BEZPIECZEŃSTWO W SIECI

ZBIGNIEW GONTAR

Projekt dofinansowany ze środków rządowego programu wieloletniego na rzecz Osób Starszych „Aktywni+” na lata 2021-2025

Autor
Zbigniew Gontar

Ilustracje
Grzegorz Kalinowski

Skład
Katarzyna Ciach

ISBN: 83-86227-19-2

Wydawca
Fundacja Rozwoju Przedsiębiorczości im. Prof. Jerzego Dietla
ul. Piotrkowska 86
90-103 Łódź
e-mail: fundacja@frp.lodz.pl

Zespół
dr Ewa Sadowska-Kowalska, dr Małgorzata Sikorska, Łukasz Kielan,
Krzysztof Kucharski, Małgorzata Bujacz, Agnieszka Bogusławska, Zbigniew Pawlak

Wydanie I
Nakład: 300 egz.

Publikacja bezpłatna

Zbigniew Gontar

Bezpieczeństwo w sieci

FRP® ROK ZAŁOŻENIA 1990
Fundacja Rozwoju Przedsiębiorczości im. Prof. Jerzego Dietla

Łódź, październik 2023

Zbigniew Gontar – doktor nauk ekonomicznych, ekspert w zakresie cyfrowej transformacji społeczeństwa, gospodarki i biznesu, pracuje w Instytucie Informatyki i Gospodarki Cyfrowej w Szkole Głównej Handlowej w Warszawie oraz w Katedrze Informatyki Uniwerystetu Łódzkiego. Członek Stowarzyszenia Informatyków - w ramach IEEE – Instytutu Inżynierów Elektryków i Elektroników, współzałożyciel Naukowego Towarzystwa Informatyki Ekonomicznej, ekspert Naukowego Centrum Badan i Rozwoju.

Grzegorz Kalinowski – artysta malarz, rysownik, fotograf, podróżnik. Dr hab., profesor Akademii Sztuk Pieknych im. Władysława Strzemińskiego w Łodzi i Europejskiej Akademii Sztuk w Warszawie. Prezes Okręgu Łódzkiego Związku Polskich Artystów Plastyków w latach 2006-2012. Uhonorowany Odzanaczeniem Zasłużony Kulturze Polskiej przez Ministra Kultury i Dziedzictwa Narodowego. Posiada w dorobku kilkadziesiąt wystaw indywidualnych i ponad 100 wystaw zbiorowych. Organizator plenerów malarskich na duńskich wyspach Bornholm, Vejrø, Møn i wielokrotnie w Prowansji (Francja).

Spis treści

1. Wstęp

Oczekiwanie, że środowisko cyfrowe jest bezpieczne, podobnie jak oczekiwanie, że góry są bezpieczne, może być mylące. W obu przypadkach istnieją zagrożenia i wymagana jest odpowiednia ostrożność. Góry mogą wydawać się malownicze i spokojne, ale nieprzygotowane na wędrówkę osoby mogą napotkać na trudności takie jak nagłe zmiany pogody, dzikie zwierzęta czy zbyt trudne do pokonania trasy. Podobnie, świat cyfrowy może wydawać się prosty i przyjazny, ale niewłaściwe zachowania, takie jak używanie słabych haseł, które zawierają Twoje imię, nazwisko, albo datę urodzenia czy klikanie w podejrzane linki, mogą prowadzić do poważnych problemów, takich jak kradzież tożsamości czy utrata wrażliwych danych.

W obu przypadkach trzeba być przygotowanym i świadomym potencjalnych zagrożeń. W górach oznacza to zazwyczaj zabranie na wyprawę odpowiedniego sprzętu, zwracanie uwagi na warunki pogodowe czy wybór trasy dostosowanej do umiejętności. W cyberprzestrzeni oznacza to używanie silnych haseł, zawierających połączenie dużych i małych liter, znaków specjalnych i cyfr, korzystanie z oprogramowania antywirusowego i zachowanie ostrożności podczas udostępniania informacji o sobie.

Poruszanie się w świecie cyfrowym jest jak chodzenie po górach. Na pierwszy rzut oka może się wydawać, że jest to łatwe i intuicyjne, ale w obu przypadkach występują ukryte zagrożenia i pułapki. Podobnie jak nieprzygotowany wspinacz może narazić się na niebezpieczeństwo z powodu braku sprzętu czy niewłaściwego przygotowania, osoba poruszająca się w świecie cyfrowym bez podstawowej wiedzy o zabezpieczeniach może również narazić się na ryzyko.

W górach potrzebujesz odpowiedniego wyposażenia, mapy i kompasu, aby bezpiecznie dotrzeć do celu. W świecie cyfrowym potrzebujesz silnych haseł, zabezpieczeń dwuskładnikowych i świadomości zagrożeń, aby chronić swoją prywatność i dane.

W obu przypadkach, odpowiednie przygotowanie i świadomość ryzyka są kluczowe do bezpiecznego i satysfakcjonującego doświadczenia.

Niestety każdego roku słyszymy o wypadkach w górach, które są wynikiem różnych czynników: braku odpowiedniego przygotowania, złych warunków pogodowych, błędów w nawigacji czy nieodpowiedniego ubrania. Podobnie w świecie cyfrowym, co roku wiele osób pada ofiarami ataków cybernetycznych, kradzieży tożsamości, oszustw i innych form zagrożeń.

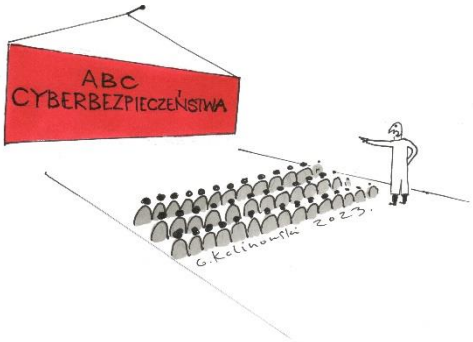
W obu przypadkach, nie zawsze można zapobiec wypadkom, nawet będąc dobrze przygotowanym i ostrożnym. Jednak podstawowe środki bezpieczeństwa mogą znacznie zmniejszyć takie ryzyko. W górach oznacza to na przykład noszenie odpowiedniego wyposażenia, informowanie innych o celu podróży i przewidywanym czasie powrotu, sprawny telefon z GPS oraz słuchanie rad ekspertów i lokalnych służb. W świecie cyfrowym podstawowe środki bezpieczeństwa to na przykład stosowanie zasady ograniczonego zaufania, aktywowanie dwuskładnikowego uwierzytelnienia czy aktualizacja oprogramowania,.

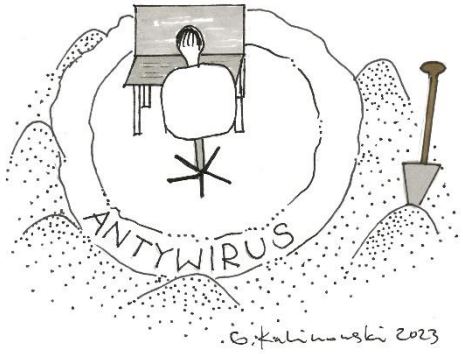
Warto również podkreślić, że zarówno wypadki w górach, jak i incydenty w świecie cyfrowym, często mają wpływ nie tylko na ofiary, ale i na ich bliskich. Dlatego tak ważne jest, by dbać o swoje bezpieczeństwo zarówno w wirtualnym, jak i w rzeczywistym świecie.

2. Główne zasady bezpieczeństwa

Oto dziesięć najważniejszych rad dla osób korzystających ze świata cyfrowego, które mogą pomóc w zapewnieniu bezpieczeństwa i komfortu podczas wędrówek po świecie cyfrowym:

1. Zanim zaczniesz korzystać ze świata cyfrowego, dobrze jest poznać podstawowe zagrożenia i sposoby ich unikania. Możesz skorzystać z różnych kursów online, poradników lub nawet zasobów dostarczanych przez bliskich znających się na technologii. My proponujemy 3 materiały wideo zatytułowane „ABC Cyberbezpieczeństwa" przygotowane przez Jerzego Surmę, profesora Szkoły Głównej Handlowej w Warszawie,

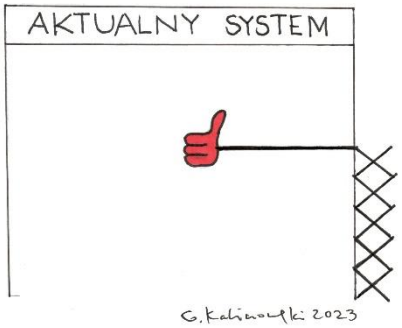




2. Zainstaluj i skonfiguruj oprogramowanie antywirusowe. Antywirusy to swoisty „sprzęt wspinaczkowy" w świecie cyfrowym. Pomagają chronić Twoje urządzenie przed zagrożeniami. Masz do dyspozycji wiele programów, stworzonych w wielu demokratycznych krajach, na przykład Antywirus NORTON 360 (USA), AVG Ultimate (Czechy), Bitdefender (Rumunia), Panda (Hiszpania), McAfee (USA), Eset (Słowacja), G Data (Niemcy), Avast (Czechy), Arcabit (Polska), Sophos (Anglia) i wiele innych. Możesz tez skorzystać z usługi chmurowej w tym zakresie.

3. Używaj różnych, skomplikowanych haseł dla różnych serwisów i aplikacji. Im bardziej złożone i unikalne hasło, tym trudniej je złamać. Nie udostępniaj ich i nie notuj. Silne hasła to jak dobrze zapięty pas bezpieczeństwa. Niezwykle ważne dla zabezpieczenia Twoich kont i danych. Gdzie tylko można, włącz weryfikację dwuetapową. To dodatkowa warstwa bezpieczeństwa, która może chronić twoje konto nawet jeśli ktoś zdobędzie Twoje hasło. Więcej na ten temat w publikacji NASK-PIB/CERT Polska, Kompleksowo o hasłach, 2022.

4. Tak jak na szlaku, warto być uważnym. Nie otwieraj podejrzanych linków, nie instaluj oprogramowania z nieznanych źródeł i nie udostępniaj osobom nieznajomym swoich danych osobowych czy finansowych.

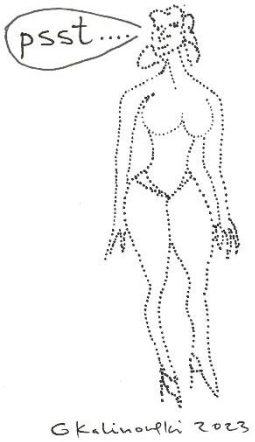


5. Regularnie aktualizuj swoje systemy i oprogramowanie. Stare wersje mogą zawierać luki bezpieczeństwa, które mogą być wykorzystane przez cyberprzestępców. Regularne aktualizacje oprogramowania to swoista „kontrola sprzętu wspinaczkowego". Pomagają w utrzymaniu bezpieczeństwa systemów i aplikacji.

