SARE°
DIGITREE GROUP

HAKER

THE GAME IS OVER!

E-BOOK O BEZPIECZEŃSTWIE W SIECI Bo chcemy, abyś był bezpieczny.

Bezpieczeństwo internetowe wydaje Ci się **ogranym tematem?**

Uważasz zmianę hasła za **niepotrzebny wysiłek?**

Myślisz, że jeśli ktoś może paść ofiarą cyberprzestępców, **to na pewno nie Ty?**

SARE°
DIGITREE GROUP

E-BOOK O BEZPIECZEŃSTWIE W SIECI Bo chcemy, abyś był bezpieczny.

Spis treści

Wstęp

Internetowy przestępca tzw. cracker, potocznie nazywany hackerem, jest anonimowy i zakłada maskę. Jest jak Joker. Będzie przekonywał, że nic Ci nie grozi. Uważaj, nie daj się wciągnąć w tę grę, i nie daj się rozegrać.

W kwestiach związanych z bezpieczeństwem w sieci, to Ty zawsze musisz mieć asa w rękawie!

Co czujesz na myśl, że ktoś potrafi wejść do Twojego domu mimo zamkniętych drzwi? Przez dłuższy czas będzie Cię dyskretnie obserwował. W pewnym momencie niezauważony, wykradnie Twoje dane osobowe, aby je sprzedać lub zaciągnąć kredyt. **Może skopiować inne prywatne lub biznesowe informacje**. Wreszcie może je zaszyfrować i zażądać okupu.

W internecie przestępcy pracują 24/7. Mają sprytnych pomocników - programy, które nieustannie sprawdzają, kto nie domknął drzwi. Oszuści zastawiają pułapki i cierpliwie czyhają na błąd użytkownika. W odróżnieniu od kradzieży dokumentów lub włamania do domu, kradzież internetowa wydaje się wirtualna... Jest jednak jak najbardziej realna i potrafi być dotkliwa. Poza stratą pieniędzy możesz zostać ograbiony z ważnych danych osobistych lub biznesowych informacji, które mogą trafić do sieci.

Dlaczego to Ty jesteś problemem?

Jak mawiają specjaliści od bezpieczeństwa IT: *problem znajduje się między klawiaturą a krzesłem (The Problem Exist Between Keyboard and Chair, PEBKAC).* **Tak, to człowiek jest najsłabszym ogniwem w długim łańcuchu zabezpieczeń**.

Dlaczego? Załóżmy, że posiadasz aktualny system operacyjny, włączony firewall, program antywirusowy, VPN, bezpieczne WiFi. Od strony technologicznej czujesz się bezpiecznie. Bezpieczny komputer jest jak dobrze zabezpieczony dom: antywłamaniowe drzwi, dobre zamki, alarm.

Pamietaj jednak, że **wiedzą o tym również przestępcy, którzy szukają luk w systemach bezpieczeństwa, przeglądarkach, ale również wykorzystują ludzkie słabości**. Zamiast wyłamywać zamek w drzwiach, chcą Cię przekonać, abyś nie przekręcał klucza - albo uchylił okno - wówczas wejdą niepostrzeżenie.

Zasada Ograniczonego Zaufania

W internecie, jak na drodze - musisz zachować zasadę ograniczonego zaufania. Gdy wsiadasz do auta, zapinasz pasy. Wybierasz samochód wyposażony w systemy bezpieczeństwa. Niezależnie jednak od inteligencji technologii, to Ty wciąż samodzielnie podejmujesz decyzje. Podobnie jest z bezpieczeństwem w sieci. Oprogramowanie daje Ci ochronę przed wirusami, ostrzega przed niebezpiecznymi stronami, blokuje ataki z zewnątrz. Ale **nie uchroni Cię przed próbą ataku, gdy uznasz za wiarygodny e-mail z banku** (który nie wpadł do SPAMu) lub wiadomość SMS o konieczności dopłaty za paczkę. To jednak od Ciebie zależy czy klikniesz w przesłany link i pobierzesz złośliwe oprogramowanie.

Jaki był sekret Kevina Mitnicka, legendarnego hackera z lat 90., który odsiedział 5 lat w więzieniu? - Łamałem ludzi, a nie hasła - taki był jego sposób. **Jeśli ktoś chce uzyskać dostęp do danych przechowywanych na komputerze - i tak go uzyska**. To kwestia czasu, umiejętności i odpowiedniej sumy pieniędzy. Ty jednak możesz utrudnić atak na tyle, że nie będzie opłacalny. Nie ulegaj emocjom, bądź podejrzliwy, gdy tylko coś odbiega od normy. Zachowaj w internecie poker face.

