MILEAGE

ANALIZA RYZYK I BARIER

WPROWADZENIE

Głównym celem projektu MILEAGE jest stworzenie nowego i bardziej angażującego sposobu wspierania umiejętności cyfrowych seniorów oraz umiejętności korzystania z mediów i informacji (MIL), aby umożliwić im korzystanie z narzędzi ICT w codziennym życiu, podnosząc świadomość na temat cyfrowych zagrożeń i sposobów radzenia sobie z nimi.

Jak?

- Opracowując raport dotyczący zagrożeń i barier, na jakie napotykają seniorzy w środowisku cyfrowym
- Dzięki opracowaniu wirtualnych scenariuszy zagrożeń (odgrywanie ról)
- Dzięki stworzeniu mikro lekcji z wyjaśnieniami dotyczącymi zdefiniowanych ryzyk
- Opracowując podręcznik dla edukatorów osób dorosłych z wytycznymi wspierającymi działania szkoleniowe (efekt multiplikacji).

Niniejszy raport, dotyczący ryzyka i barier przedstawia główne media społecznościowe, narzędzia komunikacji i inne platformy, które są obecnie powszechnie używane. Opisujemy ryzyka i niebezpieczeństwa z nimi związane: każdy problem lub ryzyko jest analizowane i proponowane jest rozwiązanie, aby je przezwyciężyć, wymieniając również kompetencje potrzebne i aktywowane w tym celu.

Dokument ten został stworzony, aby dać trenerom, seniorom i ogółowi społeczeństwa informacje związane ze środowiskiem cyfrowym, z którym seniorzy stykają się w swoim codziennym życiu, oferując pewne wskazówki i porady, aby zwiększyć kompetencje cyfrowe seniorów i ich zaufanie do świata cyfrowego. Dokument ten będzie pomocny przy opracowywaniu treści szkoleniowych oraz scenariuszy ryzyka stworzonych w ramach projektu w celu wspierania umiejętności korzystania z mediów i informacji przez seniorów.

MILEAGE

1. WHATSAPP

Nazwa mediów społecznościowych / narzędzia	**WHATSAPP**
Informacje ogólne	WhatsApp to darmowy program do komunikacji pobierany na smartfony. Wysyła wiadomości, zdjęcia, audio i wideo przez Internet. Usługa jest dość podobna do usług wysyłania wiadomości tekstowych, ale ponieważ WhatsApp wysyła wiadomości przez Internet, jest znacznie tańszy niż wysyłanie wiadomości tekstowych. Możesz również użyć Whatsapp na komputerze, odwiedzając stronę Whatsapp i pobierając program dla Maca lub Windowsa. Ze względu na funkcje, takie jak czat grupowy, wiadomości audio i udostępnianie lokalizacji, jest bardzo popularny wśród młodzieży.
Ryzyko związane z mediami społecznościowymi/ narzędziem: **Prywatność, dokładność, własność, dostępność, Naruszenie prawa, Prawo autorskie**	Prywatność Kradzież profilu Nagrywanie rozmów (cyberprzestępstwa)
Bariery/trudności dla dorosłych	Ustawienia prywatności.
Niebezpieczeństwo mediów/narzędzi społecznościowych u dorosłych	Hakerzy Niezaszyfrowane kopie zapasowe
Rozwiązania, które możemy mieć	Nigdy nie udostępniaj nikomu swojego kodu rejestracyjnego ani kodu PIN do weryfikacji dwuetapowej. Utwórz kod dla swojego urządzenia. Śledź, kto ma dostęp do Twojego telefonu na poziomie fizycznym. Znajomość aplikacji i jej ustawień.

2. VIBER

Nazwa mediów społecznościowych / narzędzia	**VIBER**
Informacje ogólne	Viber to darmowa aplikacja, która umożliwia użytkownikom wykonywanie darmowych połączeń, wysyłanie wiadomości tekstowych, zdjęć i filmów do innych użytkowników Viber. Może być używany do łączenia się z osobami na całym świecie i działa zarówno na urządzeniach mobilnych, jak i komputerach stacjonarnych. Aplikacja do przesyłania wiadomości miała 236 milionów miesięcznych aktywnych użytkowników w lutym 2015 roku. Udostępnianie zdjęć, wideo i czat grupowy to popularne funkcje dla młodych konsumentów, podobne do WhatsApp.
Ryzyko związane z mediami społecznościowymi/ narzędziem: **Prywatność, dokładność, własność, dostępność, Naruszenie prawa, Prawo autorskie**	Cyberprzemoc Prywatność Spamowe połączenia
Bariery/trudności dla dorosłych	Ustawienia prywatności
Niebezpieczeństwo mediów/narzędzi społecznościowych u dorosłych	Hakerzy
Rozwiązania, które możemy mieć	Śledzenie, kto ma dostęp do Twojego telefonu na poziomie fizycznym. Znajomość aplikacji i jej ustawień. Blokowanie innego użytkownika w serwisie Viber (Podczas odbierania wiadomości od nieznanego kontaktu).

3. FIRMY OFERUJACE NOCLEGI

Nazwa mediów społecznościowych / narzędzia	**FIRMY OFERUJĄCE NOCLEGI**
Informacje ogólne	Za dostawcę zakwaterowania uważa się każdego, kto zapewnia zakwaterowanie za wynagrodzeniem lub kto zakwaterował więcej niż 5 cudzoziemców, z wyjątkiem przypadków, w których cudzoziemiec i dostawca mogą być uznani za pozostających w bliskich stosunkach. Przykłady: **Hotele, B&B, Airbnb, Booking**
Ryzyko związane z mediami społecznościowymi/ narzędziem: **Prywatność, dokładność, własność, dostępność, Naruszenie prawa, Prawo autorskie**	Oszustwa Dezinformacja / wprowadzanie w błąd Oszustwa związane z kartami
Bariery/trudności dla dorosłych	Wykorzystanie technologii do rezerwacji noclegów Warunki, które nie są widoczne
Niebezpieczeństwo mediów/narzędzi społecznościowych u dorosłych	Wykorzystanie technologii do rezerwacji noclegów Warunki, które nie są widoczne Niedostępne dla osób starszych Izolacja
Rozwiązania, które możemy mieć	Trudności te nie oznaczają, że starzenie się w miejscu zamieszkania jest nieosiągalnym lub niepożądanym celem, ale raczej, że wymagane jest szeroko zakrojone planowanie zarówno na poziomie jednostki, jak i społeczności. Pierwszym etapem jest edukacja firm zajmujących się zakwaterowaniem na temat finansowych i fizycznych problemów, z jakimi mogą się spotkać, jeśli pozostaną w swoim dotychczasowym domu, a także dostępnych rozwiązań, aby je rozwiązać. Podobnie jak zapewnienie, że samorządy lokalne są świadome i przygotowane na problemy, z którymi zmierzą się ich seniorzy.

4. FIRMY LOTNICZE

Nazwa mediów społecznościowych / narzędzia	**FIRMY LOTNICZE**
Informacje ogólne	Organizacja, która zapewnia transport lotniczy dla pasażerów i towarów.
Ryzyko związane z mediami społecznościowymi/ narzędziem: **Prywatność, dokładność, własność, dostępność, Naruszenie prawa, Prawo autorskie**	Oszustwa Dezinformacja Oszustwa związane z kartami
Bariery/trudności dla dorosłych	Wykorzystanie technologii do rezerwacji lotu
Niebezpieczeństwo mediów/narzędzi społecznościowych u dorosłych	Wykorzystanie technologii do rezerwacji lotu Warunki, które nie są widoczne Niedostępne dla osób starszych
Rozwiązania, które możemy mieć	Planuj z wyprzedzeniem Badanie podróży lotniczych seniorów i pomoc w tym zakresie Zarządzaj parkingiem tak, aby uwzględnić problemy związane z mobilnością Przygotuj się na ochronę lotniska Sprawdź, czy są zniżki na bilety lotnicze dla seniorów Wybierz odpowiedni **czas** lotu

5. PLATFORMY RANDKOWE

Nazwa mediów społecznościowych / narzędzia	**PLATFORMY RANDKOWE**
Informacje ogólne	Platformy randkowe to strony internetowe lub aplikacje, które umożliwiają osobom kontakt i komunikację w celu rozwinięcia związku. Dostęp do tych stron często wymaga od użytkowników podania danych osobowych, takich jak wiek, płeć i lokalizacja geograficzna. Istnieją setki różnych platform randkowych. Mogą być one ogólnotematyczne lub wyspecjalizowane dla danego typu relacji (miłosnej, erotycznej, przyjacielskiej) lub typu członków (przynależność religijna lub etniczna, orientacja seksualna, grupa wiekowa). Niektóre z najbardziej znanych platform to: **Meetic, Tinder, Bumble, eDarling, Badoo, OkCupid** itp. Chociaż większość platform randkowych jest darmowa, niektóre wymagają miesięcznego abonamentu lub opłacenia dodatkowych płatnych funkcji.
Ryzyko związane z mediami społecznościowymi/ narzędziem:	Prywatność Sum
Bariery/trudności dla dorosłych	Główną trudnością dla seniorów związaną z platformami randkowymi jest praktyczne wykorzystanie tych narzędzi. Aby móc korzystać z takich platform, seniorzy potrzebują dość zaawansowanej wiedzy z zakresu ICT. Na przykład do zalogowania się potrzebują adresu e-mail, co oznacza, że muszą wiedzieć, jak stworzyć adres e-mail i jak go używać. Platforma wymaga również wgrywania zdjęć, ale seniorzy niekoniecznie wiedzą, jak to zrobić.
Niebezpieczeństwo mediów/narzędzi społecznościowych u dorosłych	**Prywatność** Użytkownicy dzielą się osobistymi informacjami na platformach randkowych, mając nadzieję na znalezienie najlepszych dopasowań. Informacje, którymi się dzielą, obejmują zdjęcia, orientację seksualną, wiek, religię, płeć, ich hobby, czy mają dzieci, wzrost itp. Ponadto, platformy randkowe często oferują opcję powiązania ich profili z ich kontami w mediach społecznościowych, takich jak Facebook lub Instagram, umożliwiając synchronizację aplikacji randkowej z mediami społecznościowymi i wyświetlanie informacji osobistych, takich jak zdjęcia, które są automatycznie ładowane na ich profilu randkowym. Kilka platform randkowych doświadczyło naruszenia bezpieczeństwa, co może być szczególnie szkodliwe dla użytkowników, ponieważ na tych platformach udostępniane są wrażliwe dane. **Sum**

	Seniorzy, którzy rejestrują się na platformach randkowych, często są samotni (rozwiedzeni, owdowiali) i dlatego pokładają duże nadzieje w spotkaniu potencjalnego partnera. Jednak na tych platformach zdarza się wiele fałszywych profili i oszustw. Ludzie udają coś, czym nie są i inwestują się w sentymentalną relację, by nawiązać więź, a następnie wykorzystać ją do wydobycia pieniędzy.
Rozwiązania, które możemy mieć	Przed założeniem konta użytkownicy powinni zapoznać się z polityką prywatności i warunkami świadczenia usług danej platformy. Ważne jest, aby wstrzymać się z przeczytaniem i zrozumieniem tych warunków tak bardzo, jak to możliwe, aby móc wyrazić świadomą zgodę. Catfishing może spowodować prawdziwe szkody. Aby temu zapobiec, użytkownicy mogą poprosić o rozmowę wideo z osobą, z którą rozmawiają, aby zweryfikować, czy pasuje ona do zdjęć na stronie internetowej. Użytkownicy mogą również korzystać z narzędzi takich jak **Google Reverse Photo Search**, aby zweryfikować, czy zdjęcie jest oryginalne, czy też pochodzi od kogoś innego. Co najważniejsze, ważne jest, aby użytkownicy ufali swojemu przeczuciu, jeśli czują, że są wyłudzani, a zatem zachowują ostrożność w dzieleniu się wieloma szczegółami.

6. BANKOWOŚĆ ONLINE

Nazwa mediów społecznościowych / narzędzia	**BANKOWOŚĆ ONLINE**
Informacje ogólne	Bankowość internetowa znana jest również jako bankowość internetowa, net banking lub bankowość elektroniczna. Jest to elektroniczny system płatności, który umożliwia klientowi banku lub instytucji finansowej dokonywanie transakcji finansowych lub niefinansowych online za pośrednictwem Internetu. Usługa ta daje dostęp online do prawie wszystkich usług bankowych, tradycyjnie dostępnych w lokalnym oddziale, w tym przelewów, depozytów i płatności rachunków online dla klientów. Dostęp do niego może uzyskać każda osoba fizyczna, która zarejestrowała się w banku do bankowości internetowej, posiadająca aktywny rachunek bankowy lub dowolna instytucja finansowa. Bankowość internetowa oferuje całodobowy dostęp do rachunków użytkowników każdego dnia. Jest szybka i wygodna, pozwala na wykonywanie transakcji w dowolnym miejscu, czasie, na dowolnym urządzeniu (komputer, smartfon, tablet) z dostępem do Internetu Niektóre banki internetowe to tradycyjne banki, które oferują również bankowość internetową, podczas gdy inne są tylko online i nie mają fizycznej obecności. Według Eurostatu w 2020 roku średnia populacji korzystającej z bankowości internetowej w UE wynosiła 60%. W Czechach osiągnęła ona 70%, ale w Polsce było to już tylko 49%. We Włoszech 86,8 proc. osób, które korzystają z internetu, korzystało również ze strony lub aplikacji związanej z bankowością. W najnowszym raporcie World Retail Banking Report, 57% konsumentów twierdzi, że obecnie preferuje bankowość internetową (online) od tradycyjnej bankowości oddziałowej. A 55% konsumentów woli obecnie korzystać z mobilnych aplikacji bankowych, aby być na bieżąco ze swoimi finansami, co stanowi wzrost z 47% w erze przed pandemią.
Ryzyko związane z mediami społecznościowymi/ narzędziem: **Prywatność, dokładność, własność, dostępność, Naruszenie prawa, Prawo autorskie**	Prywatność Cyberprzestępstwa: kradzież danych i oszustwa.