6. Uzyskaj wsparcie bliskich. Rodzina i przyjaciele, którzy są bardziej doświadczeni w korzystaniu z nowych technologii, mogą być doskonałym wsparciem. Mogą pomóc w rozwiązaniu problemów, jak również udzielić wartościowych rad. Twoimi przyjaciółmi są na pewno NASK – Państwowy Instytut Badawczy (nask.pl) oraz CERT Polska (cert.pl).

7. Pamiętaj o wyborze właściwego czasu i miejsca. Podobnie jak w rzeczywistych podróżach, warto znać swoje ograniczenia. Nie spędzaj zbyt dużo czasu online i korzystaj z sieci w miejscach, które uznajesz za bezpieczne. Używaj bezpiecznych połączeń (HTTPS) i VPN, gdy korzystasz z mniej bezpiecznych publicznych sieci Wi-Fi.

8. Nie zapominaj o kontroli prywatności. Zwracaj uwagę na ustawienia prywatności na różnych platformach i serwisach, aby kontrolować, jakie informacje są publiczne. Nie udostępniaj w sieci zbyt wielu informacji o sobie. Mogą one zostać użyte do kradzieży tożsamości lub innych form oszustwa. Sprawdź, czy Twoje dane są bezpieczne na portalu Ministerstwa Cyfryzacji (https://bezpiecznedane.gov.pl/).



9. Kiedy szukasz informacji, dbaj o rzetelność źródeł i bądź krytyczny wobec tego, co czytasz. W świecie cyfrowym pełnym fałszywych informacji (ang. fake news), dobrze jest korzystać z zaufanych źródeł informacji i weryfikować rzetelność otrzymanych danych.

10. Jeżeli nabyłeś już pewne umiejętności i wiedzę na temat bezpiecznego poruszania się w świecie cyfrowym, podziel się tym z innymi. Może to być nieocenione dla osób, które są mniej doświadczone w tej dziedzinie. Zgłoś każdy incydent naruszenia bezpieczeństwa w świecie cyfrowym do CERT Polska (https://incydent.cert.pl).

Korzystanie ze świata cyfrowego, podobnie jak wędrówki górskie, niesie ze sobą pewne ryzyka, ale stosując się do tych zasad, można je znacząco zminimalizować. Bezpieczeństwo cyfrowe powinno być dla każdego priorytetem.

3. Podstawowe oszustwa internetowe

Oszustwo w świecie cyfrowym ma wiele twarzy: e-maile z perspektywą rzekomo milionowej wygranej, fałszywe sklepy internetowe, fałszywe strony internetowe, ataki za pomocą złośliwego oprogramowania, kradzież tożsamości i wiele innych. W większości przypadków oszuści próbują zdobyć dane osobowe, takie jak hasła lub numery PIN, w celu wykorzystania niczego niepodejrzewających ofiar.

Aby nie dać się nabrać na typowe oszustwa, omówimy tutaj różne ich typy.

Oszustwa internetowe często mają miejsce za pośrednictwem poczty elektronicznej, SMS-ów lub sieci społecznościowych. Warto zajrzeć do poradnika opublikowanego przez NASK-PIB/CERT Polska, „Bezpieczna poczta i konta społecznościowe", 2021, (https://cert.pl/uploads/docs/CERT_Polska_Bezpieczna_poczta_i_konta_spolecznosciowe.pdf), aby dowiedzieć się co oznacza bezpieczna poczta i konta społecznościowe.

Cyberprzestępcy proszą Cię zazwyczaj o...

1. przesłanie danych do logowania. Może to obejmować Twój adres e-mail, hasło i inne poufne informacje, takie jak PIN. Czasami osoby te proszą również o dokumenty, takie jak zeskanowany lub sfotografowany dowód osobisty. Nie zawsze jest to oznaka przestępstwa. Warto jednak w takiej sytuacji zachować ostrożność.
2. zrobienie przelewów. Jeśli dasz się nabrać na typowe „oszustwo na wnuczka", oszuści otrzymają określoną kwotę pieniędzy bezpośrednio z Twojego konta, podczas gry Ty będziesz przekonany, że pomagasz wnukowi lub innej bliskiej osobie.
3. telefon do przyjaciół i rodziny. W takim przypadku Twój rachunek telefoniczny zostanie obciążony odpowiednią kwotą, te połączenia telefoniczne są bowiem płatne i zazwyczaj bardzo kosztowne.
4. kliknięcie łącza będącego przynętą w tak zwanym ataku phishingowym. Kliknięcie tego linku przeniesie Cię na fałszywą witrynę internetową, gdzie otrzymasz możliwość zalogowania się do fałszywego konta łudząco podobnego do na przykład Twojego konta bankowego. Oszuści przechwytują wówczas Twoje dane do logowania, co oznacza w praktyce wyczyszczenie Twojego konta ze wszystkich zgromadzonych tam pieniędzy i innych aktywów. Czasami ta fałszywa witryna instaluje również złośliwe oprogramowanie na Twoim komputerze.
5. otworzenie załącznika. Powoduje to również zainstalowanie złośliwego (bądź śledzącego) oprogramowania na Twoim komputerze. Niektóre oszustwa polegają na zachęcaniu do otwarcia dokumentu, filmu czy innych plików, które mogą zawierać złośliwe oprogramowanie. Śledzenie Twoich działań w świecie cyfrowym to norma i nie zawsze jest to przestępstwo. W praktyce, prawie każda witryna śledzi legalnie Twoje działania w świecie cyfrowym, instalując na Twoim urządzeniu pliki cookies (pol. ciasteczka).
6. udostępnienie kodu weryfikacyjnego. Oszuści często proszą o udostępnienie kodu, który został wysłany na Twoją skrzynkę e-mailową lub numer telefonu w ramach dwuetapowej weryfikacji. Nie dając się na to nabrać, zabezpieczasz swoje konto przed przejęciem.
7. odpowiedzi na pytania, które mogą wydawać się niewinne, ale w rzeczywistości służą zgromadzeniu informacji, które później wykorzystają przeciwko Tobie, na przykład do wyboru stosownej przynęty w ataku phishingowym.
8. zdalny dostęp do komputera. Oszuści często podają się za przedstawicieli firm technologicznych i proszą o udostępnienie zdalnego dostępu do komputera, twierdząc, że muszą rozwiązać problem techniczny.

Ofiarą oszustw w świecie online może być każdy. Oszuści wybierają potencjalne ofiary na podstawie przypadkowych numerów telefonów lub wycieków danych. Oszuści często używają technik marketingowych, takich jak legalne reklamy, mailing czy media społecznościowe, aby dotrzeć do potencjalnych ofiar. Nieuczciwe firmy reklamują pozornie bezpieczne inwestycje, aby

przyciągnąć nieświadomych ryzyka klientów. Co więcej, te reklamy są często umieszczane w świecie cyfrowym w sposób legalny, co dodatkowo buduje fałszywe poczucie bezpieczeństwa. Po wyrażeniu zainteresowania ofertą przez przyszłą ofiarę ataku, firmy te przystępują do agresywnych działań, mających na celu wyłudzenie pieniędzy. Oszuści w świecie cyfrowym to często bardzo młode osoby, które mają technologiczną przewagę nad osobami w wieku 60+. Z drugiej strony, mamy do czynienia także z profesjonalnymi hakerami, którzy posiadają zaawansowane umiejętności i narzędzia, umożliwiające im przeprowadzenie skomplikowanych ataków. Obie te grupy wykorzystują swoje umiejętności do wyłudzania pieniędzy, kradzieży danych czy innych form oszustwa, często skierowanych przeciwko starszym osobom, które nie są na tyle biegłe w technologii, by się przed tym efektywnie bronić. Obrona przed młodymi oszustami technologicznymi jest zazwyczaj mniej skomplikowana. Podstawowe zasady bezpieczeństwa, takie jak nieklikanie w podejrzane linki czy używanie silnych haseł, zwykle są wystarczające. Jednak obrona przed profesjonalnymi hakerami jest znacznie trudniejsza, wymaga bardziej zaawansowanych środków, takich jak uwierzytelnianie wieloskładnikowe (np. podanie PINu i potwierdzenie SMSem), zaktualizowane oprogramowanie zabezpieczające i ciągła świadomość zagrożeń cyberbezpieczeństwa. W obu przypadkach, edukacja i świadomość są kluczowe, ale poziom zabezpieczeń powinien być dostosowany do rodzaju i skali potencjalnego zagrożenia.

Musimy mieć też świadomość istnienia ciemnego Internetu (ang. Darknet), który jest dostępny tylko przez specjalne przeglądarki. Znajdziemy tam zarówno fora dyskusyjne na niszowe tematy, jak i działalność kryminalną, od handlu narkotykami po sprzedaż danych osobowych. Wchodzenie w tę część Internetu bez odpowiedniego przygotowania i wiedzy jest ryzykowne. Podobnie jak w przypadku wspinaczki na Rysy, gdzie nieodpowiednie przygotowanie czy zaniedbanie mogą prowadzić do poważnych konsekwencji, tak samo wyprawa w ciemny Internet może zakończyć się naruszeniem prywatności, utratą danych lub nawet kryminalną odpowiedzialnością.

Nasza broszura koncentruje się na bezpieczeństwie w „jasnym" Internecie, podkreślając, że dla większości osób nie ma potrzeby ani powodu, aby zapuszczać się w jego mroczniejsze zakamarki.

4. Główne zagrożenia

FAŁSZYWE INWESTYCJE

Opis: Oszukańcze plany finansowe oferujące wysokie zyski przy minimalnym ryzyku, mające na celu wprowadzenie inwestorów w błąd i wykorzystanie ich wpłat w nieuczciwy sposób lub utratę środków.

Schemat działania: Oszust nawiązuje kontakt, często przez email czy media społecznościowe, i przedstawia „okazję inwestycyjną" z obietnicą wysokich zysków, np. udział w ważnych krajowych przedsięwzięciach biznesowych, inwestycje z udziałem sztucznej inteligencji, zakup złota. Używa presji czasowej, aby skłonić ofiarę do szybkiej wpłaty. Po otrzymaniu wpłaty, znika, a inwestycja jest stracona.

Jak się bronić: Zawsze dokładnie weryfikuj informacje o firmie i jej ofercie oraz konsultuj się z niezależnym doradcą finansowym. Nigdy nie inwestuj więcej, niż jesteś gotów stracić, i unikaj ofert obiecujących gwarantowane, wysokie zyski.

