mail sono validi e indirizzare più efficacementele vittime per ripetuti tentativi di spam. Ricorda che anche le e-mail inviate da un indirizzo familiare possono creare problemi: molti virus si diffondono scansionando il computer vittima alla ricerca di indirizzi e-mail e inviandosi a questi indirizzi sotto forma di e-mail dal proprietario del computer infetto.

Trattare gli allegati e-mail con cautela

Gli allegati e-mail sono comunemente usati dai truffatori online per intrufolarsi un virus sul tuo computer. Questi virus possono aiutare il truffatore a rubare informazioni importanti dal tuo computer, compromettere il tuo computerin modo che sia aperto a ulteriori attacchi e abusi e convertire il tuo computer in un "bot" da utilizzare in attacchi denial-of-service e altri crimini online. Come notato sopra, un indirizzo "da" familiare non è garanzia di sicurezzaperché alcuni virus si diffondono prima cercando tutti gli indirizzi e-mail su un computer infetto e poi inviandosi a questi indirizzi. È possibile che il computer del tuo amico sia infetto da un virus del genere.

Usa il buon senso

Quando arriva un'e-mailnella tua casella di posta che ti promette un sacco di soldi per poco sforzo, ti accusa di violare il Patriot Act o ti invita a unirti a un complotto per accaparrarti fondi non reclamati che coinvolgono persone che non conosci in un paese dall'altra parte del mondo, prenditi un momento per considerarela probabilità che l'e-mail sia legittima.

Installa il software antivirus e tienilo aggiornato

Se non l'hai ancora fatto, dovresti installare un software antivirus sul tuo computer. Se possibile, è necessario installare un programma antivirus dotato di unafunzione di aggiornamento automatico. Ciò contribuirà a garantire sempre la protezione più aggiornata possibile contro i virus. Inoltre, dovresti assicurarti che il software antivirus che scegli includa una funzione di scansione della posta elettronica. Ciò contribuirà a mantenere il computer privo di virus trasmessi tramite e-mail.

Installare un Personal Firewall e mantenerlo aggiornato

Un firewall non impedirà alle e-mail truffa di farsi strada nella tua casella di posta. Tuttavia, può aiutare a proteggerti se apri inavvertitamente un allegato contenente virus o introduci malwaresul tuo computer seguendo le istruzioni contenute nell'e-mail. Il firewall, tra le altre cose, aiuterà a prevenire il traffico in uscita dal computer all'utente malintenzionato. Quando il firewall personale rileva comunicazioni sospette in uscitadal computer, potrebbe essere un segno che hai inavvertitamente installato programmi dannosi sul tuo computer.

Scopri le politiche e-mail delle organizzazioni con cui fai affari

La maggior parte delle organizzazioni che fanno affari online ora hanno politiche chiare su comecomunicare con i propri clienti tramite e-mail. Molti, ad esempio, non ti chiederanno di fornire informazioni sull'account o personali via e-mail. Comprendere le politiche delle organizzazioni con cui fai affari può aiutarti a

	individuare ed evitare phishing e altre truffe. Tieni presente, tuttavia, che non è mai una buona idea inviare informazioni sensibili tramite e-mail non crittografate. **Configurare il client di posta elettronica per la sicurezza** Esistono diversi modi per configurare il client di posta elettronica per renderti meno suscettibile alle truffe via email. Ad esempio, la configurazione del programma di posta elettronica per visualizzare l'e-mail come "solo testo" ti aiuterà a proteggerti dalle truffe che usano impropriamente HTML nelle e-mail. **Altri modi per proteggersi dalle truffe via email** La prevenzione, attraverso la consapevolezza, è uno strumento vitale nella lotta contro i truffatori. Ci sono alcuni consigli utili per aiutarti a evitare di essere truffato al telefono, online, per posta o a portata di mano. Ci sono alcuni t ip generaliper proteggersi dal diventare vittima di una truffa. Non fornire mai informazioni personali. Questo può essere utilizzato per rubare la tua identità e accedere agli account. Controlla sempre le credenziali di qualsiasi azienda o professionista legale di cui non sei sicuro. Puoi cercarli su Companies House(link esterno si apre in una nuova finestra / scheda) per scoprire il loro background o cercare recensioni online. Non effettuare pagamenti anticipati fino a quando non sei sicuro che l'azienda con cui hai a che fare sia legittima. Evita di essere aggiunto allemailing list di cui i truffatori a volte entrano in possesso. **Indizi per individuare le e-mail truffa** I truffatori stanno diventando sempre più scaltri nel falsificare e-mail e messaggi falsi, in diverse lingue. È sempre importante cercare segni di una contraffazione, come ad esempio: Generico Greetings Scarsa qualità della grammatica, del vocabolario Possibili errori di ortografia Progettazione imperfetta di elementi grafici **Poni queste domande** Perché vengo contattato?

	Questa cosa è troppo bella o troppo cattiva per essere vera? So davvero chi è il mio amore online? Ho mai incontrato il mio amore online? Sono mai stato in una connessione telefonica o video con lui? Mi chiede ripetutamente soldi, citando possibili spese di viaggio, acquisti di passaporti o varie cose drammatiche e altre storie? **TEST DI TRUFFA - Utilizzali per i passaggi per scansionare le tue e-mail** Sembra troppo bello per essere vero Contattato all'improvviso Richiesta di dati personali Il denaro è richiesto RICORDA: istituzioni finanziarie, società di servizi, forze dell'ordine, enti governativi, fornitori di servizi Internet etelematici o altri enti pubblici: Non chiederà MAI il pagamento in voucher. Non ti chiederà MAI di trasferire denaro perché il tuo account è compromesso. Non ti minaccerà MAI al telefono, per lettera o e-mail per non aver pagato una tassa. Non minaccerà MAI arrest se il pagamento non viene effettuato immediatamente. Non chiederà MAI soldi per un "regalo gratuito", una "commissione amministrativa" o come parte di una promozione. Non ti chiederà MAI di rivelare i codici di sicurezza del tuo account o le password online per intero. Non chiamerà MAI di punto in bianco e chiederà un accesso remotoal tuo computer o dispositivi o per scaricare software. Non ti informerà MAI sulle dichiarazioni dei redditi via e-mail, SMS o posta vocale.