Nie daj się złowić!

Najpopularniejsza metoda wyłudzenia danych to **PHISHING** - połączenie słów fishing (wędkowanie) i phreaking (oszukiwanie systemów telekomunikacyjnych). Phishing to taktyka cyberprzestępców, której celem jest wyłudzenie określonych informacji - na przykład przejęcia **danych logowania, szczegółów karty kredytowej) lub nakłonienia ofiary do określonych działań**. Hakerzy podszywają się pod osobę lub znaną instytucję (np. bank, pocztę, operatora komórkowego, czy firmę energetyczną), której Twoje dane są niezbędne do świadczenia usług.

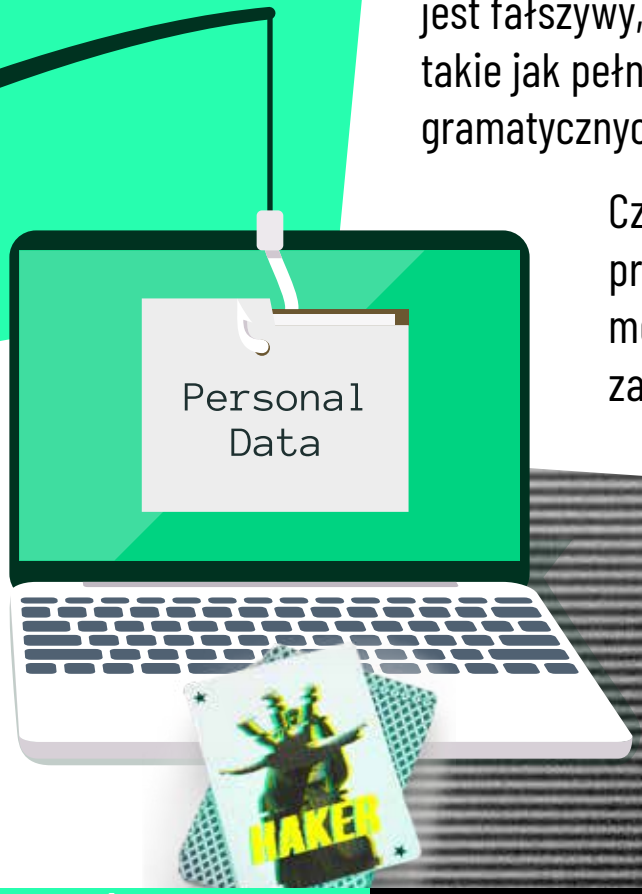
Najczęściej próby wyłudzeń phishingowych otrzymujemy w postaci fałszywej wiadomości e-mail, SMSach oraz poprzez komunikatory, np. w social mediach. Takie wiadomości najczęściej zawierają **link lub załącznik do pobrania złośliwego oprogramowania**. To działanie oparte na prostej socjotechnice, wiedzy o błędach w ludzkim zachowaniu.

Nie daj się złowić!

Przykład?

E-mail, rzekomo z Twojego banku z informacją, że z powodu podejrzenia włamania należy zmienić hasło, ma sprawić, że część osób pod wpływem impulsu zareaguje bezkrytycznie.
Jeśli przypuszczasz, że otrzymany link, np. od firmy sprzedającej energię jest fałszywy, nie klikaj w niego! Zwróć uwagę na elementy wiadomości, takie jak pełna nazwa nadawcy - sprawdź, czy nie zawierają błędów gramatycznych lub ortograficznych.

Czy wiesz, że Twoje dane mogą trafić w ręce przestępcy przez tzw. **keylogger** - złośliwe oprogramowanie monitorujące klawiaturę użytkownika, zapisujące hasła i inne poufne dane?