FAŁSZYWE SKLEPY INTERNETOWE

Opis: Fałszywe sklepy internetowe to strony udające legalne sklepy, które oferują atrakcyjne produkty w celu wyłudzenia pieniędzy. Po dokonaniu płatności towar nie jest wysyłany, a strona przestaje odpowiadać na kontakt.

Schemat działania: Fałszywy sklep zachęca do zakupów przez reklamy w mediach społecznościowych i e-maile. Używa taktyk presji czasowej, by przyspieszyć zakupy. Po opłaceniu produktu, klient zostaje zignorowany i nie otrzymuje zamówienia.

Jak się bronić: Kluczowe jest dokładne zbadanie strony przed dokonaniem zakupu. Obejmuje to sprawdzenie opinii o sklepie, certyfikatów bezpieczeństwa oraz innych wskaźników wiarygodności jak adres czy numer telefonu. Zawsze warto porównać ceny produktów z innymi sklepami; jeśli oferta wydaje się zbyt dobra, aby była prawdziwa, najprawdopodobniej jest to oszustwo. Nie polegaj wyłącznie na atrakcyjnych zdjęciach produktów czy obietnicach szybkiej dostawy.

SMS-Y, KTÓRE WYGLĄDAJĄ JAK OD BANKU CZY INNEGO ZAUFANEGO ŹRÓDŁA, ALE SĄ PRÓBĄ WYŁUDZENIA

Opis: Fałszywe SMS-y to oszustwo, w którym ofiary otrzymują mylące wiadomości z linkami lub instrukcjami mającymi na celu wyłudzenie danych. Oszuści często podszywają się pod znane organizacje, aby skłonić do podjęcia niebezpiecznych działań, takich jak wprowadzenie kodu PIN czy wykonanie przelewu. Metoda ta jest powszechna i skuteczna ze względu na rozpowszechnienie użycia SMS-ów.

Schemat działania: Fałszywe SMS-y zachęcają do kliknięcia w link prowadzący do strony imitującej np. bank. Po wpisaniu na niej swoich danych, ofiara umożliwia oszustom dostęp do konta, haseł i wrażliwych informacji. Oszuści wykorzystują te dane do nieautoryzowanych transakcji czy kradzieży tożsamości, a po ataku często zmieniają taktykę, aby unikać wykrycia. Niektóre ofiary są atakowane wielokrotnie z użyciem różnych metod.

Jak się bronić: Najważniejsze jest, aby nie kliknąć na linki od nieznanych lub podejrzanych numerów. Jeśli SMS wydaje się ważny, zawsze dobrze jest potwierdzić jego autentyczność, kontaktując się bezpośrednio z daną instytucją. Dodatkową warstwą ochrony może być zainstalowane oprogramowanie antywirusowe na smartfonie. Podejrzane SMS-y warto zgłaszać do właściwych organów i blokować numer, aby zapobiec dalszym próbom oszustwa. Na ważnych kontach online warto również włączyć uwierzytelnianie dwuskładnikowe.

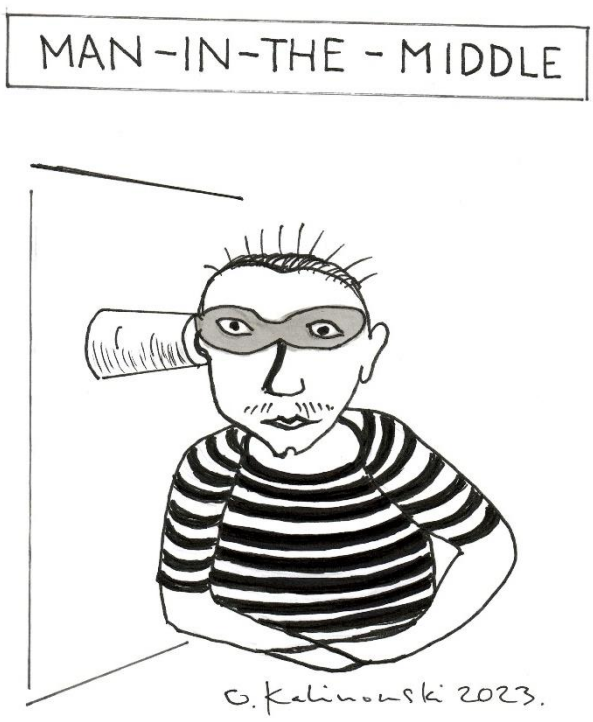
FAŁSZYWI KONSULTANCI

Opis: Fałszywi konsultanci udają ekspertów w różnych dziedzinach, aby wyłudzić pieniądze czy dane osobowe. Używają pozornej wiedzy i autorytetu, by zyskać zaufanie ofiar i nakłonić je do ryzykownych działań, jak inwestycje w wątpliwe projekty czy udostępnienie poufnych informacji.

Schemat działania: Fałszywi konsultanci pozyskują ofiary przez reklamy i media społecznościowe, podając się za ekspertów z fałszywymi referencjami. Wywierają presję czasową, prezentując nadmiernie korzystne oferty i budują zaufanie, po czym namawiają do uiszczenia „opłat początkowych" czy udostępnienia danych finansowych. Po zdobyciu tego, co chcieli, znikają, często zmieniając identyfikatory i dezaktywując strony. W niektórych przypadkach powracają do tych samych ofiar z nowym oszustwem.

Jak się bronić: Zawsze weryfikuj tożsamość i referencje. Nie udostępniaj wrażliwych danych i unikaj wpłat w pośpiechu. Bądź ostrożny z linkami i załącznikami w e-mailach oraz korzystaj z bezpiecznych metod płatności. Jeżeli oferta wydaje się zbyt dobra, aby była prawdziwa, prawdopodobnie jest to oszustwo. W razie wątpliwości, skonsultuj się z zaufanymi osobami i zgłoś podejrzane działania odpowiednim organom.

MAN-IN-THE-MIDDLE



Opis: Oszuści pozycjonują się między tobą a stroną, do której próbujesz się połączyć (na przykład twoim bankiem), aby przechwycić i ewentualnie zmodyfikować przesyłane informacje.

Schemat działania: Oszust monitoruje sieci, często publiczne Wi-Fi, aby przechwycić dane między dwoma komunikującymi się stronami, jak np. użytkownikiem i jego bankiem online. Może tylko podsłuchiwać lub aktywnie modyfikować dane, jak np. zmieniać kwoty w transakcjach bankowych. Wykorzystuje zdobyte informacje, takie jak hasła i numery kart, do różnych celów, od nieautoryzowanych transakcji po kradzież tożsamości, starając się przy tym zatrzeć ślady swojej działalności.

Jak się bronić: Najważniejsze jest unikanie korzystania z publicznych sieci Wi-Fi do dokonywania ważnych transakcji. Jeżeli musisz korzystać z publicznej sieci, zalecane jest użycie sieci VPN, która zaszyfruje twoją komunikację. Upewnij się także, że strony, z którymi się łączysz, korzystają z protokołu HTTPS, co dodatkowo zabezpiecza twoje dane. Ważne jest również włączenie uwierzytelniania dwuskładnikowego na swoich kontach oraz używanie silnych i unikatowych haseł, najlepiej przechowywanych w menedżerze haseł.

PLIKI LUB LINKI WYSYŁANE W E-MAILACH LUB SMS-ACH, KTÓRE MOGĄ ZAINSTALOWAĆ ZŁOŚLIWE OPROGRAMOWANIE NA TWOIM KOMPUTERZE LUB TELEFONIE

Opis: Niebezpieczne załączniki to złośliwe pliki dołączone do e-maili lub SMS-ów, mające na celu zainfekowanie komputera, kradzież danych lub nieautoryzowany dostęp. Są często maskowane jako pilne lub ważne wiadomości, by skłonić użytkownika do ich otwarcia.

Schemat działania: Oszuści wysyłają sfałszowane e-maile lub SMS-y od pozornie zaufanych źródeł z pilnymi komunikatami i załącznikami. Otwarcie załącznika uruchamia złośliwy kod, który może wykraść dane, zainfekować komputer ransomwarem lub otworzyć drzwi do dalszych ataków. Dane są przesyłane do cyberprzestępców, którzy mogą je wykorzystać na różne sposoby i często usiłują ukryć swoje działania. Metoda ta jest często stosowana na różnych ofiarach z drobnymi zmianami, aby uniknąć wykrycia.

Jak się bronić: Zawsze zastanów się dwa razy, zanim otworzysz nieoczekiwany załącznik w e-mailu czy SMS-ie, zwłaszcza jeśli pochodzi od nieznajomego nadawcy lub zawiera pilny komunikat. Używaj aktualnego oprogramowania antywirusowego, a także zaktualizuj regularnie system operacyjny i inne oprogramowanie. Ponadto, nie udostępniaj wrażliwych informacji bez weryfikacji tożsamości nadawcy i stosuj zasady ostrożności, takie jak uwierzytelnianie dwuskładnikowe, gdzie to możliwe.

NIEBEZPIECZNE PŁATNOŚCI PRZEZ INTERNET

Opis: Niebezpieczne płatności przez Internet to transakcje narażone na oszustwa i ataki cybernetyczne. Oszuści używają metod takich jak phishing czy ataki Man-in-the-Middle, by zdobyć wrażliwe dane i wykonać nieautoryzowane transakcje. Ofiary mogą stracić pieniądze i narazić się na problemy z bezpieczeństwem oraz prywatnością.

Schemat działania: Oszuści identyfikują potencjalne ofiary przez naruszenia danych lub inżynierię społeczną, a następnie przekierowują je na fałszywe strony internetowe. Używają technik phishingowych z wiadomościami podkreślającymi pilność, aby zdobyć dane

osobiste ofiar. Zdobyte informacje wykorzystują do nieautoryzowanych transakcji, jak przelewy czy zakupy online. Mogą też próbować obejść dodatkowe zabezpieczenia, takie jak uwierzytelnianie dwuskładnikowe. Po zdobyciu korzyści, oszuści usuwają ślady i mogą sprzedawać zdobyte informacje lub używać ich w przyszłości.

Jak się bronić: Oszuści identyfikują potencjalne ofiary przez naruszenia danych lub inżynierię społeczną, a następnie przekierowują je na fałszywe strony internetowe. Używają technik phishingowych z wiadomościami podkreślającymi pilność, aby zdobyć dane osobiste ofiar. Zdobyte informacje wykorzystują do nieautoryzowanych transakcji, jak przelewy czy zakupy online. Mogą też próbować obejść dodatkowe zabezpieczenia, takie jak uwierzytelnianie dwuskładnikowe. Po zdobyciu korzyści, oszuści usuwają ślady i mogą sprzedawać zdobyte informacje lub używać ich w przyszłości.