Nome del social media / strumento	**PHISHING**
Generalità	Le truffe rivolte agli anziani sono un business molto grande che deruba gli anziani dei loro risparmi guadagnati duramente, dei fondi pensione e persino dei benefici governativi. I danni possono essere devastanti. Mentre ci sono molti metodi che i criminali informatici usano per frodare gli anziani, phishing è una delle truffe più antiche e conosciute di Internet. Il phishing è un tipo di bufala su Internet in cui i truffatori utilizzano e-mail e altri metodi per rubare informazioni personali, come dettagli finanziari o password di account. Questo approccio ha guadagnato il suo

	nome insolito perché utilizza "esca" attraente per attirare le persone sui siti Web e sollecitare i loro dati con falsi pretesti. Il phishing non è la stessa cosa dello spam. Mentre lo spam è solo un altro termine per posta indesiderata e annunci indesiderati, gli attacchi di phishing sono tentativi deliberati di sottrarrele tue informazioni e utilizzarle in modi dannosi. Le truffe di phishing via e-mail vengono eseguite online da truffatori esperti di tecnologia e criminali di furti di identità. Usano spam, siti Web falsi costruiti per sembrare identici ai siti reali, e-mail e messaggi istantanei perconvincerti a divulgare informazioni sensibili, come password di conti bancari e numeri di carte di credito. Una volta abboccata al phisher, possono utilizzare le informazioni per creare account falsi a tuo nome, rovinare il tuo credito e rubare i tuoi soldi o persino la tua identità.
Rischio associato ai social media/strumento: **Privacy, accuratezza, proprietà, accessibilità, violazione delle leggi, copyright**	Esistono tre componenti principali per una truffa di phishing: (1) L'attacco è condotto tramite comunicazioni elettroniche. Sebbene l'e-mail sia comune, il phishing può anche essere effettuato tramite messaggi di testo, account di social media, messaggi vocali e persino telefonate. (2) Tutte le forme di phishing mirano a convincerti che una comunicazione falsaè reale e credibile. L'utente malintenzionato afferma di essere un individuo o un'organizzazione familiare e affidabile per te. (3) L'obiettivo di un attacco di phishing è ottenere informazioni personali sensibili, come credenziali di accesso, dettagli bancari o numeri di carta di credito. Con tutti gli attacchi di phishing, il truffatore offre una presentazione attentamente elaborata volta a farti fare clic su un collegamento, scaricare un allegato o fornire informazioni personali specifiche. Alcuni esempi comuni di attacchi di phishing includono: **Una richiesta di aiuto:** con un goaldi tirare le corde del tuo cuore, l'aggressore ti invia un'e-mail fingendo di essere un buon amico o parente (ad esempio, tuo nipote). Affermano di essere in difficoltà finanziarie e richiedono immediatamente la tua assistenza. In che modo i criminali informatici sono in grado di colpirepersone che conosci? Con i social media, i truffatori hanno accesso a più informazioni personali che mai. Ciò consente loro di rendere i loro messaggi altamente mirati e spesso molto credibili. **Sei il vincitore del primo premio:** ricevi un messaggio che si congratula con te per essere il vincitore di un premio molto grande, che si tratti di un pacchetto di viaggio irresistibile o di biglietti gratuiti per l'evento dell'anno. Ti viene chiesto di fornire i tuoi dati personali per richiedere il premio. **Il tuo conto bancario è stato compromesso:** ricevi un avviso "urgente" che sembra provenire dalla tua banca, che ti avvisa di attività sospette sul tuo account. Ti viene

quindi chiesto di fare clic su un collegamento che ti porta a un sito Web, dove ti verrà richiesto di confermare l'informazione sul tuo conto bancario.

Il governo ti sta cercando: poche cose nella vita sono così stridenti come un avviso formulato autorevolmente da un'organizzazione governativa. I truffatori lo sanno, motivo per cui molte e-mail di phishing sembrano provenire dal governo. Un'e-mail come questa in genere ha un tono minaccioso e menziona sanzioni grandi e spaventose, a meno che tu non fornisca il pagamento o i dati personali richiesti.

Questi tipi di attacchi di phishing hanno anche un rovescio della medaglia. In alcuni casi, vengono inviati durante la stagione fiscale, offrendoti un generoso rimborso dopoaver confermato i tuoi dati finanziari.

Perché il phishing funziona così bene?

Le e-mail, i messaggi di testo, i messaggi vocali e persino le chiamate vocali non vengono autenticati. Ciò significa che, proprio come una cartolina inviata per posta, non c'è un vero modo per convalidare da dove provengono. Ciò offre ai truffatori molta libertà di imitare marchi affidabili nelle loro comunicazioni. Il phishing è una delle minacce più comuni e pervasive.

I phisher sofisticati sono molto abili nella creazione di modelli di e-mail e siti Web falsi chesono quasi indistinguibili dalla realtà, fino all'URL (indirizzo del sito Web) e ai certificati di sicurezza. Potresti pensare di ricevere un messaggio credibile da una banca, un negozio online o una società di carte di credito. E se non stai prestando molta attenzione, potresti non notare l'inganno fino a quando non è troppo tardi.

Tipi di phishing che devi sapere per stare al sicuro

Il phishing viene in genere effettuato tramite spoofing di e-mail, messaggistica istantanea e messaggi di testo. È un modo ingannevole di far sì che le persone rivelino informazioni personali. È anche una forma di inganno per scaricare malware o ransomware su un sistema. In entrambi i casi, l'autore ottiene un accesso privilegiato alle informazioni sensibili. Questa è una minaccia sempre più frustrante perché ci sono numerosi modi attraverso i quali i perpetratori attaccano.

Il phishing si è evoluto per diventare qualsiasi cosa i criminali informatici abbiano bisogno che sia per rubare letue credenziali. I loro metodi ora assumono molte forme e se non hai familiarità con termini come smishing, vishing, pharming e BEC, ecco una guida:

STANDARD PHISHING

	Casting a Wide Net - Nella sua forma più elementare, il phishing standard è il tentativo di rubareinformazioni confidenziali fingendo di essere una persona o un'organizzazione autorizzata. Non è un attacco mirato e può essere condotto in massa. **PHISHINGING VIA E-MAIL** Lo scenario di phishing più comune assume la forma di e-mail dannose inviate a individui che imitanoun'organizzazione automatica. Conosciuto anche come spam phishing, questo tipo di attacco consente al criminale informatico di accedere a un gran numero di clienti registrati su un sito. Quindi le e-mail di phishing vengono spesso inviate in massa. C'è un'alta possibilità di successo, poiché alcuni individuifuori dal lotto cadranno spesso preda (9). **MALWARE PHISHING** Attenzione alle macro Utilizzando le stesse tecniche, questo tipo di phishing introduce bug sgradevoli convincendo un utente a fare clic su un collegamento o scaricare un allegato Quindi il malware può essere installato su una macchina. Attualmente è la forma più utilizzata di attacco di phishing. **PHISHING DI SEAR** Catturare il Big One - Dove la maggior parte degli attacchi di phishing getta un'ampia rete, sperando di invogliare il maggior numero possibile di utenti ad abboccare, lo spear phishing comporta una ricerca approfondita di unobiettivo predefinito e ad alto costo, spesso basandosi su informazioni disponibili pubblicamente per uno stratagemma più convincente. Ciò implica anche una tecnica in cui il phisher si rivolge a un individuo o un gruppo specifico di individui piuttosto che a una base di utenti generica. Questi attacchi hanno successo proprio perché sono più personalizzati. L'autore personalizza le e-mail con il nome, l'azienda, il numero di telefono e informazioni simili del destinatario, facendo credere al bersaglio di condividere una qualche forma di connessione con il mittente. Ottenere e-mail di spear-phishing convincenti richiede molto tempo poiché il phisher deve acquisire più dati davarie fonti. Non c'è da meravigliarsi quindi che questo tipo di attacco dannoso sia prevalente su piattaforme di social media come LinkedIn, dove il phisher può utilizzare tattiche di ingegneria sociale. **SMS + PHISHING = SMISHING** Just Don't Click - Il phishing abilitato agli SMSutilizza i messaggi di testo come metodo per fornire collegamenti dannosi, spesso sotto forma di codici brevi, per intrappolare gli utenti di smartphone nelle loro truffe. L'avvento della tecnologia