Bariery/trudności dla dorosłych	Trudności dla dorosłych seniorów dotyczą kwestii strachu i zaufania, a także braku wiedzy i wskazówek, jak korzystać z systemu bankowości internetowej swojego banku.
Niebezpieczeństwo mediów/narzędzi społecznościowych u dorosłych	**Brak zaufania** Dane zebrane przez Casalo i wsp. (2007) wykazały, że bezpieczeństwo i prywatność strony internetowej, użyteczność i reputacja mają bezpośredni i istotny wpływ na zaufanie konsumentów do strony internetowej usług finansowych. Zauważono, że zaufanie jest kluczowym czynnikiem pośredniczącym w rozwoju bankowości internetowej. **Oszustwa i kradzież danych** Ryzyko to jest raczej powszechną obawą niż częstym problemem. Rzeczywiście, według badania przeprowadzonego w 2020 r. przez Europejską Agencję Praw Podstawowych, jedna czwarta Europejczyków (24%) bardzo obawia się, że dane dotyczące ich internetowego konta bankowego lub karty płatniczej zostaną niewłaściwie wykorzystane. Jednak ogólnie rzecz biorąc, mniej niż 1 na 10 (8%) doświadczył oszustwa związanego z bankowością internetową lub kartą w ciągu pięciu lat poprzedzających badanie. Bardziej narażeni na takie doświadczenia są mieszkańcy Wielkiej Brytanii (24%), Francji (19%) i Danii (15%). **Bezpieczeństwo** Zagrożenie bezpieczeństwa związane jest z rosnącą liczbą oszukańczych stron internetowych banków, z fałszywymi e-mailami rzekomo wysyłanymi z banków, z wykorzystaniem programów typu koń trojański do przechwytywania identyfikatorów i haseł użytkowników. Ryzyko hakerskie (haker wchodzący na konto bankowe i kradnący środki) również istnieje, choć jest bardzo rzadkie. **Prywatność** Według badania z 2020 roku opublikowanego przez KPMG, 87% konsumentów twierdzi, że prywatność danych jest podstawowym prawem człowieka. Jednak 68% twierdzi, że nie ufa firmom, które etycznie sprzedają ich dane osobowe. **Naruszenie danych i phishing** W 2020 roku specjaliści odkryli problem bezpieczeństwa w pewnym banku, piątym co do wielkości w Europie i szesnastym na świecie. Belgijski oddział banku miał błędną konfigurację w swojej domenie internetowej, co pozwalało na pobieranie jej plików. Pliki te zawierały wrażliwe informacje (nazwisko, e-mail, telefon), które mogły być wykorzystane przez hakerów do potencjalnego wyłudzenia danych klientów banku. Phishing to rodzaj ataku często wykorzystywany do kradzieży danych użytkownika, w tym danych logowania i numerów kart kredytowych. Dochodzi do niego, gdy napastnik, podając się za

	zaufany podmiot, nakłania ofiarę do otwarcia wiadomości e-mail, komunikatora lub SMS-a i wykrada jej dane.
Rozwiązania, które możemy mieć	**Nauka korzystania z bankowości internetowej - tutorial** Aby w praktyce poprowadzić Cię w korzystaniu z narzędzia bankowości internetowej, poproś swojego bankiera o tutorial banku. Każdy bank ma taki opracowany. **Bezpieczeństwo i bankowość internetowa** Portale bankowości internetowej są zabezpieczone unikalnymi identyfikatorami Użytkownika/Klienta oraz hasłami. Niektóre z nich wymagają bezpiecznego klucza (urządzenia), które generuje unikalny kod przy każdym połączeniu). **Przewidywanie oszustw** W kontekście bankowości internetowej, przewidywanie oszustw polega na tworzeniu profili klientów w oparciu o informacje historyczne zebrane podczas czynności związanych z bankowością internetową (używane terminale, zwyczajowy czas i miejsce połączenia, przebieg połączenia i czynności, itp.), a następnie przewidywaniu stopnia oszustwa dla bieżącej operacji, poprzez porównanie aktualnego zachowania klienta z jego profilem. Jeśli stopień oszustwa zostanie uznany za wysoki, operacja zostaje zablokowana. **Reakcja na oszustwo** Banki oferują również bezpośrednią linię (telefoniczną lub internetową) do zgłaszania oszustw, jak również wskazówki dotyczące zapobiegania oszustwom. **Praktyczne wskazówki** ● Używaj bezpiecznych haseł i regularnie je aktualizuj ● Wybierz unikalne hasła dla każdego cyfrowego konta bankowego, nie używaj tego samego hasła do wielu kont ● Używaj bezpiecznego narzędzia do przechowywania haseł ● Unikaj korzystania z niezabezpieczonych publicznych sieci Wi-Fi podczas uzyskiwania dostępu do kont finansowych online ● Wiedza, jak rozpoznać oszustwa typu phishing za pomocą wiadomości e-mail lub SMS ● Odwiedzaj tylko bezpieczne strony internetowe ● Zainstaluj na swoich urządzeniach ochronę przed oprogramowaniem szpiegowskim i złośliwym. ● Skonfiguruj alerty, aby śledzić swoje konta i monitorować aktywność transakcji ● Włącz uwierzytelnianie wieloczynnikowe

7. PŁATNOŚCI ONLINE

Nazwa mediów społecznościowych / narzędzia	**PŁATNOŚCI ONLINE**
Informacje ogólne	Płatności online dokonywane są na stronach e-commerce za pomocą kart kredytowych, ale także za pomocą e-portfeli. Przelewy bankowe, karty wirtualne i bony towarowe to także inne metody płatności cyfrowych. Według Statista, w 2019 roku jeden na pięciu Europejczyków wolał korzystać z aplikacji płatniczych Fintech podczas zakupów online. Karty debetowe uplasowały się jako najpopularniejsza metoda płatności online, a Apple Pay i Google Pay były używane przez mniej więcej trzy procent respondentów. Jeśli chodzi o e-portfele, dane są nadal niedostępne, ale jest to rynek, który stale rośnie. Platformy płatności online i e-portfele: • PayPal • Google Pay • Apple Pay • Ali Pay • Samsung Pay • Mobikwik • Paytm • Amazon Pay • Portfel Microsoft • Stipe • Klarna
Ryzyko związane z mediami społecznościowymi/ narzędziem: **Prywatność, dokładność, własność, dostępność, Naruszenie prawa, Prawo autorskie**	Prywatność Cyberprzestępstwa: kradzież danych i oszustwa internetowe.
Bariery/trudności dla dorosłych	Trudności, jakie napotykają dorośli seniorzy, wiążą się z kwestią strachu i zaufania, ponieważ przypadki oszustw płatniczych są bardzo mediatyzowane. Druga trudność dotyczy praktycznego wykorzystania tego narzędzia. Różne rodzaje płatności online mogą być trudne do zrozumienia, a liczne kroki niezbędne do ich zawarcia mogą stanowić techniczne wyzwanie.
Niebezpieczeństwo mediów/narzędzi	**Prywatność** O ile dziś gotówka pozwala na anonimowe płatności - a więc brak śledzenia dokonanych zakupów i brak zagrożenia dla prywatności - o tyle inaczej jest w

społecznościowych u dorosłych	przypadku płatności internetowych, które są wysoce identyfikowalne (adres IP, imię, nazwisko, adres, numer karty itp.). **Kradzież danych** Ilość danych udostępnianych podczas transakcji płatniczych online rodzi pytanie o kradzież danych. Według Norton Global Cyber Safety Report 2019 ponad połowa respondentów doświadczyła cyberprzestępstwa, natomiast 1 na 3 padł ofiarą w ciągu ostatnich 12 miesięcy. W skali międzynarodowej narażono 4,1 mld rekordów i nastąpił wzrost o 54% liczby zgłoszonych naruszeń. **Oszustwo internetowe** Według Europejskiego Banku Centralnego, łączna wartość oszukańczych transakcji z wykorzystaniem kart wydanych na całym świecie wyniosła w 2018 roku 1,80 mld euro. Jeśli chodzi o karty wydane tylko w strefie euro, łączna wartość oszukańczych transakcji kartami wyniosła w 2018 roku 0,94 mld euro.
Rozwiązania, które możemy mieć	**Uwierzytelnianie wieloczynnikowe (MFA) lub uwierzytelnianie dwuczynnikowe (2FA)** Jest to metoda uwierzytelniania elektronicznego, w której użytkownik otrzymuje dostęp do usługi dopiero po udanym przedstawieniu dwóch lub więcej dowodów (lub czynników) mechanizmowi uwierzytelniania: **Wiedza**: coś, co wie tylko użytkownik, zwykle prezentowana jako odpowiedź na pytanie, np. imię zwierzęcia domowego **Posiadanie**: coś co posiada tylko użytkownik np. smartfon lub token. W przypadku smartfona na telefon użytkownika zostanie wysłany sms z kodem do wpisania. **Inherence**: coś, co tylko użytkownik obejmuje wykorzystanie rozpoznawania oczu i twarzy lub odcisków palców. **Poproś o CVV** Są to trzy cyfry znajdujące się za kartą kredytową, które są zadawane podczas transakcji płatniczej w Internecie, aby upewnić się, że jesteś w posiadaniu swojej karty kredytowej. **Bezpieczne przetwarzanie płatności** Dzieje się to za pośrednictwem portali płatności online, które posiadają certyfikaty PCI, SSAE-16 i HIPAA. Klienci i dostawcy nie muszą się martwić, że ich wrażliwe dane zostaną wycieknięte i skradzione przez hakerów.

8. INSTAGRAM

Nazwa mediów społecznościowych / narzędzia	**INSTAGRAM**
Informacje ogólne	Instagram to amerykański serwis społecznościowy do udostępniania zdjęć i filmów. Aplikacja umożliwia użytkownikom przesyłanie mediów, które można edytować za pomocą filtrów i organizować za pomocą hashtagów i tagów geograficznych. Posty mogą być udostępniane publicznie lub wstępnie zatwierdzonym zwolennikom. Użytkownicy mogą przeglądać treści innych użytkowników według tagów i lokalizacji, a także przeglądać trendowe treści. Użytkownicy mogą polubić zdjęcia i śledzić innych użytkowników, aby dodać ich treści do osobistego kanału. W serwisie dodano również funkcje przesyłania wiadomości, możliwość umieszczania wielu zdjęć lub filmów w jednym poście oraz funkcję "stories", która pozwala użytkownikom zamieszczać zdjęcia i filmy w sekwencyjnym kanale, przy czym każdy post jest dostępny dla innych przez 24 godziny. Na koniec 2021 roku w Czechach było 2,9 mln użytkowników. Jest to najszybciej rozwijająca się sieć. Największą popularnością cieszy się wśród użytkowników w wieku od 15 do 29 lat.
Ryzyko związane z mediami społecznościowymi/ narzędziem: **Prywatność, dokładność, własność, dostępność, Naruszenie prawa, Prawo autorskie**	Prywatność Kradzież profilu Wpływ na zdrowie psychiczne (objawy depresyjne, lęk, stres, uzależnienia, zadowolenie z wyglądu, fałszywa autoprezentacja, obraz ciała, samotność, wykluczenie społeczne, satysfakcja z życia itp.)
Bariery/trudności dla dorosłych	Trudność w znalezieniu rówieśników (71% użytkowników Instagrama ma mniej niż 35 lat). Prośba o podanie danych osobowych (jak data urodzenia). Ustawienia prywatności.
Niebezpieczeństwo mediów/narzędzi społecznościowych u dorosłych	Prywatność - użytkownik sieci powinien zwrócić uwagę na to, kogo śledzi i przez kogo jest śledzony, czy też kto może zobaczyć dane osobowe i zdjęcia/filmy. Kradzież profilu - konto może zostać "skradzione", zdjęcia użytkownika mogą zostać wykorzystane gdzie indziej lub hakerzy mogą działać w jego imieniu.
Rozwiązania, które możemy mieć	Znajomość aplikacji i jej ustawień, zasad jak zachowywać się na Instagramie. Stosowanie silnego hasła i jego regularna zmiana. Dwuczynnikowe uwierzytelnianie (w komputerze i w telefonie). Prywatne konto dla osobistego profilu. Korzystanie wyłącznie z autoryzowanych aplikacji.

9. SKYPE

Nazwa mediów społecznościowych / narzędzia	**SKYPE**
Informacje ogólne	Skype to zastrzeżona aplikacja telekomunikacyjna prowadzona przez Skype Technologies, oddział firmy Microsoft, najbardziej znana z telefonii wideo opartej na technologii VoIP, wideokonferencji i połączeń głosowych. Posiada również komunikatory internetowe, przesyłanie plików, połączenia debetowe z telefonami stacjonarnymi i komórkowymi (przez tradycyjne sieci telefoniczne) oraz inne funkcje. Skype jest dostępny na różnych platformach desktopowych, mobilnych i konsolach do gier wideo. Popularność skype'a znacznie wzrosła podczas pandemii.
Ryzyko związane z mediami społecznościowymi/ narzędziem: **Prywatność, dokładność, własność, dostępność, Naruszenie prawa, Prawo autorskie**	Prywatność Kradzież profilu Nagrywanie rozmów (cyberprzestępstwa)
Bariery/trudności dla dorosłych	Ustawienia prywatności.
Niebezpieczeństwo mediów/narzędzi społecznościowych u dorosłych	Niezamówione telefony. Nieufność wobec innych użytkowników.
Rozwiązania, które możemy mieć	Znajomość aplikacji i jej ustawień. Dobrze dobrane tło - gdzie skierowana jest kamera (aby nie pokazać wyposażenia mieszkania itp.). Wyłączaj aparat, gdy nie jest potrzebny. Wycisz się podczas rozmowy (nie włączaj np. telewizora), wycisz mikrofon, gdy nie jest to konieczne. Używanie słuchawek. Nie tolerować wejścia niechcianych uczestników, nie klikać w podejrzane linki.

10. FAKE NEWS

Nazwa mediów społecznościowych / narzędzia	**FAKE NEWS**
Informacje ogólne	Fake news, czyli potocznie dezinformacja, definiowana jest jako "artykuły informacyjne, które są celowo i weryfikowalnie fałszywe i mogą wprowadzić czytelników w błąd" (Allcott i Gentzkow, 2017, s.213) Termin "fake news" nie jest nowy. Wardle i Derakhshan (2017) rozbili termin fake news na trzy różne rodzaje. Zdefiniowali dezinformację jako "fałszywą informację udostępnianą bez szkodliwych intencji", dezinformację jako "fałszywą informację udostępnianą ze szkodliwymi intencjami" i wreszcie malinformację zdefiniowali jako "prawdziwą informację udostępnianą w celu wyrządzenia szkody" (s.5). Gdzie indziej badacze Lazer et al. (2018, s.2) zdefiniowali fake news jako "sfabrykowane informacje, które naśladują treści mediów informacyjnych w formie, ale nie w procesie organizacyjnym lub intencji". Dlatego Fake-News często odnosi się do wiadomości, które są fałszywe, ale które wydają się być uzasadnionymi wiadomościami. Internet jest powszechnym źródłem fałszywych wiadomości, przy czym fałszywe wiadomości są często promowane i rozpowszechniane w mediach społecznościowych. Fake news może dotyczyć dowolnego tematu. Na przykład, znaczna ilość fake newsów została wyprodukowana na temat koronawirusa i szczepionek.
Ryzyko związane z mediami społecznościowymi/ narzędziem: **Prywatność, dokładność, własność, dostępność, Naruszenie prawa, Prawo autorskie**	Ludzie na całym świecie są świadkami dramatycznego wzrostu dostępu do informacji i komunikacji. Podczas gdy niektórzy ludzie są głodni informacji, inni są zalewani przez treści drukowane, nadawane i cyfrowe. Ostatnie badania przeprowadzone globalnie wśród ludzi wykazały, że mają oni problem z krytycznym myśleniem o mediach i oceną ich wiarygodności, zwłaszcza w sieci. Wśród wielu kwestii, badanie sugerowało, że większość ludzi -... nie mają dobrego zrozumienia, co stanowi "fake news" a co "real news". nie potrafił odróżnić artykułów sponsorowanych od prawdziwych wiadomości. nie zadał sobie trudu, by sprawdzić, skąd pochodzą zdjęcia w sieci i ślepo zaakceptował ich kontekst. nie potrafił odróżnić prawdziwego artykułu informacyjnego od prawdziwie wyglądającego fake newsa w mediach społecznościowych. nie potrafił wskazać stronniczych treści pochodzących z niezależnych źródeł informacji wspieranych przez takie grupy jak firmy lobbingowe jako mniej wiarygodnych niż główne źródło informacji