PROŚBY O SZYBKI PRZELEW POD RÓŻNYMI PRETEKSTAMI, CZĘSTO OD OSÓB PODSZYWAJĄCYCH SIĘ POD ZNAJOMYCH

Opis: Prośby o przelew są standardową formą komunikacji finansowej, ale również często wykorzystywaną metodą oszustwa. Oszuści podszywają się pod znane instytucje czy osoby, wykorzystując manipulację i inżynierię społeczną, aby skłonić ofiary do wysłania pieniędzy na fałszywe konta. Takie działania mogą prowadzić do dużych strat finansowych i ryzyka kradzieży tożsamości.

Schemat działania: Oszuści zbierają informacje o potencjalnych ofiarach i wysyłają im fałszywe e-maile czy SMS-y, podszywając się pod znane instytucje lub osoby. W komunikatach proponują pilne przelewy na konta kontrolowane przez siebie. Jeżeli ofiara przystaje, środki są szybko przenoszone na inne konta, często w innych krajach. Po udanym oszustwie, kontakt z ofiarą jest zrywany, a ślady działania są usuwane. Schemat ten jest powtarzany na różnych ofiarach z drobnymi modyfikacjami.

Jak się bronić: Ważna jest świadomość różnych typów zagrożeń i ich mechanizmów. Używaj silnych, różnorodnych haseł i menedżera haseł. Włącz uwierzytelnianie dwuskładnikowe, gdzie to

możliwe, i utrzymuj aktualne oprogramowanie antywirusowe. Unikaj klikania w podejrzane linki i zawsze weryfikuj tożsamość osoby, która prosi o przekazanie środków lub danych osobowych. Regularnie monitoruj swoje konta bankowe i bądź ostrożny z tym, co i gdzie publikujesz o sobie. W razie podejrzeń, zgłoś oszustwo odpowiednim organom i swojemu bankowi.

SOCJOTECHNIKA

Opis: Różne metody manipulacji psychologicznej, używane do zmuszenia ludzi do ujawnienia poufnych informacji, takich jak hasła czy numery kart kredytowych.

Schemat działania: Oszuści najpierw zbierają informacje o ofierze z publicznych źródeł jak media społecznościowe. Analizują te dane, aby znaleźć słabe punkty i planują strategię oszustwa. Wybierają kanały komunikacji i tożsamość, za którą się podszywają. Następnie kontaktują się z ofiarą, stosując techniki manipulacji. Po udanej manipulacji realizują główny cel, jak wyłudzenie danych czy kradzież środków, a potem przerywają kontakt i usuwają ślady. Zdobyte zasoby wykorzystują w kolejnych oszustwach lub sprzedają na czarnym rynku.

Jak się bronić: Zwiększ swoją świadomość o różnych typach oszustw i zabezpiecz swoje informacje, ustawiając odpowiednie poziomy prywatności w mediach społecznościowych. Używaj silnych haseł i włącz uwierzytelnianie dwuskładnikowe gdziekolwiek to możliwe. Zawsze weryfikuj tożsamość osób, które proszą o Twoje dane, i nie klikaj w podejrzane linki czy załączniki. Jeśli podejrzewasz oszustwo, zgłoś to odpowiednim organom i monitoruj swoje konta bankowe.

SPOOFING

Opis: Oszuści mogą fałszować numery telefonów, aby wydawało się, że dzwonią z zaufanych instytucji. Mogą w ten sposób próbować wyłudzić informacje osobiste czy dane do logowania.

Schemat działania: Oszuści wybierają metodę spoofingu i zbierają potrzebne informacje o potencjalnych ofiarach. Określają cel oszustwa i przygotowują narzędzia. Następnie manipulują ofiarą, używając sfałszowanych identyfikatorów i technik psychologicznych. Po osiągnięciu celu, wykorzystują zdobyte informacje dla dalszych działań przestępczych i zacierają ślady. Skuteczne metody często są potem ponownie używane.

Jak się bronić: Nauczyć się podstaw bezpieczeństwa cybernetycznego i być uważnym na podejrzane wiadomości czy strony. Zainstaluj program antywirusowy, używaj dwuskładnikowego uwierzytelniania i silnych haseł. W sytuacjach kryzysowych szybko zmień dane dostępu. Regularnie aktualizuj oprogramowanie i w razie wątpliwości weryfikuj informacje niezależnym kanałem.

Jak widzisz, oszustwa internetowe to różne sposoby, w jaki nieuczciwi ludzie mogą próbować oszukać Cię w Internecie, żeby zdobyć Twoje dane, pieniądze czy coś, co jest dla Ciebie ważne. Mogą na przykład podszyć się pod kogoś, kogo znasz i poprosić o pieniądze, albo wysłać Ci fałszywy e-mail czy SMS, żebyś kliknął w link, który Cię okradnie. Dlatego tak ważne jest, żeby być w Internecie ostrożnym, tak jak byśmy byli ostrożni, gdy ktoś dzwoni do naszego domu i pyta o osobiste informacje.

Rozpoznanie oszustw internetowych bywa czasami trudne, ale jest kilka znaków, na które można zwrócić uwagę:

- ☞ nieznany nadawca - jeśli e-mail lub wiadomość SMS pochodzi od osoby lub instytucji, z którą nie masz żadnych wcześniejszych kontaktów, bądź ostrożny;
- ☞ błędy językowe - oszustwa internetowe są zjawiskiem globalnym i nie ograniczają się do jednej narodowości czy języka. Niemniej jednak, ze względu na dominującą rolę języka angielskiego w komunikacji online, wiele oszustw jest dokonywanych w tym języku. To jednak nie oznacza, że są one generowane wyłącznie w świecie anglojęzycznym. Język angielski jest często używany ze względu na jego szeroki zasięg i potencjalnie większą liczbę ofiar. Oszuści mogą być zlokalizowani w różnych częściach świata i korzystać z tłumaczy lub automatycznych narzędzi do tłumaczenia, aby dotrzeć do ofiar nie mówiących po angielsku. Z tego powodu przetłumaczone na język polski zawierają błędy gramatyczne lub stylistyczne;
- ☞ zbyt dobre, żeby było prawdziwe - oferowane „nagrody” lub „okazje” często są zbyt atrakcyjne, żeby były prawdziwe;
- ☞ niespodziewana prośba o dane osobiste - jeśli ktoś niespodziewanie prosi o Twoje hasło, numer karty kredytowej czy inne poufne informacje, prawdopodobnie jest to próba oszustwa;

- nieścisłości w adresie strony internetowej - zawsze sprawdzaj, czy strona internetowa, na której się znajdujesz, ma prawidłowy adres. Oszuści często tworzą strony, które na pierwszy rzut oka wyglądają jak znane serwisy. Często używają w tym celu adresów URL, które są tylko nieznacznie różne od prawdziwych adresów znanych stron. Na przykład, zamiast „www.pkobp.pl" mogą użyć „www.pkopb.pl" albo „www.pko-bp.com". Różnica jest czasem tak subtelna, że łatwo ją przeoczyć;
- brak protokołu bezpieczeństwa (https) - sprawdzaj, zanim wypełnisz jakiś formularz w Internecie, czy strona używa protokołu „https" zamiast „http". „Https" oznacza, że połączenie jest zabezpieczone;
- nieścisłości w e-mailach i wiadomościach SMS - jeżeli mail od banku czy innego zaufanego źródła wygląda inaczej niż zwykle, zawiera podejrzane linki lub załączniki, lepiej go nie otwierać;
- sprawdź opinie i oceny - jeśli kupujesz coś w Internecie, zawsze sprawdzaj opinie o sprzedawcy;
- podejrzane załączniki - nigdy nie otwieraj załączników od nieznanych nadawców. Mogą one zawierać złośliwe oprogramowanie;
- nacisk i pośpiech - oszuści często wywierają presję, mówiąc, że musisz szybko podjąć decyzję.

Jeżeli zauważysz którekolwiek z tych znaków, zachowaj ostrożność i, jeśli to możliwe, skontaktuj się z zaufaną osobą, która pomoże Ci ocenić sytuację.

5. Jak chronić się przed zagrożeniami?

Całkowite wyeliminowanie zagrożeń w cyfrowym świecie jest praktycznie niemożliwe. Technologie i metody wykorzystywane przez oszustów i hakerów ciągle się rozwijają, co oznacza, że metody obrony muszą być stale aktualizowane i dostosowywane do nowych typów ataków. Najlepszym podejściem do zarządzania tymi zagrożeniami jest podejście warstwowe, które zakłada zastosowanie wielu różnych środków zabezpieczających. To może obejmować zarówno techniczne środki bezpieczeństwa, takie jak firewalle, antywirusy i szyfrowanie, jak i praktyki zarządzania ryzykiem, takie jak edukacja, regularne audyty i testy penetracyjne.

Edukacja i świadomość są ważne, ponieważ wiele ataków, szczególnie tych opartych na inżynierii społecznej, wykorzystuje ludzkie błędy i niedoprecyzowania. Szkolenia i regularne przypomnienia o najlepszych praktykach mogą pomóc w minimalizacji ryzyka. Warto tu zajrzeć do Raportów rocznych z działalności CERT Polska dostępnych online.

Warto również zastosować monitoring kont i transakcji oraz opracować plan działania odpowiedzi na incydenty.

Chociaż nie można całkowicie wyeliminować ryzyka, można je znacząco zminimalizować i przygotować się na skuteczne reagowanie w przypadku incydentu.

Zabezpiecz swój dostęp do kont online za pomocą bezpiecznych haseł

Konta online przechowują wrażliwe dane, od informacji osobowych do danych finansowych. W rękach oszustów takie informacje mogą prowadzić do kradzieży tożsamości, nieautoryzowanych transakcji i innych problemów. Silne hasła są pierwszą linią obrony w zabezpieczaniu kont, a ich brak może umożliwić oszustom dostęp nie tylko do jednej usługi, ale też do innych powiązanych kont. Odpowiednia ochrona hasłowa jest kluczowa dla bezpieczeństwa online i może być wymagana przez różne regulacje lub warunki ubezpieczenia.

Bezpieczne hasła są kluczowym elementem ochrony online. Oto kilka przykładów haseł, które można uznać za „bezpieczne”:

J@zdaRower3mPoP@rku!
Cz3k0lat@_K@wa2021
P!otn0_Drz3w0$
Trudn3Hasl0#2023
Qw3r+Yui0p@$$

Kiedy tworzysz hasło, zaleca się, aby:

- miało co najmniej 12 znaków,
- zawierało duże i małe litery,
- używało znaków specjalnych (!, @, #, $, %, ^, &, *, (,) itd.),
- zawierało cyfry,
- było unikalne dla każdej usługi, z której korzystasz.