	mobile ha portato una miriade di vantaggi nella comunicazione e nell'online banking. Al momento giusto, ha aperto un nuovo punto di contatto per individui senza scrupoli per commettere più crimini. Uno di questi è lo smishing, in cui i criminali informatici attirano le vittime tramite messaggi di testo a: Visita siti web canaglia Scarica app dannose Contatta il supporto tecnico Che si tratti di un codice coupon o di un'offerta per vincere biglietti gratuiti o denaro gratuito, un tentativo di smishing richiederà il più delle volte di fare clic su un collegamento che ti reindirizza a un sito web. Abbastanza comuni sono anche i link che attivano il download automatico di app pericolose. Sebbene sembrino provenire da fonti legittime con URL a te familiari, mirano semplicemente a rubare informazioni personali o installare malware sul tuo dispositivo mobile. **PHISHING SUI MOTORI DI RICERCA** Eseguiciò che scegli - In questo tipo di attacco, i criminali informatici aspettano che tu venga da loro. Il phishing dei motori di ricerca inserisce siti fraudolenti, spesso sotto forma di annunci a pagamento, nei risultati dei termini di ricerca più diffusi. **VISHING** Tenerti in linea - Vishing coinvolge unattore fraudolento che chiama una vittima fingendo di provenire da un'organizzazione rispettabile e cercando di estrarre informazioni personali, come informazioni bancarie o sulla carta di credito. Molto spesso, il "chiamante" sull'altra linea suona ovviamente come un robot, ma con l'avanzare della tecnologia, questa tattica è diventata più difficile da identificare. **PHARMING - Avvelenare la pozza d'acqua** Conosciuto anche come avvelenamento DNS, il pharming è una forma tecnicamente sofisticata di phishing che coinvolge il sistema dei nomi di dominio (DNS) di Internet. Pharming reindirizza il traffico web legittimo verso una pagina falsificata all'insaputa dell'utente, spesso per rubare informazioni preziose. All'apertura del sito Web, del collegamento o dell'allegato dannoso, il computer viene automaticamente caricato con malware che si diffonde ad altri sistemi all'interno dell'azienda. Per perpetuare attacchi watering hole di successo, l'hacker identificherà spesso i siti Web che visiti regolarmente e monitorerà i modelli di posta elettronica. Con il pharming, il perpetratore non attacca gli individui. Piuttosto, l'attacco è diretto alDNS (Domain Name System), dove il truffatore provoca l'avvelenamento della cache DNS. Ciò modifica l'indirizzo IP associato al nome di un sito Web, quindi anche quando le persone inseriscono il nome del sito corretto, il truffatore può comunque reindirizzare gli utenti al sito Web dannoso.

	Anche semeno diffuso, il targeting del server DNS potrebbe compromettere milioni di richieste URL da parte degli utenti web. **CLONE PHISHING** In questo tipo di attacco, un losco attore apporta modifiche a un'e-mail esistente, risultando in un'e-mail quasi identica (clonata) ma con uncollegamento legittimo, un allegato o un altro elemento scambiato con uno dannoso. Questi attacchi non possono decollare senza prima un attaccante compromettere un account di posta elettronica, quindi una buona difesa è l'utilizzo di password forti e uniche abbinate all'autenticazione a due fattori. **MAN-IN-THE-MIDDLE** The Public WiFi Phisherman - Un attacco man-in-the-middle coinvolge una corrispondenza di monitoraggio delle intercettazioni tra due parti ignare. Quando questo viene fatto per rubare credenziali o altre informazioni sensibili, diventa un attacco di phishing man-in-the-middle. Questi attacchi vengono spesso effettuati creando reti WiFi pubbliche fasulle in bar, centri commerciali e altri luoghi pubblici. Una volta iscritto, l'uomo nel mezzo può phishing per informazioni o inviare malware sui dispositivi **MALVERTISINAG** Quell'annuncio non è quello che pensi che sia - Questo tipo di phishing sfrutta gli exploit all'interno di software pubblicitari o di animazione per rubare informazioni da utenti mirati. Il malvertising è solitamente incorporato in annunci dall'aspetto normale e inserito susiti Web legittimi come Yahoo.com, ma con codice dannoso impiantato all'interno. **SPOOFING DI DOMINI** Il secondo tipo di phishing via e-mail si presenta sotto forma di spoofing del dominio, in cui l'autore falsifica il nome di dominio di un'organizzazione notevole. Questa tecnica rende l'orecchio dell'appcome se si ricevesse un'e-mail da un'azienda legittima. Gli indirizzi e-mail sono univoci, quindi il phisher può solo imitare l'indirizzo dell'organizzazione. Lo fanno usando la sostituzione dei caratteri come "r" e "n" insieme per "rn" invece di "m". Altrimenti, usail nome dell'organizzazione con un dominio diverso, nella speranza che solo la parte locale dell'indirizzo e-mail appaia nella posta in arrivo del destinatario. Uno spoofing di dominio potrebbe anche creare un sito Web fraudolento che assomiglia al vero affare. Avrebbero resoesplicati il design del sito reale. Ancora una volta, l'enfasi è sulla frase "sembra". Mentre il dominio falso può essere simile, non è identico al sito web originale. **GEMELLO MALVAGIO** I punti di accesso WI-FI sono frequentati da orde di persone alla ricerca di connessioni wireless veloci per navigare sul web e svolgere altre attività basate su

Internet. L'hacker in questo scenario replica l'hotspot WI-FI con un falso. Quando gli utenti si connettono, sono quindi in grado di intercettare il loro traffico di rete. L'utente malintenzionato ruba nomi account e password. Il phisher è anche in grado di visualizzare tutti gli allegati a cui l'utente accede mentre si trova sulla rete compromessa. I punti di accesso WI-FI vulnerabili includono quelli di bar, aeroporti, centri commerciali, ospedali e altri punti di riferimento pubblici.

Esempi reali di attacchi di phishing

Secondo una recente ricerca di Google, c'è stato un aumento di 3505 siti Web di phishing da gennaio a marzo 2020. Un altro sondaggio di Check Point Research ha rivelato che il 64% delle aziende nell'ultimo anno è stato vittima di attacchi di phishing. Ulteriori risultati di Verizon hanno confermato che il phishing è coinvolto nel 78% degli incidenti di spionaggio informatico. Questi sono cinque degli esempi più importanti:

L'attacco alla caccia alle balene porta al licenziamento del boss della FACC

Nel 2016, la società aerospaziale austriaca FACC era stata oggetto di uno dei più importanti attacchi balenieri di sempre, soprannominato Fake President Incident, in cui l'aggressore ha portato via $ 56 milioni. In un classico attacco di whaling, l'autore si è spacciato per il CEO e l'invio di un'e-mail a un dipendente del dipartimento finanziario ha richiesto un trasferimento immediato di fondi.

L'attacco non è costato solo perdite finanziarie all'azienda, ma è anche costato la sua posizione al CEO dell'epoca, Walter Steph. Sebbene i dettagli non siano stati rivelati, il sacco era per violazione dei doveri.

Spear Phishing mirato a Ubiquiti Networks Inc.