	W obliczu licznych problemów związanych z mową nienawiści, cyberprzemocą, zhakowanymi treściami na YouTube czy fake newsami itp. jesteśmy świadkami pilnych wezwań do lepszego zarządzania środowiskiem medialnym - zwłaszcza do uregulowania internetu. Jednak w obliczu zderzenia praw pozytywnych i negatywnych, trudności regulacyjnych, potężnych globalnych firm i krótkoterminowej polityki, wezwanie to szybko zmienia się w wezwanie do rzekomo "łagodniejszego" rozwiązania, jakim jest edukacja społeczeństwa korzystającego z Internetu.
Bariery/trudności dla dorosłych	To, co martwi uczonych, to wpływ fałszywych wiadomości na percepcję społeczną powodujący, że podejmują oni rozsądne decyzje w oparciu o błędne informacje (Tandoc i in., 2018). Dzieje się tak tym bardziej, gdy użytkownicy najchętniej dzielą się negatywnymi wiadomościami, a w przypadku ostatniej pandemii pojawiło się wiele wiadomości związanych z Covid-19, które są negatywne (Nyilasy, n.d.). 374 W związku z tym Chen i in. (2011) podkreślili, że jednostki muszą być biegłe w nowych mediach, aby kompetentnie angażować się w to nowe środowisko. Najbardziej widocznym niebezpieczeństwem związanym z "fake news" jest fakt, że dewaluuje i delegitymizuje głosy ekspertów, autorytatywne instytucje i koncepcję obiektywnych danych - wszystko to podważa zdolność społeczeństwa do angażowania się w racjonalny dyskurs oparty na wspólnych faktach. Zauważono trzy dodatkowe szkody: po pierwsze, problem rosnącej fragmentacji i upolitycznienia; po drugie, promowanie "bezpiecznych wiadomości" kosztem trudnych lub wymagających historii; po trzecie, konieczność przeznaczania przez wiarygodne źródła coraz mniejszych środków na obalanie nieprawdziwych informacji (co wiąże się z kosztami finansowymi i reputacyjnymi).
Niebezpieczeństwo mediów/narzędzi społecznościowych u dorosłych	Szczególny niepokój budzi rosnąca liczba seniorów, którzy szybko przyswajają sobie media społecznościowe i stają się podatni na dezinformację. Starsi użytkownicy mogą być szczególnie narażeni na problemy związane z przyswajaniem fałszywych informacji, ale istnieją czynniki, które mają uniwersalny wpływ na wszystkie przedziały wiekowe i zdolność ludzi do odróżniania faktów od fikcji. Wiek osoby i źródło treści są ważne przy analizie rozprzestrzeniania się dezinformacji, ale czynniki te nie wyjaśniają, dlaczego niektórzy ludzie nadal wierzą w fałszywe informacje długo po tym, jak przedstawiono im korygujące je dowody. Organizacja zajmująca się sprawdzaniem faktów stwierdziła, że istnieją trzy czynniki, które kształtują zdolność każdego człowieka do nabierania się na fałszywe informacje. Pierwszym z nich jest powtarzanie - jeśli błędne stwierdzenie jest powtarzane w kółko, staje się bardziej wiarygodne. Drugim jest sposób, w jaki informacja się pojawia. Raport wykazał, że rozmiar czcionki,

	złożoność słów, kontrast i gramatyka mają wpływ na to, jak bardzo ktoś jest skłonny uwierzyć w fałszywe stwierdzenie złożone w sieci. Zdjęcia są łatwiejsze do uwierzenia jako prawdziwe, ponieważ tworzą iluzję rzeczywistego dowodu zdarzenia i są łatwe do przetworzenia. Raport podkreśla również uprzedzenia, jakie ludzie mają już przed skonsumowaniem informacji. Poglądy ludzi wpływają na sposób, w jaki nowe informacje są akceptowane, nawet jeśli dana osoba wie, że jest inaczej. Przekonania polityczne lub społeczne mogą powstrzymać ludzi przed przyjęciem informacji, pomimo ich poziomu wykształcenia lub umiejętności korzystania z mediów. Większość seniorów słyszała termin fake news i jest świadoma, że rozprzestrzenianie się dezinformacji w sieci jest problemem. Podczas gdy ludzie w każdym wieku padają ofiarą fake news, badania wykazały, że starsi dorośli są bardziej podatni na fake news i dezinformację cyfrową. Jedno z badań wykazało, że użytkownicy Facebooka w wieku 65 lat i starsi publikowali siedem razy więcej artykułów z witryn fake news niż dorośli w wieku 29 lat i młodsi.1 Starsi dorośli są również mniej skłonni do zauważenia różnicy między reklamami, które są zaprojektowane tak, aby wyglądały jak prawdziwe wiadomości, a artykułami, które są rzeczywistymi wiadomościami. Kradzież profilu - konto może zostać "skradzione", zdjęcia użytkownika mogą zostać wykorzystane gdzie indziej lub hakerzy mogą działać w jego imieniu.
Rozwiązania, które możemy mieć	Ze względu na wyżej przytoczone problemy, obszerne badania wśród seniorów, które zostały przeprowadzone w latach 2009-2019 przez Päivi Rasi, Hannę Vuojärvi i Susannę Rivinen wykazały, że interwencje powinny być oferowane seniorom z problemami zdrowotnymi (Xie, 2011b), seniorom powyżej 76 roku życia, osobom starszym z mniejszym doświadczeniem z technologią oraz populacjom mniejszościowym z niskimi umiejętnościami w zakresie alfabetyzacji zdrowotnej, którzy mieszkają w różnych krajach (Bertera, 2014; Lee & Kim, 2018; Vaportzis et al., 2017). Należy również zapewnić interwencje i usługi dla seniorów homebound, którzy są w dużym stopniu zagrożeni izolacją społeczną (Lee & Kim, 2018). Oprócz oferowania szkoleń dla osób starszych w zakresie korzystania z technologii cyfrowych i mediów (np. González et al., 2015; Taha et al., 2016; Xie & Bugg, 2009), istnieje również ogromna potrzeba opracowania większej ilości strategii mających na celu poprawę pewności siebie i samoskuteczności osób starszych w opanowaniu działań internetowych (Chu & Chu, 2010). W odniesieniu do wymiaru "rozumienia" umiejętności korzystania z mediów, interwencje dotyczące umiejętności korzystania z mediów powinny być ukierunkowane na umiejętność korzystania z mediów w zakresie zdrowia i e-zdrowia przez osoby starsze (Manafò & Wong, 2013; Xie, 2012; Young et al., 2012). Praktyczne implikacje zajmowania się zdolnościami osób starszych do tworzenia treści medialnych, w szczególności potrzeba zwrócenia uwagi na zdolność osób starszych do opowiadania osobistych i publicznych historii o swoim życiu, aby rzucić wyzwanie mainstreamowej reprezentacji ich demografii (Manchester & Facer, 2015).

	Ustawa Komisji Europejskiej o usługach cyfrowych zamierza zająć się i uczynić bezpieczniejszą powierzchnię dostawców. Każdy obywatel musi jednak dołożyć wszelkich starań, aby wykształcić odpowiednie umiejętności, które pozwolą mu uchronić się przed krzywdą. Thierry Breton, komisarz ds. rynku wewnętrznego, powiedział: "Musimy powstrzymać infodemię i rozpowszechnianie fałszywych informacji zagrażających życiu ludzi. Dezinformacja nie może pozostać źródłem dochodów. Musimy zobaczyć większe zaangażowanie ze strony platform internetowych, całego ekosystemu reklamowego i sieci podmiotów sprawdzających fakty. Ustawa o usługach cyfrowych zapewni nam dodatkowe, potężne narzędzia do walki z dezinformacją." "Umiejętności cyfrowe to coś, czego można nauczyć i to umiejętność, którą można rozwijać. Dla seniorów ważniejsze stało się nauczenie się, jak odróżnić dezinformację od prawdziwej wiadomości. Jeśli wierzyć argumentowi, że seniorzy mają więcej problemów z dostrzeganiem fałszywych wiadomości niż młodsze grupy z powodu cyfrowego analfabetyzmu, to wynika z tego, że jest to problem, który można rozwiązać poprzez edukację cyfrową. Umiejętności cyfrowe to coś, czego można się nauczyć i co można poprawić. Jednym ze sposobów na poprawę umiejętności cyfrowych jest wzięcie udziału w kursie lub webinarium na temat umiejętności cyfrowych. Kursy te uczą seniorów, jak sprawdzać fakty i dostarczają narzędzi i technik do oceny treści online. **Jakie kroki mogą podjąć seniorzy, aby nie paść ofiarą fake-news?** Jeden z seniorów stwierdził, że "teraz zdaję sobie sprawę, że fake news jest o wiele bardziej skomplikowany i podstępny niż myślałem". Fake news nie jest jednak niczym nowym; tak długo jak słowa mogły być wypowiadane lub pióro przykładane do papieru, dezinformacja pojawiała się celowo lub błędnie. Jak ujął to jeden z artykułów Guardiana: "Era post-prawdy, rzeczywiście, rozciąga się tak daleko wstecz, jak chcesz szukać, nigdy nie było złotego wieku przejrzystości". Niezależnie od tego, czy koncepcja fake news jest nowa, czy nie, konsumowanie informacji szczególnie teraz wymaga posiadania zestawu umiejętności. Szczególnie pomocne może być zastosowanie serii pytań, które mogą pomóc w ocenie nowych informacji. Pracując nad określeniem, czy coś jest prawdziwe, zadaj sobie pytanie: Kto napisał tę informację? Jakie referencje ma autor artykułu? Czy informacje są aktualne? Czy strona jest renomowana? Czy próbują sprzedać ci jakiś produkt? Czy jakaś firma lub organizacja sponsoruje stronę?

	Czy strona wspiera alternatywne lub odmienne poglądy na omawiany temat? **Inne praktyczne strategie** **Sprawdź źródło i kontekst** Czy strony internetowe to wiarygodne, czy zaufane źródła? "Dezinformacja może pochodzić z wielu miejsc - nie wystarczy unikać miejsca, w którym myślisz, że będzie. Najlepiej jest mieć filtr, przez który przechodzą wszystkie informacje" Sprawdź na przykład sufiksy stron internetowych, czy kończą się one na .gov lub .edu i są tym samym oficjalnymi stronami rządowymi lub instytucjami edukacyjnymi, odpowiednio. Senior Planet kładzie również nacisk na rozumienie kontekstu, np. rozpoznawanie satyry. Łatwo jest pomylić zabawny obrazek lub żartobliwy artykuł z prawdziwym. **Zwróć uwagę także na wizerunek** Szukaj nieregularnych kątów i/lub dziwnego oświetlenia, aby wykryć, czy zdjęcia zostały spreparowane. Ponownie, zwróć uwagę na źródło i kontekst. **Opinie a fakty** Zrozumienie rozróżnienia między opinią a faktami, zwłaszcza że każdy może publikować treści online. 'Lateral reading' - czyli sprawdzanie innych wiarygodnych źródeł w celu weryfikacji informacji w trakcie czytania - to termin po raz pierwszy użyty przez Stanford History Education Group. Kluczowe pytania, które należy zadać sobie w trakcie: "Kto stoi za tą informacją? Jakie są dowody? Co mówią inne źródła?" Biblioteki mogą również dostarczać pomocnych zasobów. Biblioteki mogą oferować wydarzenia, aby dowiedzieć się o umiejętności korzystania z mediów - a bibliotekarze są przeszkoleni, aby "parse out informacji i wszystkich szumów każdego dnia," Zatrzymaj się przed udostępnieniem lub reakcją w sieci "Wstrzymaj się, zastanów i miej więcej powściągliwości w klikaniu". Nakłonienie kogoś do większego zaangażowania w treści click-bait poprzez polubienia lub komentarze może być dla stron internetowych sposobem na generowanie przychodów. Jeśli przyjaciele lub rodzina dzielą się błędnymi informacjami online, zaoferuj zasoby sprawdzania faktów. Uważaj na boty i trolle Boty to fałszywe, zautomatyzowane konta. Rozpoznaj je, gdy zauważysz nowe konta z niewielką liczbą obserwujących, bez zdjęcia, z dziwnymi nazwami użytkowników z dużą ilością cyfr i bezsensownymi lub podżegającymi komentarzami. Boty i trolle to często osoby sprawiające kłopoty w sieci. Niezależnie od tego, czy są to boty, czy nie, zastanów się dwa razy, czy angażujesz się w sieci z kimś, kogo nie znasz. Czy jest to konieczne lub konstruktywne?

11. OSZUSTWA EMAILOWE

Nazwa mediów społecznościowych / narzędzia	**OSZUSTWA EMAILOWE**
Informacje ogólne	Poczta elektroniczna to jeden z najkorzystniejszych sposobów komunikacji z kimkolwiek. Ale jest to również podstawowe narzędzie wykorzystywane przez napastników do kradzieży pieniędzy, danych uwierzytelniających konta i wrażliwych informacji. Jeśli użytkownicy wchodzą w interakcję z oszustem e-mailowym i podają wrażliwe informacje, może to spowodować długotrwałe problemy, w tym kradzież tożsamości, straty finansowe i uszkodzenie danych. Oszustwo e-mailowe (lub oszustwo e-mailowe) to celowe wprowadzenie w błąd w celu osiągnięcia osobistych korzyści lub zaszkodzenia innej osobie za pomocą poczty elektronicznej. Niemal natychmiast po upowszechnieniu się poczty elektronicznej zaczęto ją wykorzystywać do oszukiwania ludzi. Oszustwo z wykorzystaniem poczty elektronicznej może przybrać formę "przekrętu" lub oszustwa. Oszustwa zwykle wykorzystują wrodzoną chciwość i nieuczciwość swoich ofiar. Perspektywa "okazji" lub "czegoś za darmo" może być bardzo kusząca. Oszustwa z wykorzystaniem poczty elektronicznej, podobnie jak inne "schematy bunco", są zazwyczaj wymierzone w naiwne osoby, które pokładają zaufanie w schematach mających na celu szybkie wzbogacenie się. Obejmują one inwestycje "zbyt dobre, aby mogły być prawdziwe" lub oferty sprzedaży popularnych przedmiotów po "niemożliwie niskich" cenach. Wiele osób straciło w wyniku oszustwa oszczędności swojego życia.
Ryzyko związane z mediami społecznościowymi/ narzędziem: **Prywatność, dokładność, własność, dostępność, Naruszenie prawa, Prawo autorskie**	Wiele oszustw z wykorzystaniem poczty elektronicznej istnieje już od dawna. W rzeczywistości wiele z nich to po prostu "przetworzone" oszustwa, które powstały przed użyciem poczty elektronicznej. **Oszustwa LOTERII** Otrzymujesz e-mail, w którym twierdzisz, że wygrałeś mało znaną loterię, i zawsze z ogromną wypłatą. Możesz również zostać poproszony o wpłacenie niewielkiej kwoty, aby "uwolnić" swoją wygraną. Jesteś proszony o przesłanie danych osobowych w celu weryfikacji i nagle stajesz się ofiarą oszustwa tożsamości, a wysłane pieniądze przepadają. **Oferty pracy i bogate możliwości biznesowe** Oszustwa te obiecują możliwość zarobienia dużej ilości pieniędzy przy bardzo niewielkim wysiłku. Są one zwykle pełne zachęt takich jak "Pracuj tylko godziny w tygodniu", "Bądź swoim własnym szefem", "Ustal swoje własne godziny" i "Pracuj w domu". Wiadomości e-mail oferujące te "możliwości" często mają linie tematyczne, które wyglądają jak następujące:Make a Regular Income with

	Online; Put your computer to work for you! Aukcje; Użyj Internetu do zarabiania pieniędzy; Sekrety eBay Insider Revealed 6228; Get Rich Click Otrzymujesz niechciany e-mail z ofertą pracy, zazwyczaj nie w Twojej dziedzinie, często na stanowisku tajemniczego klienta lub podobnym. Po zaakceptowaniu oferty, otrzymujesz zapłatę czekiem lub przekazem pieniężnym, na kwotę wyższą niż oferowana przez "pracodawcę". Następnie jesteś proszony o odesłanie różnicy, tylko po to, aby odkryć, że oryginalny czek lub przekaz pieniężny był fałszywy i nie masz już pieniędzy, które wysłałeś do fałszywego pracodawcy. W większości przypadków e-mail zawiera bardzo mało szczegółów na temat charakteru możliwości biznesowych. Większość podaje adres lub stronę internetową, z której można za opłatą otrzymać "zestaw informacji" na temat danej możliwości. Możliwości te jednak zazwyczaj nie są niczym więcej niż piramidami finansowymi, w których "możliwość" polega na tym, że jesteś w stanie zwerbować więcej niczego niepodejrzewających ludzi, aby kupili to oszustwo. Ostatecznie, oszustwo zostaje zdemaskowane lub pula nowych rekrutów wysycha i kończy się niepowodzeniem. **Oszustwa charytatywne** Po wielkich klęskach żywiołowych lub głośnych tragediach publicznych, oszuści próbują wykorzystać nastroje społeczne. Zakładają fałszywe strony internetowe i konta, a następnie przygotowują emocjonalne wiadomości e-mail z prośbą o fundusze, które nigdy nie trafiają do ofiar. Oszustwa te mogą być skuteczne, ponieważ grają na współczuciu i dobrej woli ludzi! **Oszustwa beneficjentów** Otrzymujesz e-mail od kogoś, kto chce szybko przenieść trochę pieniędzy. Te e-maile czasami pochodzą od osób podających się za ważnego biznesmena lub osobę funkcyjną, która twierdzi, że ma miliony do wyprowadzenia z kraju i chce twojej pomocy w zamian za część zysków. **The** Imitator Wiele oszustw imituje legalne firmy, starając się oszukać konsumentów. Najprostszym sposobem na uniknięcie tych podróbek jest nie klikanie na link wysłany w niezamówionej wiadomości e-mail. Znajdź link do firmy na własną rękę za pomocą wyszukiwarki lub, jeśli znasz adres firmy, wpisz go samodzielnie. **Oszustwa związane z naprawą komputerów** Oszustwo, które zaczyna się w świecie rzeczywistym i szybko przenosi się do świata online, otrzymujesz telefon od kogoś, kto twierdzi, że pracuje dla "Microsoftu" lub innej dużej firmy programistycznej, twierdząc, że może naprawić problemy z komputerem, takie jak powolna prędkość Internetu. Brzmi