NASZ PROTIP

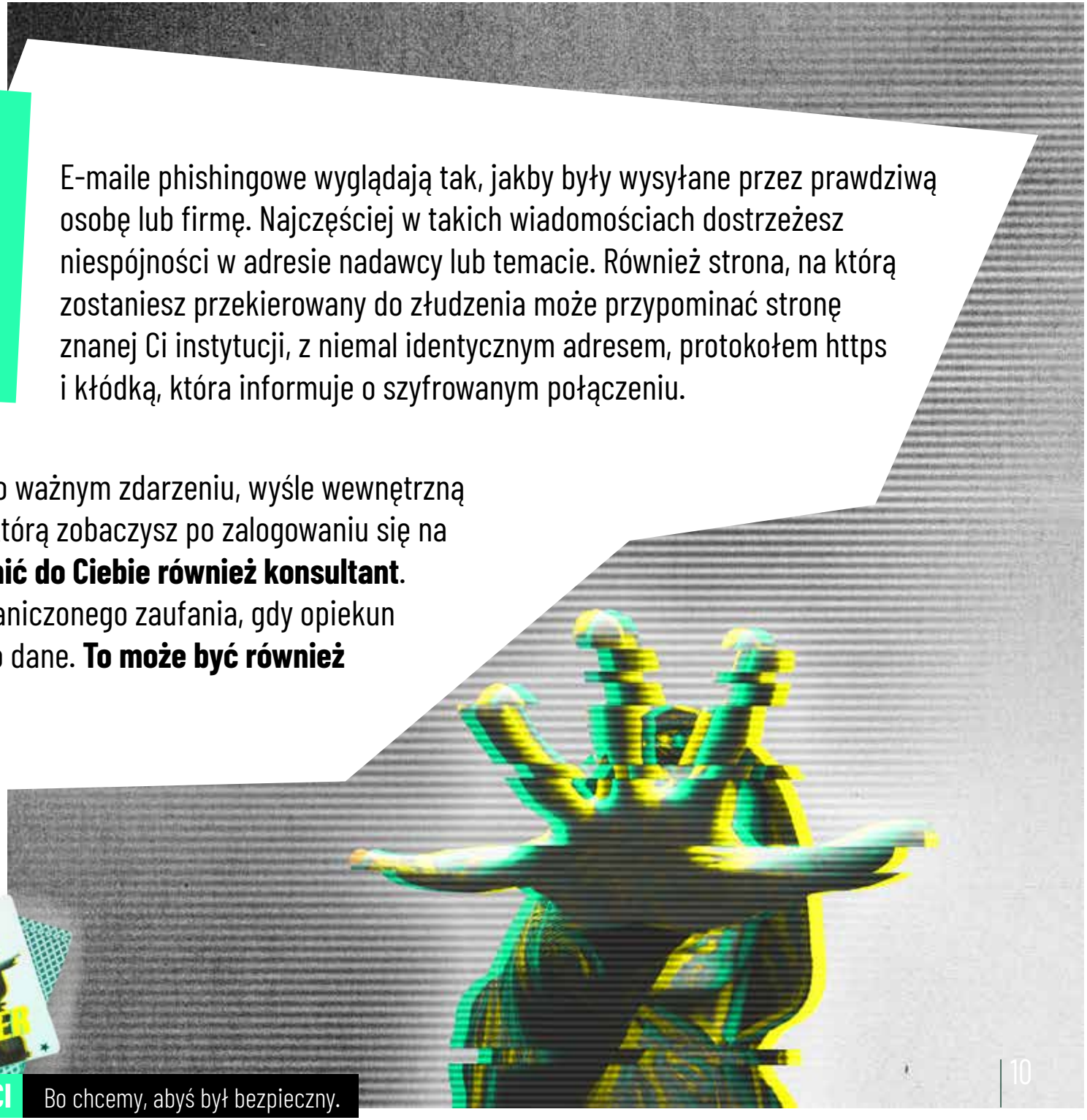
Nie odwiedzaj podejrzanych stron. Uważaj na podejrzane ankiety, sondy od nieznanych nadawców wiadomości z ofertą darmowego przetestowania darmowego produktu. Nie pobieraj oprogramowania, darmowych gier czy wygaszaczy ekranu z niepewnych źródeł. Pobrane oprogramowanie szpiegowskie będzie wyglądać jak zwykły plik. Regularnie aktualizuj przeglądarkę i system operacyjny. Koniecznie korzystaj z oprogramowania antywirusowego, które pomaga w ochronie przed złośliwymi programami i ostrzeże przed stronami wyłudzającymi informacje. Pamiętaj jednak, żeby nie polegać na antywirusie w 100% - w wielu przypadkach daje złudne poczucie bezpieczeństwa.

Niestety nie ma JEDNEGO skutecznego narzędzia do walki ze złośliwym oprogramowaniem.

Jak rozpoznać atak hakerski?