Korzystaj z menedżera haseł

Korzystanie z menedżera haseł zwiększa Twoje bezpieczeństwo online przez generowanie silnych haseł, ich szyfrowane przechowywanie i synchronizację między urządzeniami. Funkcje takie, jak: automatyczne wypełnianie i powiadomienia o atakach, dodatkowo ułatwiają zarządzanie kontami.

Przykłady:

- Rejestrujesz się w nowym sklepie internetowym. Zamiast używać tego samego hasła, które już masz do innego konta, menedżer haseł generuje dla Ciebie silne i unikatowe hasło.
- Otrzymujesz e-mail o naruszeniu bezpieczeństwa na jednym z serwisów, na których masz konto. Dzięki menedżerowi haseł, szybko możesz zmienić przechowywane w nim hasło, nie martwiąc się o jego skomplikowaną strukturę, bo wszystko jest zaszyfrowane.
- Logujesz się na swoje konto bankowe. Zamiast wpisywać login i hasło ręcznie, menedżer haseł automatycznie wypełnia te pola.

- Korzystasz z różnych urządzeń – komputera w domu, smartfona i tabletu na wakacjach. Dzięki menedżerowi haseł, masz dostęp do wszystkich swoich haseł na każdym z tych urządzeń.
- Zapomniałeś hasła do swojego konta na portalu społecznościowym. Menedżer haseł pozwala na łatwe odzyskanie lub zresetowanie hasła.
- Jeden z serwisów, do których masz konto, zostaje zaatakowany. Menedżer haseł wysyła Ci powiadomienie i sugeruje zmianę hasła na tym konkretnym serwisie.

Stosuj uwierzytelnianie dwuskładnikowe

Stosowanie uwierzytelniania dwuskładnikowego (2FA) dodaje dodatkową warstwę bezpieczeństwa do Twoich kont online. Działa przez wymaganie dwóch różnych form identyfikacji: coś, co wiesz (hasło) i coś, co masz (np. telefon). Dzięki temu, nawet jeżeli ktoś zdobędzie Twoje hasło, nie będzie mógł zyskać dostępu do konta bez drugiego składnika. Jest to skuteczny i prosty sposób na zwiększenie ochrony Twojego cyfrowego życia.

Przykład:

Prosty przykład uwierzytelniania dwuskładnikowego to logowanie do konta e-mail. Po wpisaniu swojego loginu i hasła (pierwszy składnik), system wysyła na Twój zarejestrowany numer telefonu SMS z jednorazowym kodem (drugi składnik). Dopiero po wprowadzeniu tego kodu masz dostęp do swojego konta. Dzięki temu, nawet jeżeli ktoś zdobędzie Twoje hasło, nie będzie w stanie zalogować się bez kodu, który otrzymałeś SMS-em.

Wykonuj regularne kopie zapasowe, stosując zasadę 3-2-1

Wykonuj regularne kopie zapasowe danych, stosując zasadę 3-2-1: utwórz trzy kopie ważnych plików, przechowuj je na dwóch różnych nośnikach i jedną z nich umieść w innym fizycznym miejscu.

Przykład:

Masz oryginalny plik z ważnymi dokumentami na dysku twardym swojego komputera. Tworzysz dwie dodatkowe kopie tego pliku.

Jedną kopię przechowujesz na zewnętrznym dysku twardym, a drugą w chmurze (na przykład na Google Drive czy Dropbox).

Ponieważ jedna z kopii jest w chmurze, jest przechowywana w innej lokalizacji geograficznej, co zapewnia dodatkową ochronę w przypadku lokalnej awarii, takiej jak pożar w Twoim domu.

Wykonuj regularne aktualizacje oprogramowania na komputerze i telefonie

Aktualizacja oprogramowania to proces aktualizacji istniejącego programu lub systemu operacyjnego, mający na celu usunięcie błędów, dodanie nowych funkcji i poprawienie bezpieczeństwa. Regularne jej wykonywanie na komputerze i smartfonie (który również jest formą komputera) jest kluczowe dla utrzymania ich bezpieczeństwa. Aktualizacje dostarczają nie tylko nowe funkcje i poprawiają wydajność, ale co najważniejsze, zabezpieczają luki w zabezpieczeniach. Producenci oprogramowania ciągle analizują i poprawiają swoje produkty, a instalacja najnowszych wersji chroni przed różnymi zagrożeniami, takimi jak: ataki hakerskie, malware czy ransomware. Pomijanie aktualizacji może znacząco zwiększyć ryzyko naruszenia bezpieczeństwa Twoich urządzeń.

Przykład:

Załóżmy, że używasz smartfona z systemem Android i pojawiła się nowa aktualizacja systemu. Zawiera ona zarówno nowe funkcje, jak i poprawki zabezpieczeń. Jeżeli zaniedbasz jej instalację, twój smartfon staje się bardziej podatny na różnego rodzaju ataki, takie jak phishing czy zainfekowanie malware. W dodatku, brak aktualizacji może sprawić, że nie będziesz mógł korzystać z najnowszych funkcji i udogodnień oferowanych przez system. Regularne aktualizowanie oprogramowania zapewni, że twoje urządzenie będzie działało optymalnie i będzie bezpieczne przed zagrożeniami.

Regularnie sprawdzaj swój system za pomocą zaktualizowanego programu antywirusowego

Regularnie sprawdzanie systemu za pomocą programu antywirusowego to jak robienie przeglądów technicznych samochodu. Tak jak mechanik analizuje stan pojazdu, program antywirusowy skanuje komputer w poszukiwaniu zagrożeń. Co więcej, wiele programów antywirusowych wykonuje te skany automatycznie w określonych odstępach czasu, działając w tle i zapewniając ciągłą ochronę. Dzięki temu użytkownik może czuć się bezpieczniej, nawet jeśli nie pamięta o regularnym uruchamianiu skanu.

Po pobraniu nowej aplikacji, pliku czy gry na smartfonie, program antywirusowy uruchamia automatyczny skan. Podczas tego procesu, aplikacja antywirusowa analizuje kod oraz inne elementy pobranego oprogramowania, szukając znanego złośliwego oprogramowania, jak malware czy spyware. Jeżeli skan zakończy się wynikiem negatywnym, oznacza to, że pobrana aplikacja czy gra są wolne od znanych zagrożeń i mogą być bezpiecznie używane. W przypadku wykrycia potencjalnego zagrożenia, program antywirusowy wyświetli ostrzeżenie i zaleci działania, takie jak usunięcie szkodliwej aplikacji.

Nie otwieraj nieznanych linków i załączników

Nie otwieraj linków i załączników od nieznanych lub podejrzanych źródeł, aby zminimalizować ryzyko infekcji malware, ataków phishingowych czy kradzieży danych. Zachowanie ostrożności w tym zakresie jest kluczowym elementem cyberbezpieczeństwa. Otwarcie nieznanych linków lub załączników może prowadzić do kradzieży danych osobowych i poufnych informacji, zainfekowania Twojego urządzenia malware, ransomware czy innym złośliwym oprogramowaniem, umożliwienia atakującym zdalnego dostępu do Twojego urządzenia.

Przykład:

Otrzymujesz e-mail, który wygląda jak wiadomość od Twojego banku, z prośbą o natychmiastowe zalogowanie się na konto w związku z podejrzaną aktywnością. E-mail zawiera link, który prowadzi do strony wyglądającej niemal identycznie jak oficjalna strona Twojego banku. Po wpisaniu swojego loginu i hasła, te dane trafiają w ręce oszustów, którzy mogą teraz zalogować się na Twoje prawdziwe konto bankowe i wykonać nieautoryzowane transakcje.

Zakrywaj obiektyw kamery w laptopie

To prosta, ale skuteczna metoda zabezpieczenia przed potencjalnym nieautoryzowanym dostępem do kamery przez złośliwe oprogramowanie lub hakerów Zakrycie kamery zapobiega potencjalnemu naruszeniu Twojej prywatności przez osoby trzecie, które mogą zdalnie aktywować kamerę bez Twojej wiedzy. Jeżeli haker uzyska dostęp do Twojego laptopa, to dostęp do kamery może być dla niego dodatkowym źródłem informacji o Tobie, Twoim miejscu zamieszkania czy nawykach. W ekstremalnych przypadkach, obrazy z kamery mogą być używane do celów szantażu lub dojścia do innych poufnych informacji.

Przykład:

Możesz użyć specjalnych naklejek przeznaczonych do zakrywania kamer w laptopach, które są łatwo dostępne w sprzedaży. Alternatywnie, kawałek taśmy izolacyjnej czy nawet kartka papieru i kawałek taśmy klejącej mogą być tymczasowym rozwiązaniem.

Wyłącz automatyczne wykrywanie lokalizacji w smartfonie

Ciągłe śledzenie Twojej lokalizacji przez różne aplikacje może naruszać Twoją prywatność. Te dane mogą być zbierane, przechowywane i w niektórych przypadkach sprzedawane stronom trzecim. Jeżeli Twój telefon zostanie zainfekowany przez złośliwe oprogramowanie, hakerzy mogą używać danych o lokalizacji do różnych celów, w tym do dokładniejszego profilowania Twojej osoby lub nawet fizycznego śledzenia. Włączona funkcja lokalizacji może zużywać więcej danych mobilnych oraz energii baterii. Wyłączenie tej funkcji daje Ci większą kontrolę nad tym, kiedy i jakie aplikacje mają dostęp do Twojej lokalizacji.

Przykład:

W ustawieniach smartfona, zwykle w sekcji „Prywatność" lub „Lokalizacja", możesz wyłączyć automatyczne wykrywanie lokalizacji. W niektórych systemach możesz też zarządzać ustawieniami lokalizacji dla poszczególnych aplikacji, co pozwala na bardziej zróżnicowaną kontrolę. Wyłączenie tej funkcji może ograniczyć niektóre funkcje aplikacji, które na niej polegają (np. mapy, usługi pogodowe), ale zyskujesz na tym zwiększenie prywatności i potencjalne bezpieczeństwo.

Nie wykonuj zakupów online i bankowości w publicznych sieciach

Nie wykonuj zakupów online i bankowości w publicznych sieciach Wi-Fi , a jedynie na urządzeniach zabezpieczonych za pomocą uwierzytelniania dwuskładnikowego.