Nel giugno del 2015, la società americana di tecnologia di rete Ubiquiti Networks è diventata l'obiettivo di una campagna e-mail di pesca subacquea. L'aggressore ha impersonato dirigenti di alto rango di una filiale estera con indirizzi e-mail falsificati e sosia del dominio. I dipendenti sono stati ingannati nel credere di ricevere richieste legittime daparte dei funzionari della società di trasferire fondi su un conto sicuro. Ubiquiti Networks non era a conoscenza di essere stata truffata fino a quando non è stata informata dell'attività dall'FBI. Non ha subito alcun compromesso per i suoi sistemi, ha perso $ 46,7 milioni in fondi trasferiti.

Truffa delle fatture di Facebook e Google

Tra il 2013 e il 2015, le società colossi statunitensi Facebook e Google sono state truffate da $ 100 milioni in un elaborato schema di frode telematica. L'autore ha creato una falsa attività impersonando la società taiwanese Quanta Computer. Quest'ultimo ha condotto regolarmente transazioni multimilionarie con le società di social media e, nel corso dei due anni, l'attaccante avrebbe inviato e-mail di phishing con fatture false da pagare su falsi conti bancari. Lo schema ha evitato il sospetto per così tanto tempo creandodocumenti giustificativi fasulli per le transazioni e sigilli aziendali falsi. L'aggressore è stato successivamente identificato

	come il lituano Evaldas Rimasauskas, che è stato condannato a cinque anni di carcere dopo il suo arresto nel 2017. **Apple Smishing** Nel 2020, una delle più grandi aziende di smartphone al mondo, Apple, è stata segnalata per essere stata l'obiettivo di una campagna di smishing. Con una falsa chat Apple, i messaggi informavano gli utenti di aver vinto la possibilità di far parte del programma di test 2020 di Appleper il nuovo iPhone 12. Ai destinatari è stato richiesto di pagare una tassa di consegna. Reindirizzando a un sito Web dannoso, gli aggressori hanno dirottato le credenziali della carta di pagamento delle vittime. Le persone al giorno d'oggi conservano molte informazioni sensibili sui loro smartphone e l'uso diffuso di iPhone e iPad li ha resi obiettivi ricorrenti per gli schemi di phishing via SMS. Gli aggressori inviano regolarmente messaggi agli utenti. Questi messaggi conterranno un link da seguire per sbloccare un account ID Apple congelato o per evitare che scada damessaggi futuri del tipo. Altri escheranno gli utenti con l'idea che sia stato trovato un iPhone perso. Le vittime vengono ingannate dalle loro credenziali di accesso e gli hacker ottengono l'accesso ai loro media, documenti e altre informazioni memorizzate sul dispositivo. Come minaccia continua, l'importo perso durante i tentativi riusciti si aggiunge alle statistiche per le perdite annuali di criminalità informatica. Anche se non tutti cadono vittima, l'aggressore guadagna ricompense significative per la piccola percentuale di persone che non erano più sagge. **Violazione della sicurezza RSA** Tutto ciò che serviva a un utente malintenzionato per ottenere l'accesso al sistema di rete della popolare società di sicurezza informatica era un'e-mail con oggetto "Piano di reclutamento 2011". Nell'e-mail c'era un file Excel infetto da virus e, una volta aperto da un dipendente sconosciuto,ha dato all'attaccante l'accesso a password private. Rendendo questo un perfetto esempio di un attacco di phishing watering hole. Ironia della sorte, la RSA fornisce servizi di sicurezza informatica a diversi rami del governo degli Stati Uniti e ad altre imprese commerciali. Questo brha dato agli hacker l'accesso alle reti dei dipartimenti governativi degli Stati Uniti, diventando una minaccia persistente avanzata. Guarda questo video https://www.youtube.com/watch?v=4AcROYO8BLA
Barriere/difficoltà per gli adulti	Le e-mail, i messaggi di testo, i messaggi vocali e persino le chiamate vocali non vengono autenticati. Ciò significa che, proprio come una cartolina inviata per posta, non c'è un vero modo per convalidare da dove provengono. Ciò offre ai

	truffatori molta libertà di imitare marchi affidabili nelle loro comunicazioni. Il phishing è una delle minacce più comuni e pervasive. I phisher sofisticati sono molto abili nella creazione di modelli di e-mail e siti Web falsi che sono quasi indistinguibili dalla realtà, fino all'URL (indirizzo del sito Web) e ai certificati di sicurezza. Potresti pensare di ricevere un messaggio credibile da una banca, un negozio online o una società di carte di credito. E se non stai prestando molta attenzione, potresti non notare l'inganno fino a quando non è troppo tardi.
Pericolo deisocial media/strumento negli adulti	Secondo Wikipedia, il phishing è un tentativo fraudolento di ottenere dati sensibili impersonandosi come entità affidabile. Proprio come qualsiasi altro tipo di frode, l'autore può causare una quantità significativa di danni, specialmente quando la minaccia persiste per un periodo prolungato. 11 Proprio come qualsiasi altro tipo di frode, l'autore può causare una quantità significativa di danni, specialmente quando la minaccia persiste per un periodo prolungato. Le frodi via e-mail contengono un elenco di effetti negativi,tra cui perdita di denaro, perdita di proprietà intellettuale, danni alla reputazione, talvolta con ripercussioni irreparabili. Sebbene le persone anziane raramente riferiscano di essere vittime di crimini informatici finanziari, vi sono prove che gli utenti online più anziani sono a rischiocrescente. Secondo la ricerca, isolamento sociale, problemi cognitivi, fisici e di salute mentale; Lo status di ricchezza, le limitate competenze o consapevolezza della sicurezza informatica, gli atteggiamenti sociali e il contenuto delle truffe hanno portato alla vittimizzazione. La perdita finanziaria per i bambini più anziani è stata quasi il doppio per truffa rispetto alle vittime più giovaniTuttavia, è importante notare che la perdita finanziaria per le vittime più anziane (quelle di età pari o superiore a 55 anni) era probabilmente quasi il doppio per truffa rispetto a quella per i gruppi di età più giovani. Inoltre, si può supporre che, per molte persone anziane con un reddito fisso (e nessun mezzo facile per costruire nuovi risparmi, ad esempio), è probabile che sia più difficile per loro sostituire il denaro perso a causa di frodi rispetto alle persone in età lavorativa. Quasi la metà (4-9%) di tutte le persone di età pari o superiore a 75 anni vive da sola; e il 17% delle persone anziane ha meno contatti settimanali con familiari, amici e vicini. Le persone socialmente più isolate possono essere più vulnerabili alle frodi, ad esempio, se hanno lapossibilità di discutere con gli altri. **In che modo gli anziani cadono preda del phishing?** L'atto di truffare gli anziani è un problema enorme in tutto il mondo. Le truffe che iniziano su Internet stanno diventando sempre più frequenti anche tra questa