	to pomocnie, więc kiedy e-mail dociera do Twojej skrzynki, pobierasz program zdalnego dostępu, który pozwala oszustom przejąć kontrolę nad Twoim komputerem. **"Urzędowe zawiadomienie** Oszustwa te próbują oszukać konsumentów, aby uwierzyli, że otrzymali wiadomość e-mail, która wymaga od nich podjęcia pewnych działań. Często podając się za agencje rządowe, e-maile te informują o jakimś problemie. Ten przykład został wysłany w maju, czyli w czasie, kiedy ludzie są bardziej skłonni uwierzyć, że ogłoszenie pochodzi od IRS. Tutaj masz poczuć ulgę, że IRS potwierdza, że otrzymali twoją płatność, a następnie być zaniepokojonym, że jest problem i kliknąć bez zastanowienia. **Ankieta** Oszustwa te opierają się na ludzkim pragnieniu wypowiedzenia się na temat problemów i bycia wysłuchanym w sprawach bieżących. W roku wyborczym jednym ze smaków jest sondaż dotyczący głosowania, ale każdy gorący temat może się sprawdzić: globalne ocieplenie, stosunek do wojny, postępowanie w przypadku ostatniej klęski żywiołowej i tak dalej. **Oszustwa dotyczące zdrowia i diety** Oszustwa dotyczące zdrowia i diety żerują na niepewności niektórych ludzi co do stanu ich samopoczucia. Te niepewności sprawiają, że niektórzy ludzie są szczególnie podatni na oszustwa, ponieważ mogą być niechętni lub zakłopotani, aby omówić swoje problemy z lekarzem, lub nie mogą sobie pozwolić na zakup legalnych leków lub leczenia. Oszustwa próbują zwabić konsumentów obietnicami szybkich napraw i niesamowitych rezultatów, cenami zniżkowymi, szybką dostawą, zniesieniem wymogów dotyczących recept, prywatnością i dyskretnym opakowaniem. E-mail oferujący te przedmioty będzie miał linie tematyczne, które wyglądają jak następujące: Increase Your Sexual Performance Drastically; CONTROL YOUR WEIGHT!!!; Need to lose weight for summer?; Natural Health Remedy That Works!; Reduce body fat and build lean muscle without exercise; Young at any age; Takes years off your appearance; Gives energy and burns fat; **E-mailowy koń trojański** Wiadomości e-mail zawierające konie trojańskie obiecują coś, co może zainteresować użytkownika - załącznik zawierający żart, zdjęcie lub łatę na lukę w oprogramowaniu. Jednak po otwarciu załącznik może wykonać dowolną lub wszystkie z poniższych czynności: stworzyć lukę w zabezpieczeniach Twojego komputera; otworzyć tajne "tylne drzwi", aby umożliwić napastnikowi w przyszłości nielegalny dostęp do Twojego komputera; zainstalować oprogramowanie, które rejestruje Twoje naciśnięcia klawiszy i wysyła logi do napastnika, umożliwiając mu wyłowienie Twoich haseł i innych ważnych informacji; zainstalować oprogramowanie, które monitoruje Twoje transakcje i

	działania online; zapewnić napastnikowi dostęp do Twoich plików; zmienić Twój komputer w "bota", którego napastnik może użyć do wysyłania spamu, przeprowadzania ataków typu denial-of service lub rozprzestrzeniania wirusa na inne komputery. E-maile z końmi trojańskimi przez lata pojawiały się w różnych opakowaniach. Jednym z najbardziej znanych był wirus "Love Bug", dołączony do wiadomości e-mail z tematem "I Love You", który prosił odbiorcę o obejrzenie załączonego "listu miłosnego". Inne e-maile z koniem trojańskim zawierały następujące elementy: e-mail udający wirtualną pocztówkę; ema; il masquerading as security bulletin from a software vendor requesting the recipient applying an attached "patch"; e-mail z tematem "funny" zachęcający odbiorcę do obejrzenia załączonego "dowcipu"; e-mail twierdzący, że pochodzi od producenta oprogramowania antywirusowego zachęcający odbiorcę do bezpłatnego zainstalowania załączonego "virus sweeper". **E-mail generowany przez wirusy** Należy pamiętać, że w niektórych przypadkach znany adres "od" nie zapewnia bezpieczeństwa: Wiele wirusów rozprzestrzenia się, wyszukując najpierw wszystkie adresy e-mail na zainfekowanym komputerze, a następnie wysyłając się na te adresy. Jeśli więc komputer Twojego znajomego został zainfekowany takim wirusem, możesz otrzymać wiadomość e-mail, która być może pochodzi z komputera Twojego znajomego, ale w rzeczywistości nie została przez niego napisana. Jeśli masz jakiekolwiek wątpliwości, przed otwarciem jakiegokolwiek załącznika do wiadomości e-mail sprawdź wiadomość u osoby, którą uważasz za nadawcę. Obszerną listę różnych rodzajów oszustw e-mailowych można znaleźć pod jego linkiem - https://en.wikipedia.org/wiki/Email_fraud
Bariery/trudności dla dorosłych	Podobnie jak w przypadku każdego innego rodzaju oszustwa, sprawca może spowodować znaczne szkody, zwłaszcza gdy zagrożenie utrzymuje się przez dłuższy czas. Oszustwo e-mailowe ma listę negatywnych skutków, w tym utratę pieniędzy, utratę własności intelektualnej, uszkodzenie reputacji, czasami z nieodwracalnymi reperkusjami. Chociaż osoby starsze rzadko zgłaszają, że padły ofiarą cyberprzestępstw finansowych, istnieją dowody na to, że starsi użytkownicy Internetu są narażeni na zwiększone ryzyko. W ramach szczegółowego badania sprawdzono, w jaki sposób, dlaczego i w jakich okolicznościach starsze osoby dorosłe stają się ofiarami cyberprzestępczości, a następnie ekstrapolowano to w celu rozważenia racjonalnych strategii interwencji. Według badań, do wiktymizacji prowadziły: izolacja społeczna, problemy poznawcze, fizyczne i psychiczne, status majątkowy, ograniczone umiejętności lub świadomość w zakresie cyberbezpieczeństwa, postawy społeczne i treść oszustw. Stwierdzono, że większość interwencji mających na celu zwiększenie świadomości i umiejętności

	starszych użytkowników Internetu została dotychczas wypróbowana. Inne teoretycznie możliwe interwencje obejmują: programy zarządzania przestępcami, dostosowane środki bezpieczeństwa, zmniejszenie piętna w całym społeczeństwie oraz podnoszenie świadomości wśród grup wspierających osoby starsze.
Niebezpieczeństwo mediów/narzędzi społecznościowych u dorosłych	Wyłudzanie pieniędzy od osób starszych jest ogromnym problemem na całym świecie. Oszustwa, które zaczynają się w Internecie, stają się coraz częstsze również wśród tej populacji, zwłaszcza że osoby obeznane z Internetem zaczynają się starzeć. Oszuści nie dyskryminują, jeśli chodzi o to, od kogo próbują wyciągnąć pieniądze: bogaty, biedny, czarny, biały, 65 i zdrowy, 85 i schorowany. Będą próbowali wyciągnąć pieniądze od każdego. Badania szacują, że około 5 procent populacji seniorów (co równa się około dwóch do trzech milionów osób) cierpi z powodu jakiegoś oszustwa każdego roku. "Co gorsza, jest to bardzo prawdopodobne, że to niedoszacowanie" Jest to najbardziej prawdopodobne, ponieważ oczekuje się, że duży odsetek oszustw internetowych pozostaje niezgłoszony. Oszustwa osób starszych to gigantyczny biznes, który drenuje seniorów z ich funduszy emerytalnych i świadczeń rządowych. Zwraca uwagę, że osoby starsze tracą rocznie na oszustach około 3 miliardów dolarów. Mniej ostrożne szacunki przewidują, że seniorzy tracą nawet 36 miliardów dolarów rocznie. Podaje się również, że mediana kwoty, którą stracił ktoś powyżej 80 roku życia wyniosła ponad 1000 dolarów, a mediana kwoty, którą stracił ktoś pomiędzy 70 a 79 rokiem życia wyniosła ponad 600 dolarów. **Dlaczego seniorzy padają ofiarą oszustw mailowych? Główne problemy** Zbyt wielu seniorów pada ofiarą oszustw, ale to nie ich wina. Ta populacja jest w dużej mierze godna zaufania i składa się z finansowo płodnych osób, których zdolności poznawcze mogły się zmniejszyć z powodu różnych dolegliwości. Przyjrzyjmy się cechom i powodom, dla których osoby starsze stają się podatne na działania oszustów. Oprócz tego, że seniorzy mogą być celem ataków, oszustwa te przybierają różne formy, które wykorzystują ich słabość. **Izolacja** Samotność może zniweczyć wiele aspektów życia seniora, w tym sprawić, że stanie się on wyjątkowo podatny na oszustwa. Po pierwsze, kiedy są odizolowani, nie ma nikogo, kto mógłby sprawdzić stan ich finansów. Może być zbyt późno, aby cokolwiek zrobić, jeśli ktoś bliski dowie się o tym po latach.

	Odizolowane osoby starsze mogą być również bardziej podatne na interakcje społeczne, co może sprawić, że staną się obiektem zainteresowania oszustów, którzy wykorzystują "związek", aby rozpocząć swój plan. **Sytuacja pieniężna** Sytuacja finansowa osób starszych jest głównym powodem, dla którego stają się one celem oszustw. Z jednej strony, starsza osoba może mieć miliony dolarów pod ręką po oszczędzaniu na emeryturę i otrzymywaniu comiesięcznych czeków emerytalnych i świadczeń rządowych. To może sprawić, że osoba ta będzie nieco mniej rygorystycznie podchodzić do swoich pieniędzy, co z kolei sprawi, że e-mail lub wiadomość od "wnuka" z prośbą o pieniądze nie będzie stanowić problemu. Z drugiej strony, senior może być niepewny finansowo i potrzebować źródła dochodu typu "get-rich-quick", co sprawia, że piramida finansowa staje się atrakcyjna, ale nie wie, że nigdy nie odzyska swoich pieniędzy. **Zaufanie** Według badań ludzie, którzy dorastali w latach 20-tych, 30-tych i 40-tych - czyli ci, którzy często padają ofiarą oszustów - są zazwyczaj bardziej ufni niż inne pokolenia, co czyni ich podatnymi na oszustów, którzy chcą znaleźć najbardziej podatne osobowości. **Niebezpieczeństwo** Czasami osoby starsze są po prostu zastraszane, aby przekazać pieniądze oszustom. Czy to osobiście, czy przez telefon, oszust może bezustannie naciskać na starszą osobę o pieniądze, aż ta się złamie. Dodatkowo, oszust może kierować się niepewnością osoby starszej co do jej stanu zdrowia lub statusu społecznego, mówiąc, że musi ona zapłacić określony rachunek za leczenie, bo inaczej nie będzie mogła otrzymać ubezpieczenia zdrowotnego finansowanego przez rząd. **Obniżone poznanie z wiekiem** Wraz z wiekiem, jesteśmy bardziej narażeni na jakiś rodzaj poznawczej choroby mózgu, takich jak demencja, która wpływa na pamięć i ogólne funkcje poznawcze. Te zaburzenia poznawcze mogą wpływać na Twoją pamięć na wiele sposobów, w tym na to, kim jest Twoja rodzina i ile masz pieniędzy - i co jest prawdziwe, a co fałszywe. Oszuści będą atakować te słabości. Na przykład, oszust może zadzwonić do osoby w wieku 80 lat, udając, że jest jej wnukiem. Starsza osoba może pamiętać, że ma wnuka, ale może nie pamiętać jego prawdziwych imion ani tego, jak brzmi, więc zgodzi się z tym, co mówi oszust. **Żenada** Osoby starsze mogą po prostu wstydzić się tego, że zostały oszukane, co powoduje, że nie zgłaszają tego faktu władzom. To czyni je atrakcyjnymi celami, ponieważ oszuści wiedzą, że istnieje duże prawdopodobieństwo, że nie zostaną

	złapani za próbę (lub sukces) oszukania kogoś. Co więcej, wiele starszych osób nie ma pojęcia, gdzie zgłosić oszustwo, co niestety jest korzystne dla oszustów. Mniej ostrożne szacunki przewidują, że seniorzy tracą nawet 36 miliardów dolarów rocznie. Podaje się również, że mediana kwoty, którą stracił ktoś powyżej 80 roku życia wyniosła ponad 1000 dolarów, a mediana kwoty, którą stracił ktoś pomiędzy 70 a 79 rokiem życia wyniosła ponad 600 dolarów.
Rozwiązania, które możemy mieć	Poczta elektroniczna zapewnia nam wygodne i potężne narzędzie komunikacji. Niestety, stanowi również dla oszustów i innych złośliwych osób łatwy sposób na zwabienie potencjalnych ofiar. Oszustwa, których próbują, obejmują zarówno staroświeckie operacje typu "przynęta i zamiana", jak i schematy phishingowe wykorzystujące połączenie poczty elektronicznej i fałszywych stron internetowych w celu oszukania ofiar do ujawnienia poufnych informacji. Aby chronić się przed tymi oszustwami, należy zrozumieć, czym one są, jak wyglądają, jak działają i co można zrobić, aby ich uniknąć. Poniższe podstawowe zalecenia mogą zminimalizować Twoje szanse na padnięcie ofiarą oszustwa z wykorzystaniem wiadomości e-mail: Filtrowanie spamu. Nie ufaj niezamówionej poczcie elektronicznej. Ostrożnie traktuj załączniki do wiadomości e-mail. Nie klikaj linków w wiadomościach e-mail. Zainstaluj oprogramowanie antywirusowe i aktualizuj je na bieżąco. Zainstaluj osobistą zaporę sieciową i aktualizuj ją na bieżąco. Skonfiguruj swojego klienta poczty elektronicznej pod kątem bezpieczeństwa. **Co możesz zrobić, aby nie stać się ofiarą** **Filtrowanie Spamu** Ponieważ większość oszustw e-mailowych rozpoczyna się od niezamówionej wiadomości komercyjnej, należy podjąć środki zapobiegające przedostawaniu się spamu do skrzynki pocztowej. Większość aplikacji poczty elektronicznej i usług poczty internetowej zawiera funkcje filtrowania spamu lub sposoby, dzięki którym można skonfigurować aplikacje poczty elektronicznej do filtrowania spamu. Informacje o tym, co należy zrobić, aby filtrować spam, można znaleźć w pliku pomocy aplikacji lub usługi poczty e-mail. Być może nie uda Ci się wyeliminować całego spamu, ale filtrowanie sprawi, że duża jego część nie trafi do Twojej skrzynki pocztowej. Powinieneś być świadomy, że spamerzy monitorują narzędzia i oprogramowanie do filtrowania spamu i podejmują działania, aby je ominąć. Na przykład, spamerzy mogą używać subtelnych błędów ortograficznych, aby obejść filtry spamu, zmieniając "Potency Pills" na "Potençy Pills".

Podejdź do niechcianych wiadomości e-mail z podejrzliwością

Nie ufaj automatycznie żadnej wiadomości e-mail wysłanej do Ciebie przez nieznaną osobę lub organizację. Nigdy nie otwieraj załącznika do niezamówionej wiadomości e-mail. Co najważniejsze, nigdy nie klikaj na link wysłany w wiadomości e-mail. Sprytnie spreparowane linki mogą przenieść Cię na fałszywe strony internetowe, które mają na celu wyłudzenie od Ciebie prywatnych informacji lub pobranie wirusów, programów szpiegujących i innego złośliwego oprogramowania.

Spamerzy mogą również stosować technikę, w której wysyłają unikalne linki w każdej pojedynczej wiadomości spamowej. Ofiara 1 może otrzymać wiadomość e-mail z odsyłaczem <http://dfnasdunf.example.org/>, a ofiara 2 może otrzymać tę samą wiadomość spamową z odsyłaczem <http://vnbnnasd.exaple.org/>. Obserwując, jakie odsyłacze są żądane na ich serwerach internetowych, spamerzy mogą dowiedzieć się, które adresy e-mail są ważne i precyzyjniej namierzyć ofiary do ponownych prób spamu.

Pamiętaj, że nawet e-mail wysłany ze znanego adresu może przysporzyć problemów: Wiele wirusów rozprzestrzenia się poprzez skanowanie komputera ofiary w poszukiwaniu adresów e-mail i wysyłanie się na te adresy pod pozorem wiadomości e-mail od właściciela zainfekowanego komputera.