Unikaj wykonywania zakupów online i korzystania z bankowości internetowej na publicznych sieciach Wi-Fi, które są podatne na ataki i przechwytywanie danych. Zamiast tego, korzystaj z urządzeń zabezpieczonych uwierzytelnianiem dwuskładnikowym dla dodatkowej warstwy ochrony.

Przykład:

Załóżmy, że jedziesz pociągiem na długą trasę i zdecydujesz się skorzystać z publicznego Wi-Fi, aby zalogować się do swojego konta bankowego i sprawdzić stan konta lub dokonać przelewu. Niestety, osoba o złych zamiarach również korzysta z tej sieci i posiada narzędzia do przechwytywania transmisji danych. Ustala, że logujesz się do banku i przechwytuje Twoje dane logowania. Później wykorzystuje te dane do nieautoryzowanego dostępu do Twojego konta bankowego. Dlatego zaleca się, aby unikać korzystania z publicznych sieci Wi-Fi dla działań, które wymagają wprowadzenia poufnych informacji. Jeżeli jednak musisz to zrobić, upewnij się, że Twoje urządzenie jest zabezpieczone za pomocą uwierzytelniania dwuskładnikowego i korzystasz z połączenia VPN.

Używaj VPN

VPN (Virtual Private Network, czyli Wirtualna Sieć Prywatna) polega na tworzeniu zaszyfrowanego kanału komunikacyjnego pomiędzy Twoim urządzeniem a specjalnym serwerem VPN. Ten kanał umożliwia bezpieczne i anonimowe przesyłanie danych przez Internet. Po nawiązaniu połączenia z serwerem VPN, Twój rzeczywisty adres IP jest maskowany, a ruch internetowy jest kierowany przez serwer, co zwiększa Twoją prywatność i bezpieczeństwo online. VPN jest szczególnie użyteczny podczas korzystania z publicznych sieci Wi-Fi, gdzie istnieje zwiększone ryzyko przechwycenia danych. Oferuje też możliwość omijania blokad geograficznych i cenzury internetowej.

Przykład:

Korzystanie z publicznego Wi-Fi dla transakcji bankowych czy dostępu do konta bankowego generalnie nie jest zalecane ze względu na potencjalne zagrożenia bezpieczeństwa. Jeśli jednak musisz to zrobić, użycie VPN stanowi dodatkową warstwę ochrony. W tym przypadku, otworzysz aplikację VPN na swoim urządzeniu, zalogujesz się i wybierzesz serwer do połączenia. Po aktywacji połączenia VPN, możesz otworzyć aplikację bankową lub stronę internetową i zalogować się do swojego konta. Dzięki VPN, twoje dane będą zaszyfrowane, co utrudnia ich przechwycenie przez nieautoryzowane osoby. Po zakończeniu operacji bankowych, warto rozłączyć się z VPN, aby oszczędzić zasoby baterii i przepustowość sieci.

Używaj różnych haseł do różnych kont

Każde konto internetowe powinno mieć własne, unikatowe hasło, aby zabezpieczyć się przed ryzykiem włamania lub nieautoryzowanego dostępu. Jeżeli jedno konto zostaje naruszone, pozostałe konta pozostają bezpieczne, o ile używane są różne hasła.

Przykład:

Załóżmy, że używasz tego samego hasła dla swojego konta e-mailowego, konta bankowego i konta na portalu społecznościowym. Jeśli hakerzy zdobędą dostęp do jednego z tych kont, automatycznie zyskają możliwość dostępu do pozostałych, co może prowadzić do nieautoryzowanych transakcji bankowych i potencjalnej utraty środków, wykorzystania twojego konta e-mailowego do resetowania haseł i przejęcia innych kont rozpowszechniania niechcianych lub szkodliwych treści w Twoim imieniu na portalach społecznościowych kradzieży i wykorzystania Twoich danych osobowych w celach oszustwa lub kradzieży tożsamości.

Nie klikaj przycisków zbyt szybko w wyskakujących okienkach

Nie klikaj przycisków zbyt szybko: przyjrzyj się uważnie każdemu wyskakującemu okienku, aby zobaczyć, jakie masz opcje. Impulsywne i nieprzemyślane klikanie może prowadzić do przypadkowego udostępnienia informacji, takich jak: hasła, numery kart kredytowych czy adresy e-mail, instalacji złośliwego oprogramowania czy innych niebezpiecznych konsekwencji. Uważne czytanie i zrozumienie komunikatów i okienek dialogowych to kluczowy element cyberbezpieczeństwa.

Przykład:

Często przewijamy treści w Internecie co sprawia, że klikamy na „Akceptuj" czy „Dalej" bez głębszej refleksji. Jest to wynik nawyku i braku świadomości, że nawet małe decyzje mogą mieć duże konsekwencje. Czasami jesteśmy pod presją czasu lub stresem, co skłania nas do szybkich, nierozważnych decyzji. W tym stanie jesteśmy mniej ostrożni i mniej krytyczni. Możemy być przekonani, że nic złego nam się nie przydarzy, co jest znanym psychologicznym zjawiskiem nazywanym efektem optymizmu. Taka postawa może prowadzić do zaniedbania podstawowych zasad bezpieczeństwa. W erze Internetu jesteśmy zalewani informacjami, co może prowadzić do zmęczenia i braku ostrożności. Możemy zignorować istotne szczegóły, ponieważ nasza zdolność do przetwarzania informacji jest ograniczona. Czasami niewłaściwie oceniamy ryzyko, sądząc, że konkretna strona internetowa lub aplikacja jest bezpieczna, co prowadzi do zaniedbania ostrzeżenia czy komunikatu.

Techniki używane przez oszustów są ciągle udoskonalane, stają się coraz bardziej zaawansowane i trudne do wykrycia. Dlatego ważne jest, aby być na bieżąco z metodami zabezpieczeń i zachować ostrożność podczas korzystania z Internetu. Znajomość technik często kierowanych przeciwko osobom w wieku 60+ może znacznie zwiększyć ich świadomość i odporność na różne formy oszustw internetowych. Dzięki temu mogą Państwo korzystać z Internetu z mniejszym ryzykiem stania się ofiarą wykorzystania czy oszustwa.

6. Główne techniki używane przez oszustów

Phishing

Jest to technika wykorzystywana przez oszustów, którzy próbują wyłudzić od Ciebie poufne informacje, takie jak hasła do kont bankowych czy dane do kart kredytowych. Termin „phishing" pochodzi od angielskiego słowa „fishing", co oznacza „wędkowanie". W tym kontekście, oszuści „zarzucają sieć" w postaci fałszywych e-maili czy linków, mając nadzieję, że „złowią" nieświadomą osobę, która poda im swoje dane osobowe lub finansowe. Metafora łowienia ryb dobrze oddaje mechanizm działania tego typu oszustwa. Oszuści „zakładają przynętę" w formie wiadomości e-mail wyglądającej na oficjalną komunikację od banku, serwisu internetowego czy innej instytucji. Jeśli „ryba" – czyli potencjalna ofiara – „ugryzie", czyli kliknie w link i poda swoje dane, oszuści "zaciągają haczyk", uzyskując dostęp do konta, z którego mogą wyprowadzić środki lub wykonać inne nieautoryzowane działania.

Tak jak wędkarz musi znać techniki i taktyki, aby złowić rybę, tak oszuści phishingowi są coraz bardziej wyrafinowani w swoich metodach. Dlatego ważne jest, aby być zawsze czujnym i podejrzewać wszelkie wiadomości czy linki, które proszą o podanie ważnych danych osobistych.

Phishingowcy często są dobrze zorientowani w technologii i psychologii, umieją manipulować ludźmi i wykorzystywać ich słabości (np. ciekawość, strach, niewiedzę) do osiągnięcia swoich celów.

Kradzież tożsamości

Oszuści mogą próbować przejąć Twoją tożsamość, aby na przykład wykonać zakupy lub wziąć pożyczki na Twoje nazwisko. Uważaj na dzielenie się informacjami osobistymi w Internecie. Oto kilka typów informacji osobistych, którymi lepiej nie dzielić się publicznie w Internecie, aby zminimalizować ryzyko kradzieży tożsamości: numer pesel, dane konta bankowego, dane karty kredytowej, hasła i dane do logowania, adres zamieszkania, numer telefonu, skany lub zdjęcia dokumentów osobistych, adres e-mail, data urodzenia.

Malware

Złośliwe oprogramowanie, które może zainfekować Twój komputer kradnąc Twoje dane. Zawsze aktualizuj oprogramowanie i korzystaj z antywirusa.

Malware (złośliwe oprogramowanie) można porównać do trojańskiego konia. Na pierwszy rzut oka, plik lub link, który go przenosi, może wydawać się niewinny lub nawet użyteczny. Tak jak mieszkańcy Troi witali drewnianego konia jako dar, tak użytkownik może ściągnąć i uruchomić zainfekowany plik, myśląc, że jest on bezpieczny. Jednak w rzeczywistości ukrywa się w nim coś złośliwego, co po uruchomieniu zaczyna działać na niekorzyść użytkownika, podobnie jak żołnierze ukryci wewnątrz trojańskiego konia.

Otworzenie "trojańskiego konia" na swoim komputerze lub urządzeniu mobilnym może doprowadzić do różnych negatywnych konsekwencji, takich jak kradzież danych, zainfekowanie systemu innymi rodzajami złośliwego oprogramowania czy nawet przejęcie kontroli nad urządzeniem. Dlatego ważne jest, aby być ostrożnym i dobrze zabezpieczonym przed takimi zagrożeniami.

Złośliwe oprogramowanie (malware) może być ukryte w różnego rodzaju plikach, które na pierwszy rzut oka wydają się niewinne, takich jak filmy, książki czy pliki muzyczne. Oszuści, które tworzą malware, często korzystają z popularności pewnych treści, aby zwabić użytkowników do ich ściągnięcia.

Na przykład, możesz myśleć, że ściągasz najnowszy hit filmowy czy muzyczny, ale w rzeczywistości plik może zawierać złośliwy kod. Po ściągnięciu i otwarciu takiego pliku, malware może być aktywowane i zainfekować Twój komputer czy urządzenie mobilne, prowadząc do różnych problemów, takich jak kradzież danych osobowych, zablokowanie systemu czy nawet szantaż.

Dlatego zawsze należy być bardzo ostrożnym przy ściąganiu plików z nieznanych źródeł i korzystać z zaufanych platform do pobierania treści. Oprogramowanie antywirusowe również mogą pomóc w identyfikacji i blokowaniu złośliwych plików.