	popolazione, soprattutto quando le persone esperte di Internet iniziano a invecchiare. **Se hai risposto a un tentativo di phishing, l'utente malintenzionato può:** Dirottare i tuoi nomi utente e password Ruba i tuoi soldi e apri carte di credito e conti bancari a tuo nome Richiedi un nuovo account Numeri di identificazione personale (PIN) o carte di credito aggiuntive Effettuare acquisti Aggiungi se stessi o un alias che controllano come utente autorizzato in modo che sia più facile vedereil tuo credito Ottenere anticipi di cassa Usa e abusa del tuo numero di previdenza sociale Vendere le tue informazioni ad altre parti che le utilizzeranno per scopi illeciti o illegali Come mi ha trovato una truffa di phishing? Questo stile di furto di identità è estremamente diffuso acausa della facilità con cui persone ignare condividono informazioni personali. Le truffe di phishing spesso ti attirano con e-mail di spam e messaggi istantanei che ti chiedono di "verificare il tuo account" o "confermare il tuo indirizzo di fatturazione" attraverso quello che è in realtà un sito Web dannoso . Sii molto cauto. I phisher possono trovarti solo se rispondi. **Come faccio a sapere se sono stato vittima di phishing?** I phisher spesso fingono di essere aziende legittime. I loro messaggi possono sembrare genuini e i loro siti possono assomigliare notevolmente alla realtà. Può essere difficile capire la differenza, ma potresti avere a che fare con una truffa di phishing se vedi quanto segue: Richieste di informazioni riservate via e-mail o messaggio istantaneo Linguaggio emotivo che utilizza tattiche intimidatorie o richieste urgenti per rispondere URL errati,errori specifici o uso di sottodomini Collegamenti all'interno del corpo di un messaggio Mancanza di un saluto personale o di informazioni personalizzate all'interno di un messaggio. Le e-mail legittime provenienti da banche e società di carte di credito spesso includono numeri di conto, nome utente o password parziali. **Impatti** **Perdita di denaro** Da ogni incidente di phishing che abbia mai avuto luogo nella storia, un effetto costante è la perdita finanziaria. Le perdite finanziarie subite dai singoli consumatori sono stimate in oltre 9 miliardi di sterline all'anno.

	Tuttavia, sebbene queste cifre siano utili indicative,è probabile che sottovalutino significativamente l'entità delle perdite finanziarie subite dai singoli individui, in quanto non sembra che includano tutti i tipi di frode e, come indicato, molti reati di frode non vengono denunciati. In modo confuso, la cifra di 3,5 miliardi di sterlineviene spesso indicata come una stima delle perdite finanziarie totali subite dalle persone a causa di frodi o truffe. **Altri impatti** In generale, gli altri effetti della frode per le vittime possono variare a seconda delle circostanze individuali e dellerisorse e delle capacità esistenti, ma la gravità dell'impatto potenziale non dovrebbe mai essere sottovalutata. Gli effetti psicologici possono essere gravi e debilitante, tra cui stress, rabbia, perdita di autostima, vergogna e turbamento. L'impatto negativo dell'abuso finanziario, indipendentemente dalla fonte, può portare qualcuno ad aver bisogno di sostegno da parte dei servizi sociali, non avendo precedentemente richiesto tale aiuto. Uno studio sui reati a domicilio ha dimostrato che la salute delle vittime diminuisce più rapidamente rispetto alle non vittime di età simile L'analisi degli effetti della criminalità porta a domicilio ha rilevato che: Il 40% delle vittime ha dichiarato che ciò ha comportato una riduzione della fiducia in generale. Il 28% hadichiarato che li ha lasciati giù o depressi. Il 46% ha dichiarato di aver causato loro un danno finanziario. Il 16% non aveva detto a nessuno del crimine e il 40% di questi ha dichiarato che il motivo era l'imbarazzo. Le vittime sono spesso persone vulnerabiliche possono trovarsi in difficoltà finanziarie o essere anziane o socialmente isolate. L'impatto personale su di loro e sulle loro famiglie è spesso devastante in termini di tranquillità e salute futura. Le vittime possono essere lasciate con un'autostima danneggiata e un ridotto senso di valore elfo. Le vittime soffrono di stress, ansia e depressione. Le vite possono essere rovinate". Quasi la metà (49%) di tutte le persone di età pari o superiore a 75 anni vive da sola; e il 17% delle persone anziane ha contatti meno di settimanali con familiari, amici e vicini. Le persone che sono più socialmente isolate possono essere più vulnerabili alle frodi, ad esempio, se hanno poche possibilità di discutere le questioni con gli altri. In che modo gli anziani cadono preda del phishing?
Soluzioni che possiamo avere	La migliore difesa contro una truffa di phishing è verificare con la persona o le organizzazioni che hanno inviato l'e-mail o il messaggio prima di fare clic su qualsiasi cosa.

	Come proteggersi dal phishing? Quando ti armi di informazioni e risorse, sei più saggio sulle minacce alla sicurezza informatica e seivulnerabile alle tattiche di truffa del phishing. Segui questi passaggi per rafforzare la sicurezza del tuo computer e ottenere subito una migliore protezione dal phishing: Non fornire informazioni personali a richieste di informazioni non richieste Fornire informazioni personali solo su siti che hanno "https" nell'indirizzo web o hanno un'icona a forma di lucchetto nella parte inferiore del browser Se sospetti di aver ricevuto un'esca di phishing, contatta telefonicamente la società oggetto dell'e-mail per verificare che il messaggio sia legittimo Digitare un URL attendibile per il sito di un'azienda nella barra degli indirizzi del browser per ignorare il collegamento in un sospetto messaggio di phishing Usa password varie e complesse per tutti i tuoi account Controlla continuamente l'accuratezza dei conti personali e affronta immediatamente eventuali discrepanze Evita siti web discutibili Pratica il protocollo di posta elettronica sicuro: Non aprire messaggi provenienti da mittenti sconosciuti Elimina immediatamente i messaggi che sospetti essere spam **Assicurati di avere i migliori prodotti software di sicurezza installati sul tuo PC per una migliore protezione dal phishing:** Utilizzare la protezione del software antivirus e un firewall Ottieni protezione software antispyware Un computer non protetto è come una porta aperta per le truffe di phishing via email. Per una forma di protezione più potente, utilizzare un filtro antispam o un gateway per analizzare i messaggi in ingresso. Questi prodotti contrastano il malware pericoloso prima che possa entrare nel tuo PC, fanno la guardia ad ogni possibile ingresso del tuo computer e respingono eventuali spyware o virus che tentano di entrare, anche i ceppi più dannosi e subdoli. Sebbene siano disponibili download gratuiti di anti-spyware e antivirus, non riescono a tenere il passo con il continuo assalto di nuovi ceppi di spyware. Le forme di spyware precedentemente non rilevate possono spesso causare la maggior parte dei danni, quindi è fondamentale avere una protezione aggiornata e garantita. **Confronta e trova il miglior software di protezione dal phishing** I truffatori online cercheranno di indurti a rinunciare alle tue password o ad altre informazioni personali fingendosi siti Web legittimi. Spesso, si comportano anche allo stesso modo dei siti Web a cui accedi regolarmente. Queste minacce sono facilmente evitabili con un programma antivirus in atto. È nostro piacere mostrarti