Ostrożnie traktuj załączniki do wiadomości e-mail

Załączniki do wiadomości e-mail są powszechnie wykorzystywane przez oszustów internetowych do przemycania wirusów na Twój komputer. Wirusy te mogą pomóc oszustowi w wykradzeniu ważnych informacji z Twojego komputera, narażeniu go na dalsze ataki i nadużycia oraz przekształceniu Twojego komputera w "bota" do wykorzystania w atakach typu denial-of-service i innych przestępstwach internetowych. Jak wspomniano powyżej, znany adres "od" nie jest gwarancją bezpieczeństwa, ponieważ niektóre wirusy rozprzestrzeniają się, wyszukując najpierw wszystkie adresy e-mail na zainfekowanym komputerze, a następnie wysyłając się na te adresy. Może się zdarzyć, że komputer Twojego znajomego jest zainfekowany właśnie takim wirusem.

Użyj zdrowego rozsądku

Kiedy do Twojej skrzynki pocztowej przychodzi e-mail obiecujący Ci duże pieniądze za niewielki wysiłek, oskarżający Cię o naruszenie Patriot Act lub zapraszający Cię do przyłączenia się do spisku mającego na celu zagarnięcie nieodebranych funduszy z udziałem osób, których nie znasz, w kraju na drugim końcu świata, poświęć chwilę, aby rozważyć prawdopodobieństwo, że e-mail jest legalny.

	Zainstaluj oprogramowanie antywirusowe i aktualizuj je na bieżąco Jeśli jeszcze tego nie zrobiłeś, powinieneś zainstalować na swoim komputerze oprogramowanie antywirusowe. Jeśli to możliwe, powinieneś zainstalować program antywirusowy, który posiada funkcję automatycznej aktualizacji. Dzięki temu zawsze będziesz miał najbardziej aktualną ochronę przed wirusami. Ponadto należy upewnić się, że wybrane oprogramowanie antywirusowe zawiera funkcję skanowania poczty elektronicznej. Pomoże to utrzymać komputer wolny od wirusów przenoszonych przez pocztę elektroniczną. **Zainstaluj osobistą zaporę sieciową i aktualizuj ją na bieżąco** Zapora ogniowa nie zapobiegnie przed dostaniem się do skrzynki pocztowej wiadomości zawierającej oszustwo. Może jednak pomóc w ochronie w przypadku, gdy nieumyślnie otworzysz załącznik z wirusem lub w inny sposób wprowadzisz na swój komputer złośliwe oprogramowanie, postępując zgodnie z instrukcjami zawartymi w wiadomości. Firewall, między innymi, pomoże zapobiec ruchowi wychodzącemu z Twojego komputera do napastnika. Gdy zapora osobista wykryje podejrzane komunikaty wychodzące z Twojego komputera, może to być znak, że nieumyślnie zainstalowałeś na swoim komputerze złośliwe programy. **Poznaj zasady dotyczące poczty elektronicznej obowiązujące w organizacjach, z którymi prowadzisz interesy** Większość organizacji prowadzących działalność w Internecie ma obecnie jasne zasady dotyczące sposobu komunikowania się z klientami za pomocą poczty elektronicznej. Wiele z nich na przykład nie poprosi Cię o podanie konta lub danych osobowych za pośrednictwem poczty elektronicznej. Zrozumienie zasad obowiązujących w organizacjach, z którymi prowadzisz interesy, może pomóc Ci w wykryciu i uniknięciu phishingu i innych oszustw. Pamiętaj jednak, że wysyłanie poufnych informacji za pośrednictwem niezaszyfrowanej poczty elektronicznej nigdy nie jest dobrym pomysłem. **Skonfiguruj klienta poczty e-mail pod kątem bezpieczeństwa** Istnieje wiele sposobów na skonfigurowanie klienta poczty elektronicznej w taki sposób, abyś był mniej podatny na oszustwa. Na przykład skonfigurowanie programu pocztowego tak, aby wyświetlał wiadomości jako "tylko tekst", pomoże Ci uchronić się przed oszustwami, które nadużywają HTML w wiadomościach e-mail. **Inne sposoby ochrony przed oszustwami związanymi z wiadomościami e-mail** Zapobieganie, poprzez świadomość, jest istotnym narzędziem w walce z oszustami. Istnieje kilka przydatnych wskazówek, które pomogą Ci uniknąć oszustwa przez telefon, internet, pocztę lub w drzwiach.

	Istnieje kilka ogólnych wskazówek, które pozwolą uchronić się przed staniem się ofiarą oszustwa. Nigdy nie podawaj danych osobowych. Mogą one zostać wykorzystane do kradzieży Twojej tożsamości i uzyskania dostępu do kont. Zawsze sprawdzaj referencje każdej firmy lub prawnika, którego nie jesteś pewien. Możesz sprawdzić je na Companies House (link zewnętrzny otwiera się w nowym oknie / zakładce), aby dowiedzieć się o ich pochodzeniu lub poszukać opinii online. Nie dokonuj żadnych zaliczkowych płatności, dopóki nie upewnisz się, że firma, z którą masz do czynienia, jest legalna. Unikaj dodawania do list mailingowych, na które czasami trafiają oszuści. **Wskazówki, jak rozpoznać fałszywe e-maile** Oszuści stają się coraz bardziej przebiegli w fałszowaniu e-maili i fałszywych wiadomości, w kilku językach. Zawsze ważne jest, aby szukać oznak fałszerstwa, takich jak : Ogólne pozdrowienia Słaba jakość gramatyki, słownictwa Możliwe błędy ortograficzne Niedoskonały projekt elementów graficznych **Zadaj te pytania** Dlaczego ktoś się do mnie zbliża? Czy to coś jest zbyt dobre czy zbyt złe, by było prawdziwe? Czy naprawdę wiem, kim jest moja internetowa miłość? Czy spotkałam już swoją internetową miłość? Czy kiedykolwiek byłam z nim na połączeniu telefonicznym lub wideo? Czy wielokrotnie prosi mnie o pieniądze, powołując się na ewentualne wydatki związane z podróżą, zakupem paszportu, czy różne dramatyczne rzeczy i inne historie? **SCAM TEST - Użyj tych kroków do skanowania swoich e-maili** Wydaje się zbyt piękne, by mogło być prawdziwe Nieoczekiwanie skontaktował się z nami Zapytany o dane osobowe Pieniądze są wymagane

	PAMIĘTAJ: instytucje finansowe, przedsiębiorstwa użyteczności publicznej, organy ścigania, organy rządowe, dostawcy usług internetowych i telekomunikacyjnych lub inne organy publiczne: ➢ NIGDY nie poprosi o zapłatę w bonach. ➢ NIGDY nie poprosi Cię o przelanie pieniędzy, ponieważ Twoje konto jest zagrożone. ➢ NIGDY nie będzie grozić Ci przez telefon, listownie lub e-mailem za nieuiszczenie opłaty. ➢ NIGDY nie zagrozi aresztowaniem, jeśli płatność nie zostanie dokonana natychmiast. ➢ NIGDY nie będzie prosił o pieniądze za "darmowy prezent", "opłatę administracyjną" lub w ramach promocji. ➢ NIGDY nie poprosi o ujawnienie kodów bezpieczeństwa konta lub haseł online w całości. ➢ NIGDY nie zadzwoni znienacka i nie poprosi o zdalny dostęp do Twojego komputera lub urządzeń albo o pobranie oprogramowania. ➢ NIGDY nie poinformuje Cię o zwrotach podatkowych przez e-mail, sms lub pocztę głosową.

12. PHISHING

Nazwa mediów społecznościowych / narzędzia	**PHISHING**
Informacje ogólne	Oszustwa skierowane do seniorów to bardzo duży biznes, który okrada seniorów z ich ciężko zarobionych oszczędności, funduszy emerytalnych, a nawet świadczeń rządowych. Szkody mogą być druzgocące. Chociaż istnieje wiele metod, które cyberprzestępcy wykorzystują do wyłudzania pieniędzy od osób starszych, phishing jest jednym z najstarszych i najbardziej znanych oszustw internetowych. Phishing to rodzaj oszustwa internetowego, w którym oszuści wykorzystują pocztę elektroniczną i inne metody do kradzieży informacji osobistych, takich jak dane finansowe lub hasła do kont. Podejście to zyskało swoją niezwykłą nazwę, ponieważ wykorzystuje atrakcyjną "przynętę", aby zwabić ludzi na strony internetowe i wyłudzić ich dane pod fałszywym pretekstem. Phishing to nie to samo co spam. Podczas gdy spam to po prostu inne określenie na śmieci i niechciane reklamy, ataki phishingowe to celowe próby kradzieży informacji o użytkowniku i wykorzystania ich w szkodliwy sposób. Oszustwa typu e-mail phishing są przeprowadzane online przez zaawansowanych technicznie oszustów i przestępców zajmujących się kradzieżą tożsamości. Wykorzystują oni spam, fałszywe strony internetowe skonstruowane tak, aby wyglądały identycznie jak prawdziwe, wiadomości e-mail i komunikatory internetowe, aby podstępem zmusić Cię do ujawnienia poufnych informacji, takich jak hasła do kont bankowych i numery kart kredytowych. Gdy już złapiesz przynętę phishera, może on wykorzystać te informacje do stworzenia fałszywych kont w Twoim imieniu, zrujnowania Twojego kredytu i kradzieży Twoich pieniędzy, a nawet tożsamości.
Ryzyko związane z mediami społecznościowymi/ narzędziem: **Prywatność, dokładność, własność, dostępność, Naruszenie prawa, Prawo autorskie**	Istnieją trzy główne elementy oszustwa phishingowego: (1) Atak przeprowadzany jest za pośrednictwem komunikacji elektronicznej. Chociaż e-mail jest powszechny, phishing może być również przeprowadzony za pośrednictwem wiadomości tekstowych, kont w mediach społecznościowych, poczty głosowej, a nawet rozmów telefonicznych. (2) Wszystkie formy phishingu mają na celu przekonanie użytkownika, że fałszywy komunikat jest prawdziwy i wiarygodny. Osoba atakująca podaje się za osobę lub organizację, która jest Ci znana i godna zaufania. (3) Celem ataku phishingowego jest uzyskanie poufnych informacji osobistych, takich jak dane do logowania, dane bankowe lub numery kart kredytowych. W przypadku wszystkich ataków phishingowych oszust przekazuje starannie przygotowaną informację, która ma skłonić użytkownika do kliknięcia łącza, pobrania załącznika lub podania określonych danych osobowych.

	Niektóre popularne przykłady ataków phishingowych obejmują: **Prośba o pomoc:** Mając na celu pociągnięcie za serce, napastnik wysyła do Ciebie wiadomość e-mail, podając się za dobrego przyjaciela lub krewnego (np. Twojego wnuka). Twierdzi, że jest w trudnej sytuacji finansowej i prosi o natychmiastową pomoc. W jaki sposób cyberprzestępcy są w stanie podszywać się pod osoby, które znasz? Dzięki mediom społecznościowym oszuści mają dostęp do większej ilości naszych danych osobowych niż kiedykolwiek wcześniej. Dzięki temu mogą sprawić, że ich wiadomości będą bardzo ukierunkowane - i często bardzo wiarygodne. **Jesteś zwycięzcą nagrody głównej:** Otrzymujesz wiadomość tekstową z gratulacjami, że zostałeś zwycięzcą bardzo dużej nagrody, czy to nieodpartej oferty pakietu podróżniczego, czy też darmowych biletów na wydarzenie roku. Zostaniesz poproszony o podanie swoich danych osobowych, aby odebrać nagrodę. **Twoje konto bankowe zostało naruszone:** Otrzymujesz "pilne" powiadomienie, które wydaje się pochodzić z Twojego banku, ostrzegające o podejrzanej aktywności na Twoim koncie. Następnie użytkownik jest proszony o kliknięcie linku, który przenosi go na stronę internetową, gdzie zostanie poproszony o potwierdzenie informacji o swoim koncie bankowym. **Rząd jest za tobą**: Niewiele rzeczy w życiu jest tak szokujących, jak autorytatywnie sformułowane powiadomienie od organizacji rządowej. Oszuści wiedzą o tym, dlatego wiele wiadomości phishingowych wydaje się pochodzić od rządu. Taki e-mail ma zazwyczaj groźny ton i wspomina o dużych, przerażających karach - jeśli nie podasz żądanych przez nich płatności lub danych osobowych. Tego typu ataki phishingowe mają też swoją drugą stronę. W niektórych przypadkach są one wysyłane w sezonie podatkowym, oferując hojny zwrot pieniędzy po potwierdzeniu danych finansowych. **Dlaczego phishing działa tak dobrze?** Wiadomości e-mail, wiadomości tekstowe, wiadomości poczty głosowej, a nawet połączenia głosowe nie są uwierzytelniane. Oznacza to, że podobnie jak w przypadku kartki pocztowej wysłanej pocztą, nie ma możliwości sprawdzenia, skąd pochodzą. Daje to oszustom dużą swobodę w naśladowaniu zaufanych marek w swojej komunikacji. Phishing jest jednym z najbardziej powszechnych i wszechobecnych zagrożeń. Wyrafinowani phisherzy mają dużą wprawę w tworzeniu fałszywych szablonów wiadomości e-mail i stron internetowych, które są niemal nie do odróżnienia od prawdziwych, aż po adres URL (adres strony) i certyfikaty bezpieczeństwa. Możesz myśleć, że otrzymujesz wiarygodną wiadomość od banku, sklepu internetowego lub firmy obsługującej karty kredytowe. Jeśli nie będziesz uważał, możesz nie zauważyć podstępu, dopóki nie będzie za późno.

	Rodzaje phishingu, które musisz znać, aby pozostać bezpiecznym Phishing jest zazwyczaj przeprowadzany poprzez spoofing poczty elektronicznej, komunikatory internetowe i wiadomości tekstowe. Jest to podstępny sposób nakłaniania osób do ujawnienia danych osobowych. Jest to również forma podstępu mająca na celu pobranie do systemu złośliwego oprogramowania lub oprogramowania typu ransomware. Tak czy inaczej, sprawca uzyskuje uprzywilejowany dostęp do wrażliwych informacji. Jest to coraz bardziej frustrujące zagrożenie, ponieważ sprawcy atakują na wiele sposobów. Phishing ewoluował, aby stać się tym, czym cyberprzestępcy potrzebują, aby wykraść Twoje dane uwierzytelniające. Ich metody przybierają obecnie wiele form, a jeśli nie znasz takich terminów jak smishing, vishing, pharming i BEC, oto przewodnik: **STANDARDOWY PHISHING** Zarzucanie szerokiej sieci - W najbardziej podstawowym ujęciu, standardowy phishing to próba kradzieży poufnych informacji poprzez podawanie się za upoważnioną osobę lub organizację. Nie jest to atak ukierunkowany i może być przeprowadzany masowo. **EMAIL PHISHING** Najczęstszy scenariusz phishingu przybiera postać złośliwych wiadomości e-mail wysyłanych do osób fizycznych, naśladujących autentyczną organizację. Ten rodzaj ataku, znany również jako spam phishing, pozwala cyberprzestępcy uzyskać dostęp do dużej liczby klientów zarejestrowanych na danej stronie. E-maile phishingowe są więc często wysyłane masowo. Istnieje duże prawdopodobieństwo sukcesu, ponieważ niektóre osoby z partii często padną ofiarą. 9 **ZŁOŚLIWE OPROGRAMOWANIE PHISHING** Uważaj na makra Wykorzystując te same techniki, ten typ phishingu wprowadza paskudne błędy, przekonując użytkownika do kliknięcia linku lub pobrania załącznika dzięki czemu złośliwe oprogramowanie może zostać zainstalowane na maszynie. Jest to obecnie najczęściej stosowana forma ataku phishingowego. **SPEAR PHISHING** Złapanie dużego - Podczas gdy większość ataków phishingowych zarzuca szeroką sieć, mając nadzieję na zwabienie jak największej liczby użytkowników, którzy wezmą przynętę, spear phishing polega na intensywnym badaniu wcześniej zdefiniowanego, wysokodochodowego celu, często opierając się na publicznie dostępnych informacjach w celu uzyskania bardziej przekonującego podstępu.