Sfałszowane strony internetowe

Strony, które udają inne, często znane serwisy, aby wyłudzić od Ciebie dane. Zawsze sprawdzaj adres strony w pasku przeglądarki. Strony internetowe, które udają inne, znane serwisy, można porównać do oszustów, którzy udają na ulicy policjantów lub innych urzędników. Podobnie jak fałszywy policjant może zatrzymać Cię na ulicy, prosząc o okazanie dokumentów w celu kradzieży tożsamości, tak fałszywa strona internetowa udaje rzeczywistą, aby wyłudzić twoje dane. Tak jak w życiu rzeczywistym sprawdzasz identyfikator osoby, która twierdzi, że jest urzędnikiem, w cyfrowym świecie zawsze powinieneś sprawdzać adres strony w pasku przeglądarki. Jeśli coś wydaje się podejrzane, lepiej nie podawać żadnych informacji i zweryfikować wiarygodność strony przez inne, pewne kanały.

Nie wszystkie strony używają zabezpieczonych połączeń. Zawsze zwracaj uwagę, czy adres strony zaczyna się od „https://” zamiast „http://”. Można to porównać do różnicy między przesyłką poleconą a zwykłą przesyłką. Jeśli wysyłasz list czy paczkę w sposób polecony, masz pewność, że zostanie ona odpowiednio zabezpieczona i dostarczona tylko do wyznaczonej osoby. W przypadku zwykłej przesyłki takiej pewności nie masz — każdy może ją otworzyć czy też zagubić. W kontekście Internetu, „https://” to jak przesyłka polecona: zapewnia dodatkowe zabezpieczenie, szyfrując twoje dane, tak że są one trudniejsze do przechwycenia przez niepowołane osoby. Natomiast „http://” to jak zwykła przesyłka: twoje dane przesyłane są bez dodatkowego zabezpieczenia, co sprawia, że są bardziej narażone na kradzież. Dlatego zawsze zwracaj uwagę na to, czy strona korzysta z „https://” zamiast „http://”, szczególnie jeśli masz zamiar wprowadzać wrażliwe informacje. Oszuści często tworzą fałszywe strony, które wyglądają jak popularne, zaufane serwisy, ale nie używają zabezpieczonego połączenia HTTPS. Zamiast tego używają nieszyfrowanego połączenia HTTP, co sprawia, że jakiekolwiek dane wprowadzone na tej stronie, takie jak hasła czy informacje o karcie kredytowej, są łatwe do przechwycenia. Często te strony są zaprojektowane tak, aby wyglądać niemal identycznie jak oryginalne strony, na przykład banku, serwisu pocztowego lub sieci społecznościowej. Mogą mieć podobne logo, układ i nawet adres URL może być zbliżony do oryginału (np. „facebokk” zamiast „facebook”).

Dlatego zawsze warto sprawdzić, czy strona używa połączenia HTTPS, zwłaszcza jeśli zamierzasz wprowadzić wrażliwe dane. Jeśli zauważysz, że coś wygląda podejrzanie, najlepiej jest zamknąć stronę i nigdy nie wprowadzać żadnych danych.

7. Zakończenie

Nie zapomnij, że wiedza i ostrożność to Twoje najważniejsze narzędzia w dbaniu o cyfrowe bezpieczeństwo. Warto regularnie przypominać sobie o zasadach, które omówiliśmy, i aktualizować je w miarę pojawiania się nowych zagrożeń. Ale to nie wszystko — podziel się swoją wiedzą z rodziną i przyjaciółmi. Im więcej osób będzie świadomych ryzyk i sposobów ich minimalizacji, tym bezpieczniej będzie dla nas wszystkich. Zainwestuj w swoje bezpieczeństwo i bezpieczeństwo swoich bliskich; to inwestycja, która zawsze się opłaca. Niech ta broszura będzie początkiem Twojej świadomej przygody w świecie cyfrowym.

8. Słownik

Ograniczone zaufanie w Internecie: zasada ograniczonego zaufania w Internecie działa podobnie jak zasady ostrożności na drodze. Na drodze nie ufamy "na słowo" innym kierowcom, nawet jeśli dają sygnały czy migają światłami. Zamiast tego, stosujemy się do zasad i znaków drogowych, korzystamy z lusterek i obserwujemy otoczenie. Podobnie w Internecie, nie ufamy od razu nieznajomym osobom czy serwisom. Weryfikujemy informacje, unikamy klikania w nieznane linki, korzystamy z szyfrowania i innych mechanizmów zabezpieczających. Ograniczone zaufanie oznacza, że zawsze weryfikujemy i zabezpieczamy się przed możliwymi zagrożeniami, zamiast bezrefleksyjnie ufać. W świecie cyfrowym oszustwo często przybiera bardzo wyrafinowane i przebiegłe formy. Dzięki technologii oszuści mają możliwość podszywania się nie tylko pod instytucje, ale także pod osoby, którym zwykle ufamy, takie jak członkowie rodziny, przyjaciele czy osoby zaufania publicznego. Dlatego zawsze warto podwójnie weryfikować informacje i być ostrożnym, nawet jeśli komunikat wydaje się pochodzić od kogoś, kogo znamy i uważamy za zaufaną osobę. W sytuacjach, w których proszeni jesteśmy o podanie wrażliwych danych czy wykonanie jakichś działań, jak np. przesłanie pieniędzy, najlepiej jest dodatkowo potwierdzić tożsamość osoby przez inny kanał komunikacji.

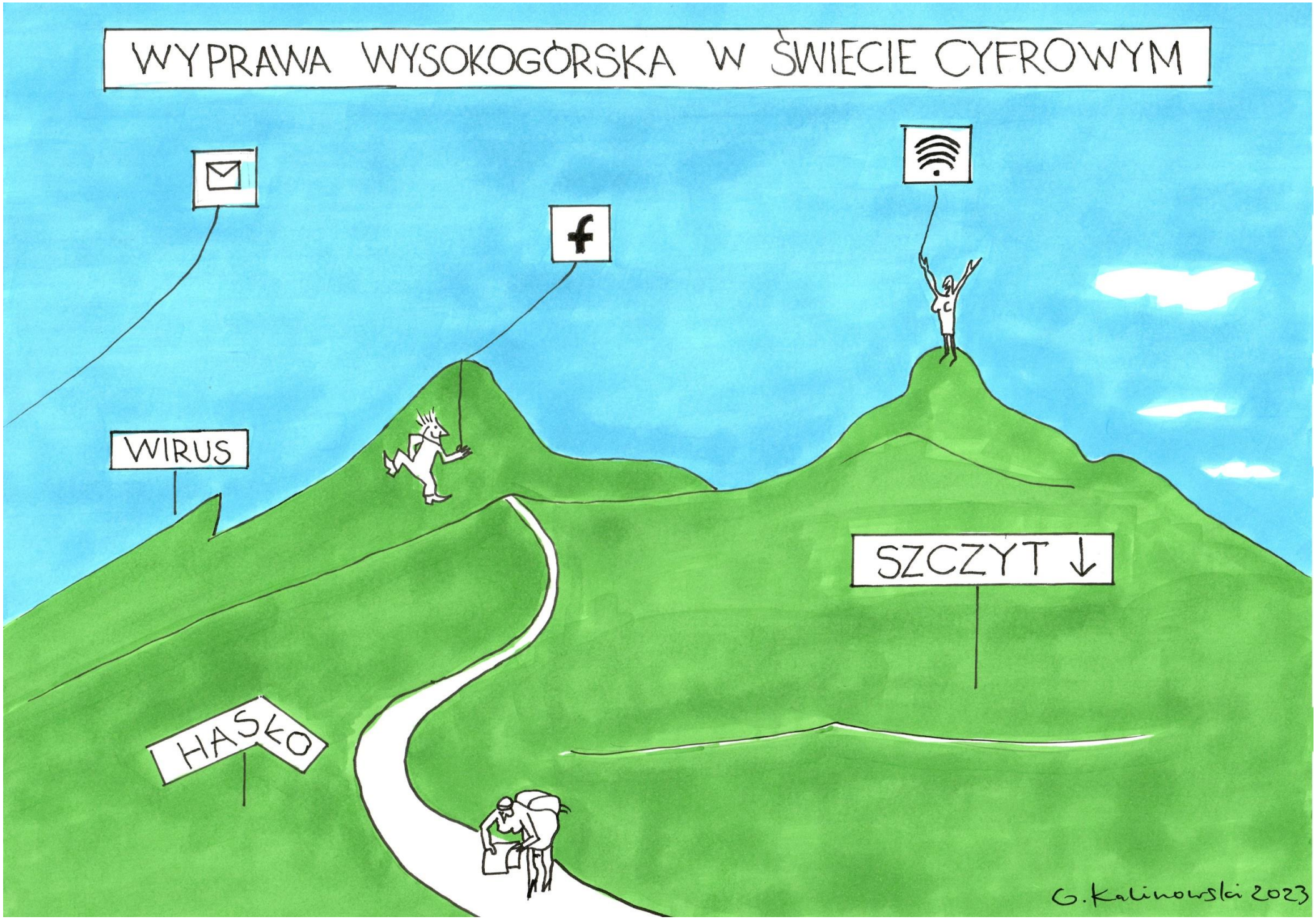
Paserstwo internetowe: oszuści w Internecie często oferują do sprzedaży rzeczy, które zostały nielegalnie nabyte, czyli praktykują paserstwo. Sprzedają różnego rodzaju aktywa, od elektroniki po luksusowe towary, twierdząc, że są ich legalnymi właścicielami, podczas gdy w rzeczywistości nie mają do nich praw własności. Osoby, które kupują takie przedmioty, często nieświadomie uczestniczą w przestępczej działalności, ponieważ kupno od pasera również jest uznawane za przestępstwo lub wykroczenie. Osoby w wieku 60+ mogą nieświadomie nabyć skradziony towar, co nie tylko naraża je na straty finansowe, ale również może skutkować konsekwencjami prawnymi. Aby bronić się przed paserstwem w Internecie, warto weryfikować autentyczność sprzedawców i produktów, unikać zbyt niskich cen i korzystać z bezpiecznych metod płatności. Zawsze używaj szyfrowanych połączeń, dokumentuj transakcje i zachowaj ostrożność przy klikaniu w linki czy otwieraniu załączników. Regularne aktualizacje oprogramowania i edukacja na temat różnych typów oszustw również zwiększają poziom bezpieczeństwa.