	quali offrono la migliore protezione contro gli attacchi di phishing senza influire sulle prestazioni del tuo computer o intralciare il nostrolavoro. **Qual è la migliore soluzione antivirus?** Bitdefender, il marchio antivirus scelto da oltre 500 milioni di utenti in 150 paesi, è uno dei principali fornitori mondiali di prodotti di sicurezza informatica per i consumatori e un pioniere nella protezione antivirus. Questo marchio ha vinto numerosi premi antivirus dalaboratori di test online, tra cui AV-Comparatives, AV-Test, PCMag e The Anti-Malware Testing Standard Organization. Il servizio di contromisure di Netcraft aiuta le organizzazioni a combattere queste tecniche. Una volta rilevato un sito di phishing, Netcraft risponde immediatamente con una serie di azioni che limiteranno significativamente l'accesso al sito e, in ultima analisi, causeranno l'eliminazione del contenuto fraudolento. L'approccio di Netcraft alla rimozione dei siti di phishing si distingue dagli altri fornitori di servizi di rimozione perla sua capacità di bloccare immediatamente l'accesso al sito per gli utenti di una vasta gamma di tecnologie. **I migliori software anti-phishing** I truffatori online cercheranno di indurti a rinunciare alle tue password o ad altre informazioni personali fingendosi siti Web legittimi. Spesso, si comportano anche allo stesso modo dei siti Web a cui accedi regolarmente. Queste minacce sono facilmente evitabili con un programma antivirus in atto. Abbiamo il piacere di mostrarti quali offrono la migliore protezione contro gli attacchi di phishingsenza influire sulle prestazioni del tuo computer o intralciare il tuo lavoro. **Certificati di contrassegno verificati?** I certificati di contrassegno verificati (VMC) ti consentono di visualizzare il tuo logo accanto al campo "mittente" nei client di posta elettronica in modo che gli utenti vedano la tua storiae che la tua organizzazione sia stata autenticata prima ancora di aprire il tuo messaggio. È l'equivalente e-mail di un segno di spunta sui social media, con requisiti di convalida e sicurezza aggiuntivi per proteggere i tuoi clienti e il tuo marchio dagli attacchi di phishing e spoofing. L'e-mail verificata dal logo fa parte di un'iniziativa innovativa, in collaborazione con Brand Indicators for Message Identification (BIMI) e i fornitori di client di posta elettronica, per promuovere un'esperienza di posta elettronica coerente, affidabile e visivamente autenticabilesia per le imprese che per i consumatori. Ecco come funziona: (guarda il video) https://www.digicert.com/content/dam/digicert/videos/digicert-vmc-product-reveal.mp4 **COME PROTEGGERSI DAGLI ATTACCHI DI PHISHING** Proteggersi dagli attacchi di phishing inizia con la conoscenza di ciò che è là fuori.

	Non fare mai clic su collegamenti da mittenti sconosciuti o se qualsiasi dettaglio sullo scambio ha destato sospetti. Non è mai possibile, passa il mouse su un link per assicurarti che la destinazione corrisponda alle tueaspettative. Nota che questo non funzionerà sui dispositivi mobili o se vengono utilizzati codici brevi, quindi fai molta attenzione sui dispositivi mobili. Se sospetti che un'e-mail sia un tentativo di phishing, ricontrolla il nome del mittente, la specificità del saluto e un piè di pagina per un pulsante fisico di annullamentodell'iscrizione. In caso di dubbio, eliminare. Se non sei sicuro che una comunicazione sia legittima, prova a contattare il marchio o il servizio tramite un altro canale (il loro sito web o chiamando una linea di assistenza clienti, ad esempio). Evita di inserire informazioni personaliidentificabili a meno che tu non sia estremamente sicuro dell'identità della parte con cui stai comunicando. Colmare tutte le lacune di sicurezza Pur rimanendo vigili terrà a bada la maggior parte degli aggressori, nessuno può essere sicuro al 100% sul propriolavoro. Dopo tutto, il phishing esiste solo oggi perché funziona. Questo è il motivo per cui è importante combinare la formazione sulla consapevolezza della sicurezza con una protezione degli endpoint aziendali di qualità, con intelligence sulle minacce potenziata dall'intelligenza artificiale, aggiornamenti basati su cloud e protezione anti-phishing in tempo reale, DNS e backup affidabile dei dati. **Per prevenire le truffe degli anziani** Se sei preoccupato per le frodi, c'è molto che puoi fare per evitare che ti accada: Impostare il monitoraggio del credito e la protezione dal furto di identità - I criminali commettono quasi sempre frodiagli anziani con l'obiettivo di portare a termine truffe finanziarie. Il modo più semplice per proteggere te stesso o le finanze della persona amata è iscriversi al monitoraggio del credito. **Ulteriori passi da intraprendere:** FERMATI: Fai un respiro e pensa alla situazione. C'è qualcosa che ti sembra sospetto? LASCIA: riagganciare, chiudere la porta o chiudere l'e-mail. Se qualcuno ti sta spingendo ad agire ora, potrebbe essere un artista della truffa. CHIEDI: Chiama un membro della famiglia per un consiglio, cerca online maggiori dettagli e scopri se le organizzazioni sono reali. Puoi anche comek un visitatore per l'identificazione. ASPETTA: Prenditi il tempo per assorbire ciò che hai imparato e fare un piano d'azione. Non affrettare le decisioni. ACT: visita solo siti Web legittimi e chiama numeri di telefono sicuri e verificati. È possibile utilizzare siti Web di recensioni indipendenti eservizi di ricerca di indirizzi e-mail per verificare l'identità di qualcuno.

	Condividi le tue storie di tentativi di frode. Chiedi ai tuoi familiari più esperti di tecnologia di condividere esempi di e-mail o messaggi truffa che hanno ricevuto. Avere un piano e una password - La condivisione anticipata del conto bancariopuò garantire che il denaro della tua famiglia rimanga al sicuro. Sii sospettoso di qualsiasi chiamata o messaggio non richiesto - Un po 'di sospetto può risparmiarti un sacco di angoscia. Sappi che queste truffe esistono e chiediti sempre: "e se?" quando ti trovi di fronte a una richiesta di denaro inutileonline o di persona.

Nome del social media / strumento	**FACEBOOK**
Generalità	Facebook è un servizio americano di social media e social networking online di proprietà di Meta Platforms. Fondata nel 2004, il suo nome deriva dalle directory face book (https://en.wikipedia.org/wiki/Face_book) spesso date agli studenti universitari americani. All'inizio l'adesione era limitata solo agli studenti di Harvard. Dal 2006, era disponibile per chiunque avesse più di 13 anni. In esso era l'applicazione mobile più scaricata. In questo momento è possibile accedere a Facebook da diversi tipi di dispositivi dotati diconnettività Int ernet. Puoi usarlo facilmente su personal computer, tablet e smartphone. Per utilizzare l'applicazione, devi essere un utente registrato, il che significa creare un profilo che riveli informazioni su di te. Dopo questo processo puoi creare messaggi di testo, incluse foto e contenuti multimediali, puoi condividerli con tutti gli altri utenti che hanno accettato di essere tuoi "amici". Facebook consente di regolare diverse impostazioni sulla privacy, o il tuo profilo è disponibile pubblicamente o è disponibile solo per ora per te utenti. L'applicazione FaceBook permette anche di comunicare tra gli utenti con Facebook Messenger. Puoi eseguire conversazioni private, ma puoi anche unirti a creare gruppi o unirti a gruppi di interesse comune.
Rischio associato ai social media/strumento: **Privacy** **accuratezza** **legame corretto,** **accessibilità** **Violazione delle leggi,** **Diritto d'autore**	Facebook è stato spesso criticato per questioni come la privacy degli utenti, la sorveglianza di massa, gli effetti psicologici della manipolazione politica, come la dipendenza e la bassa autostima, e contenuti come notizie false,teorie del complotto, violazione del copyright e incitamento all'odio. ***Privacy:*** Nella pagina FB potete trovare il link diretto alle norme sulla privacy: https://www.facebook.com/privacy/policy ***Accuratezza:***