	Oznacza to również technikę, w której phisher celuje w konkretną osobę lub grupę osób, a nie w ogólną bazę użytkowników. Ataki te odnoszą sukces właśnie dlatego, że są bardziej spersonalizowane. Sprawca dostosowuje e-maile z nazwiskiem odbiorcy, firmą, numerem telefonu i podobnymi informacjami, sprawiając, że cel wierzy, że ma jakieś powiązania z nadawcą. Stworzenie przekonujących e-maili spear-phishingowych zajmuje bardzo dużo czasu, ponieważ phisher musi pozyskać wiele danych z różnych źródeł. Nic więc dziwnego, że ten rodzaj złośliwego ataku jest powszechny na platformach mediów społecznościowych, takich jak LinkedIn, gdzie phisher może wykorzystać taktykę inżynierii społecznej. **SMS + PHISHING = SMISHING** Po prostu nie klikaj - phishing z wykorzystaniem wiadomości SMS wykorzystuje wiadomości tekstowe jako metodę dostarczania złośliwych linków, często w postaci krótkich kodów, aby wciągnąć użytkowników smartfonów w swoje oszustwa. Pojawienie się technologii mobilnej przyniosło niezliczone korzyści w komunikacji i bankowości internetowej. Jednocześnie otworzyło to nowe punkty styku dla pozbawionych skrupułów osób, które mogą popełniać kolejne przestępstwa. Jednym z nich jest smishing, gdzie cyberprzestępcy wabią ofiary za pomocą wiadomości tekstowych, aby: Odwiedzanie nieuczciwych stron internetowych Pobieranie złośliwych aplikacji Skontaktuj się z pomocą techniczną Czy to pod postacią kodu kuponu, czy też oferty wygrania darmowych biletów lub pieniędzy, próba smishingu najczęściej wymaga kliknięcia odsyłacza, który przekierowuje użytkownika na stronę internetową. Dość powszechne są również linki uruchamiające automatyczne pobieranie niebezpiecznych aplikacji. Choć wydają się one pochodzić z legalnych źródeł, a ich adresy URL są znane użytkownikowi, mają na celu jedynie kradzież danych osobowych lub zainstalowanie szkodliwego oprogramowania na urządzeniu mobilnym. **PHISHING W WYSZUKIWARCE** Ostrożnie z tym, co wybierasz - W tym rodzaju ataku cyberprzestępcy czekają, aż użytkownik przyjdzie do nich. Phishing w wyszukiwarkach polega na umieszczaniu fałszywych stron, często w formie płatnych reklam, w wynikach wyszukiwania dla popularnych haseł. **VISHING** Utrzymywanie Cię na linii - Vishing polega na tym, że nieuczciwy podmiot dzwoni do ofiary, podając się za przedstawiciela renomowanej organizacji i próbuje wyłudzić dane osobowe, takie jak informacje bankowe lub dotyczące karty

	kredytowej. Najczęściej rozmówca na drugiej linii brzmi jak robot, ale wraz z postępem technologicznym taktyka ta stała się trudniejsza do zidentyfikowania. **PHARMING - zatruwanie otworu wodnego** Znany również jako zatruwanie DNS, pharming jest technicznie zaawansowaną formą phishingu wykorzystującą system nazw domen internetowych (DNS). Pharming przekierowuje legalny ruch internetowy na sfałszowaną stronę bez wiedzy użytkownika, często w celu kradzieży cennych informacji. Po otwarciu złośliwej strony, linku lub załącznika, komputer jest automatycznie ładowany złośliwym oprogramowaniem, które rozprzestrzenia się na inne systemy w firmie. Aby utrwalić udany atak typu "watering hole", haker często identyfikuje strony internetowe, które użytkownik regularnie odwiedza, a także monitoruje wzorce wiadomości e-mail. W przypadku pharmingu, sprawca nie atakuje pojedynczych osób. Atak skierowany jest raczej na DNS (Domain Name System), gdzie oszust powoduje zatrucie pamięci podręcznej DNS. W ten sposób zmienia się adres IP powiązany z nazwą strony internetowej, więc nawet jeśli użytkownik wprowadzi poprawną nazwę strony, oszust może przekierować go na złośliwą stronę. Chociaż jest to mniej rozpowszechnione, atakowanie serwera DNS może narazić na szwank miliony żądań URL kierowanych przez użytkowników sieci. **CLONE PHISHING** W tego typu atakach podejrzany aktor dokonuje zmian w istniejącej wiadomości e-mail, w wyniku czego powstaje niemal identyczna (sklonowana) wiadomość, ale z legalnym linkiem, załącznikiem lub innym elementem zamienionym na złośliwy. Ataki te nie mogą się rozpocząć bez wcześniejszego wprowadzenia przez atakującego Dlatego dobrą obroną jest stosowanie silnych, unikalnych haseł w połączeniu z dwuskładnikowym uwierzytelnianiem. **MAN-IN-THE-MIDDLE** The Public WiFi Phisherman - Atak man-in-the-middle polega na tym, że podsłuchiwacz monitoruje korespondencję pomiędzy dwoma niczego nie podejrzewającymi stronami. Kiedy odbywa się to w celu kradzieży danych uwierzytelniających lub innych wrażliwych informacji, staje się atakiem phishingowym man-in-the-middle. Ataki te są często przeprowadzane poprzez tworzenie fałszywych publicznych sieci WiFi w kawiarniach, centrach handlowych i innych miejscach publicznych. Po podłączeniu się do nich, człowiek w środku może wyłudzać informacje lub wpychać złośliwe oprogramowanie na urządzenia **MALWARIA** Ta reklama nie jest tym, czym myślisz, że jest - Ten rodzaj phishingu wykorzystuje luki w oprogramowaniu reklamowym lub animacyjnym do kradzieży informacji od użytkowników. Malvertising jest zwykle osadzony w normalnie wyglądających

	reklamach - umieszczonych na legalnych stronach internetowych, takich jak Yahoo.com - ale z wszczepionym złośliwym kodem. **SPOOFING DOMENY** Drugi rodzaj phishingu e-mailowego występuje w postaci spoofingu domenowego, gdzie sprawca podszywa się pod nazwę domeny znanej organizacji. Technika ta sprawia, że użytkownik ma wrażenie, że otrzymuje wiadomość e-mail od legalnej firmy. Adresy e-mail są unikalne, więc phisher może jedynie naśladować adres organizacji. Robi to poprzez użycie substytucji znaków, takich jak "r" i "n" razem dla "rn" zamiast "m". W przeciwnym razie używają nazwy organizacji z inną domeną, w nadziei, że w skrzynce odbiorczej odbiorcy pojawi się tylko lokalna część adresu e-mail. Oszust domeny może również stworzyć fałszywą stronę internetową, która wygląda jak prawdziwa. Replikowałaby ona wygląd prawdziwej strony. Po raz kolejny nacisk położony jest na wyrażenie "wygląda jak". Podczas gdy fałszywa domena może być podobna, nie jest identyczna z oryginalną stroną internetową. **EVIL TWIN** Punkty dostępu WI-FI są odwiedzane przez hordy osób szukających szybkich połączeń bezprzewodowych do surfowania po sieci i wykonywania innych czynności związanych z internetem. Haker w tym scenariuszu replikuje hotspot WI-FI za pomocą fałszywki. Kiedy użytkownicy łączą się, jest wtedy w stanie podsłuchać ich ruch sieciowy. Atakujący kradnie nazwy kont i hasła. Phisher jest również w stanie zobaczyć wszystkie załączniki, do których użytkownik uzyskuje dostęp podczas przebywania w skompromitowanej sieci. Podatne na ataki punkty dostępu WI-FI znajdują się w kawiarniach, na lotniskach, w centrach handlowych, szpitalach i innych publicznych punktach dostępu. **Prawdziwe przykłady ataków phishingowych** Według ostatnich badań przeprowadzonych przez Google, w okresie od stycznia do marca 2020 roku nastąpił wzrost o 3505 stron internetowych typu phishing. Inne badanie przeprowadzone przez Check Point Research ujawniło, że 64% przedsiębiorstw w ciągu ostatniego roku padło ofiarą ataków phishingowych. Kolejne ustalenia Verizon potwierdziły, że phishing jest zaangażowany w 78% incydentów cyberszpiegostwa. Oto pięć najbardziej godnych uwagi przykładów: Atak na wieloryby prowadzi do zwolnienia szefa FACC W 2016 roku austriacka firma lotnicza FACC była przedmiotem jednego z najgłośniejszych w historii ataków typu Whaling, nazwanego Fake President Incident, w którym napastnik uciekł z 56 milionami dolarów. W klasycznym ataku whalingowym sprawca podszył się pod prezesa firmy i wysyłając e-mail do pracownika działu finansowego zażądał natychmiastowego transferu środków. Atak kosztował firmę nie tylko straty finansowe, ale także stanowisko ówczesnego prezesa Waltera Stephana. Choć szczegóły nie zostały ujawnione, zwolnienie nastąpiło z powodu naruszenia obowiązków.

	Spear Phishing skierowany do Ubiquiti Networks Inc. W czerwcu 2015 roku amerykańska firma zajmująca się technologiami sieciowymi Ubiquiti Networks stała się celem kampanii e-mailowej typu spear-fishing. Atakujący podszywał się pod wyższe rangą kierownictwo z zagranicznego oddziału firmy za pomocą spoofedowanych adresów e-mail i podróbek domen. Pracownicy dali się nabrać na to, że otrzymują od urzędników firmy uzasadnione prośby o przelanie środków na bezpieczne konto. Firma Ubiquiti Networks nie była świadoma, że została oszukana, dopóki nie została powiadomiona o tej działalności przez FBI.Nie ucierpiała w wyniku kompromisu w swoich systemach, ale straciła 46,7 miliona dolarów w przelanych funduszach. **Oszustwo z fakturami na Facebooku i Google** W latach 2013-2015, amerykańskie behemoty Facebook i Google zostały podobno wyłudzone 100 milionów dolarów w ramach skomplikowanego schematu oszustwa przewodowego. Sprawca założył fałszywą firmę podszywając się pod tajwańską firmę Quanta Computer. Ta ostatnia regularnie przeprowadzała wielomilionowe transakcje z firmami social media, a w ciągu dwóch lat napastnik wysyłał e-maile phishingowe ze sfałszowanymi fakturami, które miały być wpłacane na fałszywe konta bankowe. Schemat unikał podejrzeń przez tak długi czas, tworząc fałszywe dokumenty potwierdzające transakcje i sfałszowane pieczęcie korporacyjne. Napastnik został później zidentyfikowany jako Litwin Evaldas Rimasauskas, który otrzymał pięcioletni wyrok więzienia po aresztowaniu w 2017 roku. **Smishing Apple** W 2020 roku jedna z największych firm produkujących smartfony na świecie, Apple, stała się podobno celem kampanii smishingowej. Za pomocą fałszywego czatu Apple, wiadomości informowały użytkowników, że wygrali szansę na udział w programie testowania nowego iPhone'a 12 przez Apple w 2020 roku. Odbiorcy zostali poproszeni o uiszczenie opłaty za dostawę. Przekierowując na złośliwą stronę internetową, napastnicy porywali dane uwierzytelniające karty płatnicze ofiar. Ludzie przechowują obecnie wiele wrażliwych informacji na swoich smartfonach, a powszechne korzystanie z iPhone'ów i iPadów sprawiło, że stały się one powtarzającymi się celami dla schematów phishingu SMS. Atakujący regularnie wysyłają wiadomości do użytkowników. Wiadomości te będą zawierać link, który należy kliknąć, aby odblokować zamrożone konto Apple ID lub zapobiec jego wygaśnięciu z przyszłych wiadomości tego typu. Inni będą wabić użytkowników pomysłem, że zagubiony iPhone został odnaleziony. Ofiary są oszukiwane z ich danych logowania, a hakerzy uzyskują dostęp do ich mediów, dokumentów i innych informacji przechowywanych na urządzeniu. Jako stałe zagrożenie, kwota utracona podczas udanych prób dodaje się do statystyk rocznych strat związanych z cyberprzestępczością. Nawet jeśli nie wszyscy padają ofiarą, atakujący zarabia znaczące nagrody dla małego procentu ludzi, którzy nie byli mądrzejsi.

	Naruszenie bezpieczeństwa RSA Aby uzyskać dostęp do systemu sieciowego popularnej firmy zajmującej się cyberbezpieczeństwem, wystarczyła wiadomość e-mail z tematem "Plan rekrutacji na rok 2011". W e-mailu znajdował się zainfekowany wirusem plik Excel, który po otwarciu przez nieświadomego pracownika dawał napastnikowi dostęp do prywatnych haseł. To doskonały przykład ataku phishingowego typu "watering hole". Jak na ironię, RSA świadczy usługi z zakresu cyberbezpieczeństwa dla kilku oddziałów rządu USA i innych przedsiębiorstw biznesowych. To naruszenie dało hakerom dostęp do sieci departamentów rządowych USA, stając się Advanced Persistent Threat. Obejrzyj ten film https://www.youtube.com/watch?v=4AcROYO8BLA
Bariery/trudności dla dorosłych	Wiadomości e-mail, wiadomości tekstowe, wiadomości poczty głosowej, a nawet połączenia głosowe nie są uwierzytelniane. Oznacza to, że podobnie jak w przypadku kartki pocztowej wysłanej pocztą, nie ma prawdziwego sposobu na sprawdzenie, skąd pochodzą. Daje to oszustom dużą swobodę w naśladowaniu zaufanych marek w swojej komunikacji. Phishing jest jednym z najbardziej powszechnych i wszechobecnych zagrożeń. Wyrafinowani phisherzy mają dużą wprawę w tworzeniu fałszywych szablonów wiadomości e-mail i stron internetowych, które są niemal nie do odróżnienia od prawdziwych, aż po adres URL (adres strony) i certyfikaty bezpieczeństwa. Możesz myśleć, że otrzymujesz wiarygodną wiadomość od banku, sklepu internetowego lub firmy obsługującej karty kredytowe. Jeśli nie zwracasz uwagi, możesz nie zauważyć podstępu, dopóki nie będzie za późno.
Niebezpieczeństwo mediów/narzędzi społecznościowych u dorosłych	Według Wikipedii, phishing to nieuczciwa próba uzyskania poufnych danych poprzez podszywanie się pod godny zaufania podmiot. Podobnie jak w przypadku każdego innego rodzaju oszustwa, sprawca może spowodować znaczne szkody, zwłaszcza gdy zagrożenie utrzymuje się przez dłuższy czas. 11 Podobnie jak w przypadku każdego innego rodzaju oszustwa, sprawca może spowodować znaczne szkody, zwłaszcza gdy zagrożenie utrzymuje się przez dłuższy czas. Oszustwo e-mailowe ma listę negatywnych skutków, w tym utratę pieniędzy, utratę własności intelektualnej, uszkodzenie reputacji, czasami z nieodwracalnymi reperkusjami. Chociaż osoby starsze rzadko zgłaszają, że padły ofiarą cyberprzestępstw finansowych, istnieją dowody na to, że starsi użytkownicy sieci są narażeni na zwiększone ryzyko. Według badań, do wiktymizacji doprowadziły: izolacja społeczna, problemy poznawcze, fizyczne i psychiczne; status majątkowy,

	ograniczone umiejętności lub świadomość w zakresie cyberbezpieczeństwa, postawy społeczne i treść oszustw. Straty finansowe starszych ofiar były prawie dwukrotnie wyższe w przypadku jednego oszustwa niż w przypadku młodszych ofiar Należy jednak zauważyć, że straty finansowe starszych ofiar (osób w wieku 55 lat i starszych) były prawdopodobnie prawie dwukrotnie wyższe w przypadku jednego oszustwa niż w przypadku młodszych grup wiekowych. Można również przypuszczać, że dla wielu starszych osób o stałych dochodach (które nie mają łatwych sposobów na przykład na gromadzenie nowych oszczędności) zastąpienie pieniędzy utraconych w wyniku oszustwa będzie prawdopodobnie trudniejsze niż dla osób w wieku produkcyjnym. Prawie połowa (49 procent) wszystkich osób w wieku 75 lat i starszych mieszka samotnie, a 17 procent osób starszych utrzymuje mniej niż tygodniowy kontakt z rodziną, przyjaciółmi i sąsiadami. Osoby, które są bardziej odizolowane społecznie, mogą być bardziej narażone na oszustwa, na przykład jeśli mają mało okazji do omówienia spraw z innymi. **Jak seniorzy padają ofiarą phishingu?** Wyłudzanie pieniędzy od osób starszych jest ogromnym problemem na całym świecie. Oszustwa, które zaczynają się w Internecie, stają się coraz częstsze również wśród tej populacji, zwłaszcza że osoby obeznane z Internetem zaczynają się starzeć. **Jeśli odpowiedziałeś na oszustwo phishingowe, napastnik może ewentualnie:** Porwanie nazw użytkowników i haseł Kradnie twoje pieniądze i otwiera karty kredytowe oraz konta bankowe na twoje nazwisko Zamówienie nowych numerów identyfikacyjnych (PIN) lub dodatkowych kart kredytowych Dokonaj zakupów Dodaj siebie lub alias, który kontroluje jako autoryzowanego użytkownika, aby łatwiej było korzystać z kredytu Uzyskanie zaliczek gotówkowych Używanie i nadużywanie numeru Social Security Sprzedawać informacje o użytkowniku innym podmiotom, które wykorzystają je do niedozwolonych lub nielegalnych celów Jak oszustwo phishingowe mnie znalazło? Ten rodzaj kradzieży tożsamości jest niezwykle rozpowszechniony ze względu na łatwość, z jaką niczego nie podejrzewający ludzie dzielą się informacjami osobistymi. Oszustwa phishingowe często wabią Cię spamem i wiadomościami błyskawicznymi z prośbą o "weryfikację konta" lub "potwierdzenie adresu do