Piramida finansowa: oszukańczy model biznesowy, opierający się głównie na rekrutacji nowych uczestników zamiast na rzeczywistej sprzedaży towarów czy usług. Uczestnicy na niższych poziomach wpłacają środki finansowe, które są przekazywane tym, którzy są wyżej w hierarchii. Struktura ma kształt piramidy: im wyżej ktoś się znajduje, tym więcej potencjalnie zarabia. Jednakże, system ten jest niezrównoważony i z czasem prowadzi do jego upadku, gdyż nowi uczestnicy nie są w stanie osiągać zysków. W rezultacie, tylko osoby u szczytu piramidy odnoszą realne korzyści, podczas gdy pozostali uczestnicy są oszukiwani. Ze względu na swój wprowadzający w błąd

charakter, piramidy finansowe są nielegalne w wielu krajach. Amber Gold to polska firma działająca w latach 2009–2012, która zajmowała się inwestowaniem w złoto i inne metale szlachetne. Choć firma oficjalnie prezentowała się jako instytucja finansowa oferująca atrakcyjne zyski z inwestycji, w praktyce jej działalność miała wiele cech piramidy finansowej. Zgromadzone środki od nowych inwestorów były używane do wypłat dla osób, które zainwestowały wcześniej, zamiast faktycznego inwestowania w metale. W 2012 roku firma upadła, a jej założyciel został aresztowany i oskarżony o prowadzenie działalności o charakterze oszukańczym. Wielu inwestorów straciło zgromadzone środki, a sprawa zyskała szeroki rozgłos w mediach. Chociaż Amber Gold nie została oficjalnie sklasyfikowana jako piramida finansowa przez polskie sądy, jej działalność miała wiele cech charakterystycznych dla tego typu oszustw. Jej upadek i negatywne konsekwencje dla inwestorów są często przytaczane jako przykład zagrożeń związanych z inwestowaniem w nieuregulowane i niejasne schematy finansowe.

Pranie pieniędzy: proces, w którym nielegalnie uzyskane środki finansowe są przemieszczane i przetwarzane przez różne metody i platformy online, aby "oczyścić" je i wprowadzić do legalnego obiegu finansowego. Celem jest zatarcie śladów pochodzenia tych środków, tak aby były one trudne do wykrycia i prześledzenia przez organy ścigania. Na przykład, oszust może skontaktować się z osobą w wieku 60+, udając przedstawiciela banku lub inną zaufaną instytucję, i poprosić o przesłanie pieniędzy na określone konto „w celu weryfikacji”. W rzeczywistości te środki są prane i przekierowywane na inne konta, często w różnych krajach, aby zatrzeć ich źródło. Innym przykładem może być tzw. „oszustwo na wnuczka”, gdzie oszust udaje bliską rodzinę i prosi osobę w wieku 60+ o przesłanie pieniędzy na fałszywy cel, tak jak ratowanie życia lub wyjście z trudnej sytuacji. Po otrzymaniu pieniędzy, oszust „czyści” je, przechodząc przez różne konta lub inwestując w kryptowaluty, przed wypłaceniem w formie „czystych” środków. W wielu przypadkach osoby w wieku 60+ nie zdają sobie sprawy, że zostały wykorzystane w procesie prania pieniędzy. Pieniądze, które zostały nielegalnie uzyskane od osób w wieku 60+, przechodzą przez różne konta, inwestycje lub nawet kryptowaluty, aby zatrzeć ich pochodzenie. W efekcie, te środki stają się "legalne" w oczach prawa, co znacząco utrudnia lub wręcz uniemożliwia ich odzyskanie.

Podobnie jak turysta poruszający się w górach musi zdobyć odpowiednią wiedzę i umiejętności przed wyruszeniem na szczyt, tak i osoby korzystające ze świata cyfrowego powinny poznać zasady bezpieczeństwa cyfrowego. W górach niezbędny jest odpowiedni sprzęt, w cyfrowym świecie za to odpowiadają oprogramowanie zabezpieczające, silne hasła i aktualizacje systemów. Turysta często polega na doświadczonym przewodniku, w świecie cyfrowym pomocne są osoby z większym doświadczeniem technologicznym. Wspinaczka wiąże się z ryzykami takimi jak lawiny czy upadki z wysokości, w cyfrowym świecie zagrożenia to oszustwa i cyberprzemoc. Tak jak warunki w górach są nieprzewidywalne, technologia jest dynamiczna, dlatego ważne jest, aby być na bieżąco z nowościami i aktualizacjami, aby korzystać z Internetu w sposób bezpieczny i efektywny. Mimo wszystkich trudności, zarówno osiągnięcie szczytu w górach, jak i w świecie cyfrowym, oferuje niezwykłe nagrody: spektakularne widoki oraz dostęp do nieograniczonych zasobów informacji, komunikacji i rozrywki.


WYPRAWA WYSOKOGÓRSKA W ŚWIECIE CYFROWYM
WIRUS
HASŁO
SZCZYT ↓
G. Kalinowski 2023

9. Materiały do samodzielnej pracy

1. Jerzy Surma, profesor SGH, *ABC Cyberbezpieczeństwa | Krok 1: Rozpoznanie Zagrożeń*, https://youtu.be/x0LsaBYibew?feature=shared (dostęp: 14.10.2023).
2. Jerzy Surma, profesor SGH, *ABC Cyberbezpieczeństwa | Krok 2: Obrona Przed Atakami*, https://youtu.be/im9_-esP0Vw?feature=shared (dostęp: 14.10.2023).
3. Jerzy Surma, profesor SGH, *ABC Cyberbezpieczeństwa | Krok 3: Rekonwalescencja Po Ataku*, https://youtu.be/TC-F2BtWjig?feature=shared (dostęp: 14.10.2023).
4. Ministerstwo Cyfryzacji, *Sprawdź, czy Twoje dane są bezpieczne*, https://bezpieczne-dane.gov.pl/ (dostęp: 14.10.2023).
5. NASK-PIB/CERT Polska, *Raport roczny z działalności CERT Polska 2022*, https://cert.pl/uploads/docs/Raport_CP_2022.pdf#page=8 (dostęp: 14.10.2023) - Raporty roczne z działalności CERT Polska, zawierające zebrane dane o zagrożeniach dla polskich użytkowników Internetu.
6. NASK-PIB/CERT Polska, Jak bezpiecznie kupować w Internecie, https://cert.pl/uploads/docs/CERT_poradnik_zakupowy.pdf (dostęp: 14.10.2023).
7. NASK-PIB/CERT Polska, *Poradnik ransomware*, https://cert.pl/uploads/docs/CERT_Polska_Poradnik_ransomware.pdf (dostęp: 14.10.2023).
8. NASK-PIB/CERT Polska, *Jak się nie dać złapać w sieci nieuczciwych sprzedawców*, 2019, https://cert.pl/uploads/docs/PORADNIK_SKLEPY_CERT_AHS.pdf
9. NASK-PIB/CERT Polska, *Bezpieczna poczta i konta społecznościowe*, 2021, https://cert.pl/uploads/docs/CERT_Polska_Bezpieczna_poczta_i_konta_spolecznosciowe.pdf (dostęp: 14.10.2023).
10. NASK-PIB, 2022, *Poradnik ABC cyberbezpieczeństwa*, https://it-szkola.edu.pl/publikacje,plik,90 (dostęp: 14.10.2023).
11. NASK-PIB/CERT Polska, Kompleksowo o hasłach, 2022, https://cert.pl/posts/2022/01/kompleksowo-o-haslach/
12. Bądź z innej bajki, #grooming, https://www.gov.pl/web/badz-z-innej-bajki/grooming (dostęp: 14.10.2023) - Jeśli zamierzasz porozmawiać ze swoimi wnukami na temat bezpieczeństwa w Internecie, ta broszura to świetny punkt wyjścia. Zawiera ona fundamentalne informacje i podstawowe zrozumienie zagrożeń online, które każde dziecko powinno znać. Dzięki temu będziesz mógł przeprowadzić świadomą i rzeczową rozmowę na ten ważny temat. Choć to tylko początek, stanowi solidną podstawę, na której możesz kontynuować dalszą edukację zarówno własną, jak i swoich wnuków.
13. Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz.U. 2018 poz. 1560).
14. CERT Polska – Zgłoś incydent, https://incydent.cert.pl/
15. NASK – Państwowy Instytut Badawczy, https://www.nask.pl/
16. NASK, 2019, *Szkodliwe treści w Internecie. Nie akceptuję, reaguję. Poradnik dla rodziców*, https://www.gov.pl/attachment/b0d64cb0-3b74-4ca2-9561-29cb8490ac28 - kolejna publikacja warta przeczytania przed rozmową z wnukami na tematy bezpieczeństwa w sieci.

Rządowy program wieloletni na rzecz Osób Starszych „Aktywni+" na lata 2021–2025

Program został zainicjowany w 2021 r. Zakłada „1) wzrost zaangażowania osób starszych w kontakty społeczne poprzez wzbogacenie oferty zagospodarowania ich czasu wolnego; 2)zwiększenie zaangażowania osób starszych w procesy partycypacyjne zachodzące w życiu publicznym; 3) podnoszenie kompetencji cyfrowych seniorów oraz kształtowanie postaw sprzyjających wykorzystywaniu nowych technologii w życiu codziennym; 4) budowanie pozytywnego wizerunku starości i starzenia się oraz rozwijanie kompetencji społecznych (wiedzy, umiejętności, postaw) wobec starości u osób w każdym wieku".
Źródło: Uchwała nr 167 Rady Ministrów z dnia 16 listopada 2020 r. w sprawie ustanowienia programu wieloletniego na rzecz Osób Starszych "Aktywni+" na lata 2021-2025 (Monitor Polski, poz. 1125 z 2020 r.)

Projekt Fundacji Rozwoju Przedsiębiorczości im. Prof. Jerzego Dietla
Inicjatyw@ 60 plus – aktywizacja cyfrowa.

W programie projektu:

I. Warsztaty z zakresu wykorzystania komputera i Internetu w życiu codziennym
- Obsługa komputera i smartfona przez seniora
- Jak korzystać z Internetu
- Jak zakładać i korzystać z profilu w mediach społecznościowych
- Arkusz kalkulacyjny MS Excel w życiu codziennym
- Czas wolny w sieci

II. Spotkania informacyjno-integracyjne
- Psychologia w procesie włączenia cyfrowego
- Zdrowie a nowe technologie

III. Popularyzacja wykorzystania nowych technologii w życiu seniorów poprzez organizację wycieczek do:
- Warszawskiego Muzeum Komputerów i Gier
- Centrum Komiksu i Narracji Interaktywnej w EC1 w Łodzi

oraz opracowanie broszury „Bezpieczeństwo w sieci"

IV. Spotkanie integracyjne połączone z wykładem motywacyjnym i podsumowaniem projektu

Projekt Inicjatyw@ 60+ - aktywizacja cyfrowa dofinansowany ze środków rządowego programu wieloletniego na rzecz Osób Starszych „Aktywni+" na lata 2021–2025


NIE PODDAJEMY SIĘ
G. Kalinowski 2023