	https://www.facebook.com/policies_center/ads ***Proprietà:*** Facebook ritiene suo dovere aiutare gli individui e le organizzazioni a proteggerei loro diritti di proprietà intellettuale. I Termini e condizioni di Facebook vietano agli utenti di pubblicare contenuti che violano i diritti di proprietà intellettuale di altri, inclusi i diritti di copyright e di marchio. ***Diritto d'autore*** I diritti d'autore sono diritti statutari che proteggono le opere d'autore originali, come libri, opere musicali, film e opere d'arte. In generale, i diritti d'autore proteggono le espressioni originali, come dichiarazioni o immagini. Non proteggono fatti o idee, ma possono proteggere affermazioni o immagini originali che descrivono un'idea. Il diritto d'autore inoltre non protegge nomi, titoli o slogan. La loro protezione è garantita dalle leggi sui marchi. ***Marchi*** Un marchio è una parola, uno slogan, un simbolo o un disegno (ad esempio un marchio o un logo) che distingue i prodotti e i servizi offerti da un'entità, un gruppo o una società da quelli offerti da altre entità, gruppi o società. La funzione generale del diritto dei marchi è quella di aiutare i consumatori a riconoscere quale entità è responsabile di un particolareprodotto o servizio. https://www.facebook.com/help/399224883474207/?helpref=uf_share ***Accessibilità:*** Facebook offre un'esperienza confortevole per tutti gli utenti. Sono disponibili funzionalità e tecnologie per aiutare le persone con disabilità, come i problemi visivi e uditivi, a utilizzare Facebook il più possibile. ***Violazione delle leggi:*** Le istituzioni statali possono ritenere che il contenuto pubblicato da un utente su Facebook violi le leggi locali, possono chiedere una restrizione su questo contenuto. Se pubblichi contenuti non conformi alle leggi locali, un tribunale può ordinare una restrizione alla pubblicazione del contenuto o segnalare accuse di illegalità del contenuto da parte di istituzioni non governativee membri del pubblico. Le candidature vengono esaminate in conformità con gli impegni della Global Network Initiative e i Principi aziendali per la protezione dei diritti umani. https://transparency.fb.com/data/content-restrictions/content-violating-local-law/ ***Diritto d'autore:*** Le leggi possono variare da paese a paese. Le informazioni sul copyright sono disponibili presso l'Ufficio del copyright degli Stati Uniti o l'Organizzazione

	mondiale della proprietà intellettuale (OMPI). Facebook non fornisce consulenza legale, quindi è consigliabile consultare un avvocato se si hanno dubbisul copyright. Nella maggior parte dei paesi, il copyright è un diritto statutario che protegge le opere d'autore originali. Di solito, il creatore di un'opera originale ottiene il copyright su quell'opera al momento della creazione. Molti tipi diversi di contenuti sono protettidal diritto d'autore, tra cui: • *Materiale visivo o audiovisivo*: contenuti video, film, programmi televisivi e trasmissioni, videogiochi, dipinti, fotografie • *Contenuti audio*: canzoni, composizioni musicali, registrazioni sonore, registrazioni di dichiarazioni orali • *Contenuto scritto*: libri, opere teatrali, manoscritti, articoli, notazioni musicali Il diritto d'autore protegge solo le opere originali. Per essere considerato sufficientemente originale per la protezione del copyright, il contenuto deve essere opera dell'autore e deve essere stato creato da una determinata quantità di sforzo creativo.
Barriere/difficoltà per gli adulti	• alto livello di divulgazione dell'identità su Facebook in modo simile ad altri siti di social network. Le informazioni incluse possono essere, nome, indirizzo e-mail, indirizzo fisico, numero di telefono, sesso, città natale, data di nascita, foto, rete di amici, orientamento sessuale, stato di relazioneip, interessi, lavoro / occupazione, libri preferiti, film preferiti, musica preferita, scuola, informazioni, codice postale (o codice postale) e affiliazione politica. Le informazioni sopra menzionate sono particolarmente sensibili in quanto le persone si identificano autenticamente. • L'uso di nomi reali per rappresentare un profilo può essere incoraggiato attraverso specifiche tecniche, requisiti di registrazione o norme sociali (collegando i profili dei partecipanti con le loro identità pubbliche). • stalking, re-identificazione, reidentificazione demografica, reidentificazione del volto e furto di identità. Gli utenti possono essere manipolati attraverso l'ingegneria sociale, le molestie, lo stalking e lo spamming a causa dell'elemento di "inquietudine" • del sito • Facebook può anche creare dipendenza. • La comunicazione online è più attraentedell'interazione faccia a faccia, questo a sua volta può aumentare la socializzazione su Internet. Ciò può creare un uso compulsivo ed eccessivo dei social network online che può avere effetti negativi sui risultati sul lavoro e a casa (contrastando altre carenze comel'esaltazione, la mancanza di amici, l'aspetto fisico e le disabilità). • nessuna possibilità di denunciare gli autori di reati sessuali alla polizia, • La polizia ha sollevato preoccupazione per Facebook che non accetta di fornire un pulsante antipanico alla pagina del profilo di ogni utente, Facebook non riesce ad affrontarela minaccia dei pedofili. • l'aumento di reati come molestie e danni fisici effettivi a seguito dell'uso di Facebook

	•
Pericolo dei social media / strumento negli adulti	• Perdere il controllo del tempo che trascorri online. Il layout delle pagine, ogni pulsante, ogni colore è scelto con cura dagli esperti per attirare l'attenzione. • Il numero di account Facebook falsi è enorme - i cosiddetti troll di Internet • Gli hacker sanno molto bene come decifrare una password su FB. • È molto comune falsificare le pagine di accesso ai social network e inviare messaggi falsi • Facebook è spesso usato come strumento per diffondere informazioni false • Le informazioni che pubblichiamo noi stessi sui social media possono essere utilizzate da terzi • Il Koobface worm è stato attivo su Facebook per oltre un anno • La condivisione della tua posizione con applicazioni e altri utenti può comportare il tracciamento dell'utente (ad es. osservazione della tua posizione, furto con scasso) • Anche l'autenticazione biometrica per l'accesso, ad esempio, al telefono cellulare o ai profili online (utilizzando una scansione facciale o un'impronta digitale) è emersa come una minaccia.
Soluzioni che possiamo avere	Formazione on line su come : • Usa in sicurezza Facebook; • Cosa non pubblicare sui social network (come limitare la condivisione di informazioni private su di te) • Impostazioni sulla privacy su FB. • Creazione di una password sicura per l'account • Impostazione dell'autenticazione a due fattori. • Accettare inviti (identificare un invito dauna persona). • Mantenere aggiornati antivirus e altri software di sicurezza. • Utilizzando il modulo Conversazioni private. • Condivisione di contenuti, foto e post da altri social media. • Come segnalare contenuti che sembrano sospetti.