	faktury" za pośrednictwem złośliwej strony internetowej. Bądź bardzo ostrożny. Phisherzy mogą Cię znaleźć tylko wtedy, gdy odpowiesz. **Skąd będę wiedział, że zostałem oszukany?** Phisherzy często podszywają się pod legalne firmy. Ich wiadomości mogą brzmieć autentycznie, a witryny mogą wyglądać bardzo podobnie do prawdziwych. Może być trudno to odróżnić, ale możesz mieć do czynienia z oszustwem phishingowym, jeśli zauważysz następujące elementy: Prośby o poufne informacje za pośrednictwem poczty elektronicznej lub komunikatorów internetowych Język emocjonalny wykorzystujący taktykę straszenia lub pilne prośby o odpowiedź Błędne adresy URL, błędy ortograficzne lub używanie subdomen Linki w treści wiadomości Brak osobistego powitania lub spersonalizowanych informacji w wiadomości. Legalne wiadomości e-mail od banków i firm obsługujących karty kredytowe często zawierają częściowe numery kont, nazwę użytkownika lub hasło. **Skutk**i **Strata pieniędzy** Z każdego incydentu phishingowego, który miał miejsce w historii, jednym stałym efektem są straty finansowe. Straty finansowe doświadczane przez indywidualnych konsumentów szacuje się na ponad 9 miliardów funtów rocznie. Jednakże, chociaż dane te są użytecznymi wskaźnikami, prawdopodobnie znacznie zaniżają skalę strat finansowych poniesionych przez osoby fizyczne, ponieważ nie wydaje się, aby obejmowały one wszystkie rodzaje oszustw, a jak wskazano, wiele przestępstw związanych z oszustwami nie jest zgłaszanych. Co mylące, liczba 3,5 mld funtów jest również często określana jako szacunek całkowitych strat finansowych, których ludzie doświadczyli w wyniku oszustw lub wyłudzeń. **Inne skutki** Ogólnie rzecz biorąc, inne skutki oszustwa dla ofiar mogą się różnić w zależności od indywidualnej sytuacji danej osoby oraz jej istniejących zasobów i możliwości, ale nigdy nie należy lekceważyć powagi potencjalnego wpływu. Skutki psychologiczne mogą być poważne i wyniszczające, w tym stres, złość, utrata poczucia własnej wartości, wstyd i zdenerwowanie. Negatywny wpływ nadużyć finansowych, niezależnie od ich źródła, może spowodować, że ktoś stanie się potrzebujący wsparcia ze strony służb socjalnych, nie potrzebując wcześniej takiej pomocy. Badanie dotyczące przestępczości

	domowej wykazało, że stan zdrowia ofiar spada szybciej niż osób nie będących ofiarami w podobnym wieku Analiza skutków przestępczości domowej wykazała, że: 40 procent ofiar stwierdziło, że spowodowało to u nich ogólny spadek zaufania. 28 proc. stwierdziło, że wywołało to u nich uczucie przygnębienia lub depresji. 46 procent stwierdziło, że spowodowało to u nich straty finansowe. 16 procent nie powiedziało nikomu o przestępstwie, a 40 procent z nich podało jako powód wstyd. Ofiary to często osoby znajdujące się w trudnej sytuacji, które mogą mieć problemy finansowe, są starsze lub odizolowane społecznie. Osobiste skutki dla nich i ich rodzin są często niszczące, jeśli chodzi o przyszły spokój ducha i zdrowie. Ofiary mogą mieć zniszczoną samoocenę i obniżone poczucie własnej wartości. Ofiary cierpią z powodu stresu, niepokoju i depresji. Życie może być zrujnowane". Prawie połowa (49 procent) wszystkich osób w wieku 75 lat i starszych mieszka samotnie, a 17 procent osób starszych utrzymuje mniej niż tygodniowy kontakt z rodziną, przyjaciółmi i sąsiadami. Osoby, które są bardziej odizolowane społecznie, mogą być bardziej podatne na oszustwa, jeśli na przykład mają mało okazji do omówienia spraw z innymi. Jak seniorzy padają ofiarą phishingu?
Rozwiązania, które możemy mieć	Najlepszą obroną przed oszustwem phishingowym jest weryfikacja osoby lub organizacji, która wysłała e-mail lub wiadomość przed kliknięciem na cokolwiek. **Jak można się chronić przed phishingiem?** Gdy uzbroisz się w informacje i zasoby, będziesz mądrzejszy o zagrożenia bezpieczeństwa komputerowego i mniej podatny na taktykę oszustw phishingowych. Podejmij te kroki, aby wzmocnić bezpieczeństwo swojego komputera i od razu uzyskać lepszą ochronę przed phishingiem: Nie podawaj danych osobowych na wszelkie niezamówione prośby o informacje Podawaj dane osobowe tylko na stronach, które mają "https" w adresie internetowym lub mają ikonę kłódki na dole przeglądarki Jeśli podejrzewasz, że otrzymałeś przynętę phishingową, skontaktuj się telefonicznie z firmą, której dotyczy e-mail, aby sprawdzić, czy wiadomość jest prawdziwa Wpisz zaufany adres URL witryny firmy w pasku adresu przeglądarki, aby ominąć link w podejrzanej wiadomości phishingowej Używaj zróżnicowanych i złożonych haseł do wszystkich swoich kont Stale sprawdzać dokładność kont osobistych i od razu zajmować się wszelkimi rozbieżnościami Unikaj wątpliwych stron internetowych Praktykuj bezpieczny protokół poczty elektronicznej:

	Nie otwieraj wiadomości od nieznanych nadawców Natychmiast usuwaj wiadomości, które podejrzewasz o bycie spamem **Upewnij się, że masz zainstalowane najlepsze oprogramowanie zabezpieczające na swoim komputerze, aby uzyskać lepszą ochronę przed phishingiem:** Używaj ochrony oprogramowania antywirusowego i zapory sieciowej Uzyskaj ochronę przed oprogramowaniem antyspyware Niezabezpieczony komputer jest jak otwarte drzwi dla oszustw typu phishing z wykorzystaniem poczty elektronicznej. Aby uzyskać silniejszą formę ochrony, użyj filtra antyspamowego lub bramy do skanowania przychodzących wiadomości. Produkty te udaremniają niebezpieczne złośliwe oprogramowanie, zanim dostanie się ono do komputera, stoją na straży każdego możliwego wejścia do komputera i odpierają wszelkie programy szpiegowskie i wirusy, które próbują się do niego dostać, nawet te najbardziej szkodliwe i przebiegłe. Mimo że dostępne są darmowe programy antyszpiegowskie i antywirusowe, nie nadążają one za ciągłym napływem nowych szczepów oprogramowania szpiegowskiego. Wcześniej niewykryte formy oprogramowania szpiegowskiego mogą często wyrządzić największe szkody, dlatego tak ważne jest posiadanie aktualnej, gwarantowanej ochrony. **Porównaj i znajdź najlepsze oprogramowanie chroniące przed wyłudzaniem informacji** Oszuści internetowi próbują podstępem zmusić Cię do podania haseł lub innych danych osobowych, podszywając się pod legalne strony internetowe. Często działają one nawet tak samo jak strony, na których regularnie się logujesz. Takich zagrożeń można łatwo uniknąć, stosując program antywirusowy. Z przyjemnością pokażemy Ci, które z nich zapewniają najlepszą ochronę przed atakami typu phishing, nie wpływając na wydajność komputera i nie przeszkadzając w pracy. **Jakie jest najlepsze rozwiązanie antywirusowe?** Bitdefender, marka antywirusowa, której zaufało ponad 500 milionów użytkowników w 150 krajach, jest jednym z wiodących na świecie dostawców konsumenckich produktów cyberbezpieczeństwa i pionierem w dziedzinie ochrony antywirusowej. Marka ta zdobyła wiele nagród antywirusowych od wiodących laboratoriów testowych online, w tym AV-Comparatives, AV-Test, PCMag i The Anti-Malware Testing Standard Organization. Usługa przeciwdziałania Netcraft pomaga organizacjom w zwalczaniu tych technik. Po wykryciu witryny phishingowej, Netcraft natychmiast reaguje zestawem działań, które w znacznym stopniu ograniczą dostęp do witryny, a ostatecznie spowodują wyeliminowanie oszukańczych treści. Podejście Netcraft do usuwania stron phishingowych wyróżnia się spośród innych dostawców usług takedown dzięki możliwości natychmiastowego zablokowania dostępu do strony dla użytkowników szerokiego zakresu technologii.

	Najlepsze programy antyphishingowe Oszuści internetowi próbują podstępem zmusić Cię do podania haseł lub innych danych osobowych, podszywając się pod legalne strony internetowe. Często działają one nawet tak samo jak strony, na których regularnie się logujesz. Takich zagrożeń można łatwo uniknąć, stosując program antywirusowy. Z przyjemnością pokażemy Ci, które z nich zapewniają najlepszą ochronę przed atakami typu phishing, nie wpływając na wydajność komputera i nie przeszkadzając w pracy. **Zweryfikowane certyfikaty znaków?** Certyfikaty Verified Mark (VMC) pozwalają na umieszczenie Twojego logo obok pola "nadawcy" w klientach poczty elektronicznej, dzięki czemu użytkownicy widzą Twój znak - i to, że Twoja organizacja została uwierzytelniona - jeszcze zanim otworzą wiadomość. Jest to odpowiednik znaku jakości w mediach społecznościowych, z dodatkową walidacją i wymogami bezpieczeństwa, które pomogą chronić Twoich klientów i Twoją markę przed atakami typu phishing i spoofing. Weryfikacja logo jest częścią przełomowej inicjatywy - realizowanej we współpracy z Brand Indicators for Message Identification (BIMI) i dostawcami klientów poczty elektronicznej - mającej na celu promowanie spójnych, zaufanych i wizualnie autentycznych wiadomości e-mail zarówno dla firm, jak i konsumentów. Oto jak to działa: (obejrzyj film) https://www.digicert.com/content/dam/digicert/videos/digicert-vmc-product-reveal.mp4 **JAK CHRONIĆ SIĘ PRZED ATAKAMI TYPU PHISHING** Ochrona przed atakami phishingowymi zaczyna się od wiedzy o tym, co tam jest. Nigdy nie klikaj w linki od nieznanych nadawców lub jeśli jakiś szczegół dotyczący wymiany wzbudził podejrzenia. iedy tylko jest to możliwe, najedź kursorem na link, aby upewnić się, że miejsce docelowe odpowiada Twoim oczekiwaniom. Zauważ, że nie będzie to działać na urządzeniach mobilnych lub jeśli używane są krótkie kody, więc bądź wyjątkowo ostrożny na urządzeniach mobilnych. Jeśli podejrzewasz, że wiadomość e-mail jest próbą phishingu, sprawdź dwukrotnie nazwę nadawcy, specyfikę pozdrowienia oraz stopkę, w której znajduje się adres fizyczny i przycisk rezygnacji z subskrypcji. Jeśli masz wątpliwości, usuń. Jeśli nie jesteś pewien, czy komunikat jest uzasadniony, spróbuj skontaktować się z marką lub usługą za pośrednictwem innego kanału (na przykład ich strony internetowej lub dzwoniąc na linię obsługi klienta). Unikaj wprowadzania informacji umożliwiających identyfikację osoby, chyba że masz ogromną pewność co do tożsamości strony, z którą się komunikujesz. Zamykanie wszystkich luk w zabezpieczeniach Podczas gdy zachowanie czujności trzyma większość napastników na dystans, nikt nie może być w 100% bezpieczny w pojedynkę. W końcu phishing istnieje dziś tylko dlatego, że działa. Dlatego tak

	ważne jest połączenie szkolenia w zakresie świadomości bezpieczeństwa z wysokiej jakości ochroną punktów końcowych w przedsiębiorstwach - z inteligentną inteligencją zagrożeń, aktualizacjami w chmurze i ochroną antyphishingową-DNS w czasie rzeczywistym oraz niezawodnym tworzeniem kopii zapasowych danych. **Aby zapobiec oszustwom wśród seniorów** Jeśli obawiasz się oszustwa, możesz zrobić wiele, aby zapobiec jego wystąpieniu : Ustaw monitoring kredytowy i ochronę przed kradzieżą tożsamości - Przestępcy prawie zawsze popełniają oszustwa wobec osób starszych w celu wyłudzenia pieniędzy. Najprostszym sposobem ochrony finansów własnych lub bliskiej osoby jest zapisanie się na monitoring kredytowy. **Dalsze kroki, które należy podjąć:** **STOP:** Weź oddech i zastanów się nad sytuacją. Czy coś wydaje się podejrzane? **ODEJDŹ:** Odłóż słuchawkę, zamknij drzwi lub zamknij wiadomość e-mail. Jeśli ktoś naciska na Ciebie, abyś działał teraz, może to być oszust. **ZAPYTAJ:** Zadzwoń do członka rodziny po poradę, poszukaj w Internecie więcej szczegółów i dowiedz się, czy organizacje są prawdziwe. Możesz też poprosić gościa o identyfikację. **OCZEKIWANIE:** Poświęć czas na przyswojenie tego, czego się dowiedziałeś i ułóż plan działania. Nie spiesz się z żadnymi decyzjami. **DZIAŁAJ:** Odwiedzaj tylko legalne strony internetowe i dzwoń na sprawdzone, bezpieczne numery telefonów. Możesz skorzystać z niezależnych stron internetowych z recenzjami i usług wyszukiwania adresów e-mail, aby sprawdzić czyjąś tożsamość. Podziel się swoimi historiami o próbach oszustwa. Poproś bardziej obeznanych z technologią członków rodziny, aby podzielili się przykładami fałszywych e-maili lub wiadomości, które otrzymali. Miej plan i hasło - wczesne udostępnienie szczegółów dotyczących konta bankowego może zapewnić, że pieniądze Twojej rodziny pozostaną bezpieczne. Bądź podejrzliwy wobec każdego niezamówionego telefonu lub wiadomości - odrobina podejrzliwości może zaoszczędzić Ci wiele bólu serca. Wiedz, że takie oszustwa istnieją i zawsze zadawaj sobie pytanie "co by było, gdyby?", gdy zetkniesz się z nietypową prośbą o pieniądze czy to online, czy osobiście.

13. FACEBOOK

Nazwa mediów społecznościowych / narzędzia	**FACEBOOK**
Informacje ogólne	Facebook jest amerykańskim internetowym serwisem społecznościowym i społecznościowym należącym do Meta Platforms. Założony w 2004 roku, jego nazwa pochodzi od katalogów face book (https://en.wikipedia.org/wiki/Face_book) często wręczanych studentom amerykańskich uczelni. Na początku członkostwo było ograniczone tylko do studentów Harvardu. Od 2006 roku był dostępny dla każdego, kto ukończył 13 lat. W był najczęściej pobieraną aplikacją mobilną. W tej chwili dostęp do Facebooka możliwy jest z różnego rodzaju urządzeń wyposażonych w łączność internetową. Bez problemu można z niego korzystać na komputerach osobistych, tabletach i smartfonach. Aby korzystać z aplikacji, należy być zarejestrowanym użytkownikiem, czyli stworzyć profil ujawniający informacje o sobie. Po tym procesie możesz tworzyć posty tekstowe, w tym zdjęcia i multimedia, możesz dzielić się nimi z innymi użytkownikami, którzy zgodzili się zostać Twoimi "przyjaciółmi". Facebook pozwala na dostosowanie różnych ustawień prywatności, albo Twój profil jest dostępny publicznie, albo jest dostępny tylko dla użytkowników. Aplikacja Facebook pozwala również na komunikację między użytkownikami za pomocą Facebook Messenger. Możesz prowadzić prywatne rozmowy, ale także możesz dołączyć do tworzenia grup lub dołączyć do grup wspólnych zainteresowań.
Ryzyko związane z mediami społecznościowymi / narzędziem: **Prywatność, dokładność, nieruchomość, dostępność, Naruszenie przepisów prawa, Copyright**	Facebook często był krytykowany za kwestie takie jak prywatność użytkowników, masowy nadzór, psychologiczne efekty manipulacji politycznej, takie jak uzależnienie i niska samoocena, oraz treści takie jak fake news, teorie spiskowe, naruszenie praw autorskich i mowa nienawiści. ***Prywatność:*** Na stronie FB można znaleźć bezpośredni link do zasad prywatności: https://www.facebook.com/privacy/policy ***Dokładność:*** https://www.facebook.com/policies_center/ads ***Własność:*** Facebook uważa za swój obowiązek pomagać osobom fizycznym i organizacjom w ochronie ich praw własności intelektualnej. Regulamin serwisu Facebook zabrania użytkownikom zamieszczania treści naruszających prawa własności intelektualnej innych osób, w tym prawa autorskie i prawa do znaków towarowych.

	Copyright Prawa autorskie to ustawowe prawa, które chronią oryginalne dzieła autorskie, takie jak książki, utwory muzyczne, filmy i dzieła sztuki. Ogólnie rzecz biorąc, prawa autorskie chronią oryginalne formy wyrazu, takie jak wypowiedzi lub obrazy. Nie chronią one faktów ani idei, ale mogą chronić oryginalne wypowiedzi lub obrazy opisujące daną ideę. Prawo autorskie nie chroni również nazw, tytułów czy sloganów. Ich ochrona jest zapewniona przez prawo o znakach towarowych. ***Znaki towarowe*** Znak towarowy to słowo, slogan, symbol lub wzór (np. nazwa marki lub logo), które odróżniają produkty i usługi oferowane przez dany podmiot, grupę lub przedsiębiorstwo od tych oferowanych przez inne podmioty, grupy lub przedsiębiorstwa. Ogólną funkcją prawa znaków towarowych jest pomoc konsumentom w rozpoznaniu, jaki podmiot jest odpowiedzialny za dany produkt lub usługę. https://www.facebook.com/help/399224883474207/?helpref=uf_share ***Dostępność:*** Facebook zapewnia wygodne doświadczenia wszystkim użytkownikom. Dostępne są funkcje i technologie, które pomagają osobom niepełnosprawnym, takim jak osoby z wadami wzroku i słuchu, w jak największym stopniu korzystać z Facebooka. ***Naruszenie przepisów prawa:*** Instytucje państwowe mogą uznać, że treści publikowane przez użytkownika na Facebooku naruszają prawo lokalne, mogą wystąpić o ograniczenie tych treści. W przypadku publikowania treści niezgodnych z lokalnymi przepisami, sąd może nakazać ograniczenie publikacji tych treści lub zgłosić zarzuty, że treści te są niezgodne z prawem, od instytucji pozarządowych i członków społeczeństwa. Zgłoszenia są weryfikowane zgodnie ze zobowiązaniami Global Network Initiative oraz zasadami korporacyjnymi dotyczącymi ochrony praw człowieka. https://transparency.fb.com/data/content-restrictions/content-violating-local-law/ ***Copyright:*** Przepisy prawa mogą się różnić w zależności od kraju. Informacje o prawach autorskich można uzyskać w amerykańskim biurze ds. praw autorskich lub w Światowej Organizacji Własności Intelektualnej (WIPO). Facebook nie udziela porad prawnych, dlatego w przypadku pytań dotyczących praw autorskich zaleca się konsultację z prawnikiem. W większości krajów prawo autorskie jest ustawowym prawem, które chroni oryginalne dzieła autorskie. Zazwyczaj twórca oryginalnego utworu uzyskuje prawa autorskie do tego utworu w momencie jego stworzenia.

	Wiele różnych rodzajów treści jest chronionych prawem autorskim, w tym: • *Materiały wizualne lub audiowizualne*: treści wideo, filmy, programy i audycje telewizyjne, gry wideo, obrazy, fotografie • *Zawartość dźwiękowa*: piosenki, kompozycje muzyczne, nagrania dźwiękowe, nagrania wypowiedzi ustnych • *Treści pisane*: książki, sztuki, rękopisy, artykuły, notacje muzyczne Prawo autorskie chroni tylko oryginalne utwory. Aby treść została uznana za wystarczająco oryginalną dla ochrony praw autorskich, musi być dziełem autora i musi powstać w wyniku określonego nakładu pracy twórczej.
Bariery/trudności dla dorosłych	• wysoki poziom ujawniania tożsamości na Facebooku, podobnie jak na innych portalach społecznościowych. Informacje te mogą obejmować imię i nazwisko, adres e-mail, adres fizyczny, numer telefonu, płeć, miasto rodzinne, datę urodzenia, zdjęcie, sieć znajomych, orientację seksualną, status związku, zainteresowania, pracę/zawód, ulubione książki, ulubione filmy, ulubioną muzykę, szkołę, informacje, kod pocztowy (lub kod ZIP) i przynależność polityczną. Powyższe informacje są szczególnie wrażliwe, ponieważ ludzie identyfikują się autentycznie. • wykorzystanie prawdziwych nazwisk do reprezentowania profilu może być wspierane przez specyfikacje techniczne, wymogi rejestracyjne lub normy społeczne (łączące profile uczestników z ich publicznymi tożsamościami). • stalking, reidentyfikacja, demograficzna reidentyfikacja, reidentyfikacja twarzy i kradzież tożsamości. Użytkownicy mogą być manipulowani poprzez inżynierię społeczną, nękanie, prześladowanie i spamowanie ze względu na element "creepiness" • terenu • Facebook może też uzależniać. • Komunikacja online jest bardziej atrakcyjna niż interakcja twarzą w twarz, to z kolei może zwiększyć liczbę internetowych spotkań towarzyskich. To może stworzyć kompulsywne i nadmierne korzystanie z sieci społecznych online, które może mieć negatywny wpływ na wyniki w pracy i w domu (przeciwdziałanie innym brakom, takim jak, relacje, brak przyjaciół, wygląd fizyczny i niepełnosprawność. • brak możliwości zgłaszania przestępców seksualnych na policję, • policja wyraziła zaniepokojenie faktem, że Facebook nie zgodził się na umieszczenie przycisku alarmowego na stronie profilowej każdego użytkownika, Facebook nie zwalcza zagrożenia pedofilami • wzrost liczby przestępstw, takich jak molestowanie i rzeczywiste uszkodzenie ciała, w wyniku korzystania z Facebooka
Niebezpieczeństwo mediów/narzędzi społecznościowych u dorosłych	• Utrata kontroli nad czasem spędzanym w sieci. Układ stron, każdy przycisk, każdy kolor jest starannie dobrany przez ekspertów, aby przyciągnąć uwagę. • Liczba fałszywych kont na Facebooku jest ogromna - tzw. trolle internetowe • Hakerzy doskonale wiedzą, jak złamać hasło na FB. • Bardzo powszechne jest fałszowanie stron logowania do serwisów społecznościowych i wysyłanie fałszywych wiadomości

	• Facebook jest często wykorzystywany jako narzędzie do rozpowszechniania fałszywych informacji • Informacje, które sami publikujemy w mediach społecznościowych mogą być wykorzystywane przez osoby trzecie • Robak Koobface był aktywny na Facebooku przez ponad rok • Udostępnianie swojej lokalizacji aplikacjom i innym użytkownikom może spowodować, że będziesz śledzony (np. obserwacja miejsca pobytu, włamanie) • Jako zagrożenie pojawiło się również uwierzytelnianie biometryczne w celu uzyskania dostępu np. do telefonu komórkowego lub profili internetowych (za pomocą skanu twarzy lub odcisku palca).
Rozwiązania, które możemy mieć	Szkolenie on-line z zakresu : • Bezpieczne korzystanie z Facebooka; • Czego nie publikować na portalach społecznościowych (jak ograniczyć udostępnianie prywatnych informacji o sobie) • Ustawienia prywatności na FB. • Tworzenie bezpiecznego hasła do konta • Konfiguracja dwuskładnikowego uwierzytelniania. • Przyjmowanie zaproszeń (identyfikowanie zaproszenia od osoby). • Aktualizowanie oprogramowania antywirusowego i innych programów zabezpieczających. • Korzystanie z modułu Rozmowy prywatne. • Udostępnianie treści, zdjęć i postów z innych mediów społecznościowych. • Jak zgłaszać treści, które wydają się podejrzane.

14. GOOGLE+

Nazwa mediów społecznościowych / narzędzia	**GOOGLE+**
Informacje ogólne	**Google+** został uruchomiony 28 czerwca 2011 roku, próbując rzucić wyzwanie innym sieciom społecznościowym, łącząc inne produkty Google, takie jak Google Drive, Blogger i YouTube. Jest zwykle znany jako Google Plus, czasami nazywany G+ był siecią społecznościową należącą i prowadzoną przez Google. Istotne zmiany doprowadziły do przeprojektowania tej sieci społecznościowej w listopadzie 2015 roku. 7 marca 2019 roku podjęto decyzję o wyłączeniu sieci społecznościowej dla biznesu, a miesiąc później, 2 kwietnia, wyłączono ją również dla użytkowników osobistych. Powodem tej decyzji były zarówno niskie zaangażowanie użytkowników, jak i ujawnione wady projektowe oprogramowania, które potencjalnie umożliwiały zewnętrznym programistom dostęp do osobistych informacji jego użytkowników. Google+ nadal był dostępny jako "Google+ dla G Suite"; wszyscy użytkownicy przeszli na "Google Currents". Kolejnym krokiem będzie ostatecznie przejście z Google Currents na "Google Chat" w 2023 roku. W Google+ ludzie mogą dzielić się pomysłami i wiadomościami osobistymi, publikować zdjęcia i filmy, utrzymywać kontakt, grać w gry, planować spotkania, wysyłać życzenia urodzinowe, wspólnie odrabiać zadania domowe i prowadzić interesy, odnajdywać i kontaktować się z dawno niewidzianymi przyjaciółmi i krewnymi, recenzować książki, polecać restauracje i wspierać cele. Lista jest długa - widać, jak bardzo indywidualne jest jej zastosowanie. Sieci społecznościowe obejmują również uzyskiwanie i udzielanie walidacji oraz wsparcia emocjonalnego, wiele nieformalnych form uczenia się, a także odkrywanie zainteresowań osobistych, akademickich i przyszłych zawodowych. Musisz być zarejestrowanym użytkownikiem, aby mieć pełny dostęp do opcji Google +. Podczas dokonywania logowania/rejestracji zostaniesz poproszony o odpowiedź na kilka prostych pytań, takich jak prawdziwe imię i nazwisko, nazwa użytkownika, hasło i data urodzenia. W USA, aby uzyskać konto, musisz mieć co najmniej 13 lat, to samo w innych krajach. Będziesz miał również możliwość dodania zdjęcia profilowego, a następnie zostaniesz przeniesiony bezpośrednio do Google+. Podczas procesu rejestracji zostaniesz poproszony o "znalezienie osób, które znasz na Google+" poprzez wprowadzenie adresu e-mail z Yahoo lub Hotmail. Jest to opcjonalne. Google+ nie skontaktuje się z ludźmi z twojej listy kontaktów, ale zaimportuje kontakty z tych usług i da ci możliwość dodania kontaktów z tych usług do twoich kręgów. Po założeniu konta, przy pierwszej wizycie w Google+ zostanie zadanych kilka pytań, które są opcjonalne (nazwa szkoły lub pracy oraz miejsce zamieszkania, aby ułatwić znajomym, rodzinie i innym osobom znalezienie Cię).

Ryzyko związane z mediami społecznościowymi/ narzędziem: **Prywatność, dokładność, własność, dostępność, Naruszenie prawa, Prawo autorskie**	***Prywatność:*** Ustawienia prywatności pozwalały użytkownikom ujawniać pewne informacje wybranym przez nich kręgom. Użytkownicy mogli również zobaczyć gości swojego profilu. Istniały ustawienia prywatności, do których można się dostać klikając na swoje imię w prawym górnym rogu ekranu, a następnie Prywatność. Zawierały one linki do zarządzania kręgami, widoczności sieci (kto był w twoich kręgach i kto mógł zobaczyć, kto dodał cię do swoich kręgów) i innych ustawień. Był tam również link do sekcji pomocy prywatności Google+. ***Dokładność:*** Brak danych. ***Własność:*** Niektóre firmy zarządzające nieruchomościami używały Google+ do udostępniania własnych postów na blogu, artykułów stron trzecich, wiadomości o ich działalności lub branży w ogóle itp. Google My Business stało się centralnym punktem, w którym odwiedzający stronę internetową mogą znaleźć i dowiedzieć się więcej o Twojej firmie. ***Dostępność:*** Większość rzeczy, które można zrobić w Google+ w sieci, można również zrobić za pomocą aplikacji Google+ na smartfony z systemem Android i telefonem iPhone, a ponadto istnieje aplikacja internetowa, która działa z innymi telefonami podłączonymi do internetu. Google Messenger to funkcja dla smartfonów (ale nie dla desktopowej wersji Google+), która umożliwia grupom osób prowadzenie rozmowy. ***Naruszenie przepisów prawa:*** Google ciężko pracuje, aby egzekwować te zasady, ale z milionami użytkowników i miliardami postów nie może zrobić tego wszystkiego sam. Tu właśnie wkracza społeczność. Od nas wszystkich zależy, czy Google+ pozostanie bezpiecznym i wygodnym miejscem. Jeśli zobaczysz treść, która wydaje się naruszać standardy, możesz kliknąć strzałkę w dół po prawej stronie postu lub treści i wybrać opcję Zgłoś nadużycie. Następnie należy określić, dlaczego jest to nadużycie, zaznaczając odpowiednie pole. W lewej kolumnie profilu każdej osoby znajduje się również opcja "Zgłoś ten profil", jeśli sam profil zawiera treści, które mogą naruszać standardy społeczności Google. ***Copyright:*** Standardowym punktem odniesienia w kwestii naruszenia praw autorskich są warunki korzystania z usług Google.

	Usługa Google "Reagujemy na zawiadomienia o domniemanym naruszeniu praw autorskich i likwidujemy konta osób dopuszczających się powtarzających się naruszeń zgodnie z procesem określonym w amerykańskiej ustawie Digital Millennium Copyright Act. Dostarczamy informacji, które pomagają posiadaczom praw autorskich zarządzać ich własnością intelektualną w Internecie. Jeśli uważasz, że ktoś narusza Twoje prawa autorskie i chcesz nas powiadomić, w naszym Centrum Pomocy znajdziesz informacje o przesyłaniu powiadomień i polityce Google dotyczącej reagowania na powiadomienia."
Bariery/trudności dla dorosłych	• Najczęstszym zagrożeniem jest agresja społeczna (cyberprzemoc) • Umieszczanie kompromitujących lub szkodliwych informacji o sobie - tekstów, zdjęć lub filmów, które mogą nas zawstydzić teraz lub w przyszłości, niezależnie od tego, czy zostały umieszczone przez nas samych, czy przez innych. To jest kwestia reputacji. • Wyzwanie związane z czasem ekranowym - zbyt dużo czasu na jakąkolwiek jedną rzecz może być szkodliwe dla innych aktywności w naszym życiu. • Ryzyko nieodpowiedniego kontaktu z nieznajomymi/hakerami • Uważaj, kogo zapraszasz na hangout i zdaj sobie sprawę, że każdy zaproszony może zaprosić dodatkowe osoby, których możesz nie znać.
Niebezpieczeństwo mediów/narzędzi społecznościowych u dorosłych	Na razie Google + nie będzie zagrożeniem dla dorosłych, bo od 2019 roku sieć społecznościowa jest wyłączona.
Rozwiązania, które możemy mieć	Instrukcje lub poradniki, które pomogą w pobraniu danych umieszczonych na koncie Google + utworzonym przed 2019 rokiem.

MILEAGE

15. Partnerzy

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