Nome del social media / strumento	**GOOGLE+**
Generalità	**Google+** è stato lanciato il 28 giugno 2011, nel tentativo di sfidare altri social network, collegando altri prodotti Google come Google Drive, Blogger e YouTube. Di solito è noto come Google Plus, a volte chiamato G + era un social network di proprietà e gestito da Googl e. Cambiamenti sostanziali hanno portato a una riprogettazione di questo social network nel novembre 2015. Il 7 marzo 2019 è stato deciso di chiudere il social network per le imprese e un mese dopo, il 2 aprile, è stato chiuso anche per gli utenti personali. La ragione di questa decisione era sia il basso coinvolgimento degli utenti che i difetti di

	progettazione del software divulgati che potenzialmente consentivano agli sviluppatori esterni di accedere alle informazioni personali dei propri utenti. Google+ ha continuato a essere disponibile come "Google+ per G Suite"; tutti gli utenti sono passati a "Google Currents". Il prossimo passo sarà infine il passaggio da Google Currents a "Google Chat" nel 2023. Su Google+, le persone possono condividere idee e notizie personali, pubblicare foto e video, rimanere in contatto, giocare, pianificare incontri, inviare auguri di compleanno, fare affari insieme, trovare econtattare amici e parenti perduti da tempo, recensire libri, consigliare ristoranti e sostenere cause. L'elenco potrebbe continuare - puoi vedere quanto sia individuale il suo utilizzo. Il social networking include anche ottenere e fornire convalida e supporto emotivo, un sacco di apprendimento informale, nonché esplorare interessi personali, accademici e professionali futuri. Devi essere un utente registrato per avere pieno accesso alle opzioni di Google +. Durante l'accesso / registrazione ti verrà chiesto di rispondere ad alcune semplici domande come il tuo vero nome, un nome utente, una password e la tua data di nascita. Negli Stati Uniti per ottenere un account, devi avere almeno 13 anni, lo stesso in altri paesi. Ti verrà anche data l'opportunità di aggiungere un'immagine del profilo e lan verrai portata direttamente in Google+. Durante il processo di registrazione ti verrà chiesto di "trovare persone che conosci su Google+" inserendo un indirizzo email da Yahoo o Hotmail. Questa operazione è facoltativa. Google+ non contatterà le persone nel tuo elenco di contatti, ma importerà i contatti da tali servizi e ti darà la possibilità di aggiungere i tuoi contatti da tali servizi alle tue cerchie. Una volta creato un account, la prima volta che visiti Google+ ti verranno poste diverse domande, che sono facoltative (nome della scuola o dell'ufficio e dove vivi per rendere più facile per amici, familiari e altri trovarti).
Rischio associato ai social media/strumento: **Privacy, accuratezza, proprietà, accessibilità, violazione delle leggi, copyright**	***Privacy:*** L'impostazione della privacy consentiva agli utenti di divulgare determinate informazioni alle cerchie di loro scelta. Gli utenti possono anche vedere i visitatori del loro profilo. C'erano impostazioni sulla privacy chepotevi raggiungere facendo clic sul tuo nome in alto a destra dello schermo e poi sulla privacy. Ciò includeva collegamenti alla gestione delle cerchie, alla visibilità della rete (chi era nelle tue cerchie e chi poteva vedere chi ti aveva aggiunto alle loro cerchie) e altre impostazioni. C'era anche un link alla sezione di aiuto sulla privacy di Google+. ***Accuratezza:*** Nessun dato. ***Proprietà:*** Alcune società di gestione immobiliare hanno utilizzato Google+ per condividere i propri post sul blog, articoli di terze parti, notizie sulla propria attività o sul settore in generale, ecc.

	Google My Business è ora diventato l'hub centrale in cui i visitatori web possono trovare e saperne di più sulla tua azienda. ***Accessibilità:*** La maggior parte delle cose che puoi fare su Google+ sul Web può essere eseguita anche tramite l'app Google+ per smartphone per Android e iPhone, ed esiste un'app Web che funziona con altri telefoni connessi a Internet. Google Messenger è una funzionalità per smartphone (ma non la versione desktop di Google+) che consente a gruppi di persone di avere una conversazione. ***Violazione delle leggi:*** Google lavora duramente per rispettarequeste regole, ma con milioni di utenti e milioni di post non possono fare tutto da soli. È qui che entra in gioco la comunità. Spetta a tutti noi assicurarci che Google+ rimanga un luogo sicuro e confortevole. Se vedi contenuti che appaiono in violazionedegli standard, hai la possibilità di fare clic sulla freccia verso il basso a destra del post o del contenuto e selezionare Segnala abuso. Ti viene quindi chiesto di specificare perché è offensivo selezionando la casella appropriata. C'è anche un'opzione per "Segnala questo profilo e" nella colonna di sinistra del profilo di ogni persona se il profilo stesso contiene contenuti che potrebbero violare gli standard della community di Google. ***Diritto d'autore:*** Il riferimento standard per la questione della violazione del copyright sono i Termini di servizio di Google. Ilservizio G oogle "Rispondiamo alle notifiche di presunta violazione del copyright e chiudiamo gli account dei trasgressori recidivi secondo la procedura stabilita nel Digital Millennium Copyright Act degli Stati Uniti. Forniamo informazioni per aiutare i titolari di copyright a gestire la loro proprietà intellettuale online. Se ritieni che qualcuno stia violando i tuoi diritti d'autore e desideri inviarci una notifica, puoi trovare informazioni sull'invio di notifiche e sulle norme di Google sulla risposta alle notifiche nel nostro Centro assistenza.
Barriere/difficoltà per gli adulti	• Il rischio più comune è l'aggressione sociale (cyberbullismo) • Pubblicare informazioni imbarazzanti o dannose su di noi - testo, foto o video che potrebbero metterci in imbarazzo ora o in seguito, pubblicati da noi stessi o da altri. Questoè il problema della reputazione. • La sfida del tempo sullo schermo: troppo tempo su qualsiasi cosa può essere dannoso per altre attività nella nostra vita. • Rischio di contatto inappropriato con estranei / hacker • Fai attenzione a chi inviti a un ritrovo e renditi conto che chiunque sia invitato può invitare altre persone che potresti non conoscere.

Pericolo dei social media / strumento negli adulti	Per il momento Google + non sarà un pericolo per gli adulti, poiché il social network è chiuso dal 2019.
Soluzioni che possiamo avere	Manuali o guide che supporteranno nel download dei dati inseriti nell'account Google + creato prima del 2019.

MILEAGE

Partners

E-Seniors (France) • www.eseniors.eu

CARDET (Cyprus) • www.cardet.org

EDUCATOR (Czech Republic) • www.educatorspolek.com

Framework (Italy) • www.aframework.it

WSBINOZ (Poland) • www.wsbinoz.edu.pl

Join us!

mileageproject info@mileageproject.eu www.mileageproject.eu

Funded by the Erasmus+ Programme of the European Union

The European Commission support for the production of this publication does not constitute an endorsement of the contents which reflects the views only of the authors, 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