E-maile phishingowe wyglądają tak, jakby były wysyłane przez prawdziwą osobę lub firmę. Najczęściej w takich wiadomościach dostrzeżesz niespójności w adresie nadawcy lub temacie. Również strona, na którą zostaniesz przekierowany do złudzenia może przypominać stronę znanej Ci instytucji, z niemal identycznym adresem, protokołem https i kłódką, która informuje o szyfrowanym połączeniu.

Gdy bank zechce poinformować Cię o ważnym zdarzeniu, wyśle wewnętrzną wiadomość w systemie bankowym, którą zobaczysz po zalogowaniu się na koncie. W tej sprawie może **zadzwonić do Ciebie również konsultant**. Ale i tu musisz stosować zasadę ograniczonego zaufania, gdy opiekun będzie szczegółowo wypytywał Cię o dane. **To może być również próba wyłudzenia informacji**.



NASZ PROTIP

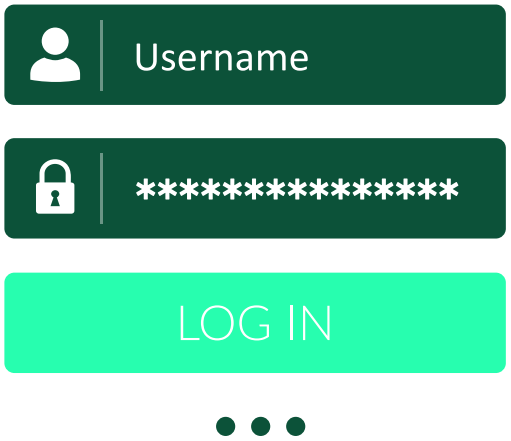
Dlatego, jeśli masz wątpliwości, samodzielnie zadzwoń do banku. Uważaj na fałszywych ekspertów ds. bezpieczeństwa, którzy mogą wysłać wiadomość informującą, że na Twoim komputerze wykryto wirusa i że zajmą się naprawą za Ciebie. Jeśli podejrzewasz, że może to być próba ataku hakerskiego, nie otwieraj takich wiadomości.

Serwis Niebezpiczenik.pl ujawnił jak oszuści, podając się za pracowników działu bezpieczeństwa mBanku, informowali o podejrzanej transakcji na koncie i konieczności zainstalowania aplikacji, która sprawdzi czy telefon nie jest zawirusowany. Jej pobranie i uruchomienie było jednoznaczne z utratą kontroli nad telefonem i przejęciem danych przez przestępców. Informacje o numerze telefonu i karty pochodziła prawdopodobnie z wycieku danych z serwisu Aliexpress, bo przestępcy używali fałszywych imion, j kich użytkownicy użyli, zakładając konto.

Stwórz ********** mocne hasło!

Mocne hasło to pierwszy krok do bezpieczeństwa. Chociaż może Cię to irytować, **wymagania związane z długością i złożonością hasła są koniecznie, jeśli hasło ma spełniać swoją rolę**. Również zmiana hasła, wymuszona regularnie przez niektóre programy, jest elementem polityki bezpieczeństwa. Jak stworzyć prawidłowe i bezpieczne hasło do konta?

Hasło musi być oryginalne. Nie powielaj haseł! W razie ataku lub kradzieży danych z jednego serwisu hakerzy mogą **próbować dopasować hasła w innym miejscu**. Takie kradzieże miały miejsca w tak popularnych serwisach jak **Morele**, **Freshmail**, **Yahoo**, **LinkedIn** czy **Microsoft**. Mimo stosowanych przez firmy środków chroniących dane, w dużej mierze to od nas zależy ich bezpieczeństwo (pamiętasz *PEBKAC?*).



Na rozszyfrowanie ciągu 5 znaków z 3 małymi literami i 2 cyframi program do łamania haseł **potrzebuje 0,03 sekundy**. *

Na złamanie hasła złożonego z 8 znaków z 4 małymi literami, 3 cyframi i 1 znakiem specjalnym **wystarczy 2,6 dnia**. *

Natomiast by rozszyfrować ciąg 10 znaków (w tym 4 małe litery, 2 duże, 2 cyfry i 2 znaki specjalne), **potrzeba aż 853 lat!** *

Liczby mówią same za siebie.

* te dane dotyczą jednej z metod łamania haseł - brute-force.

51 proc. pracowników IT, w tym specjalistów ds. bezpieczeństwa twierdzi, że używa średnio 5 tych samych haseł do swoich kont służbowych lub osobistych - wynika z badania *The 2019 State of Password and Authentication Security Behaviors*.

Hasło musi być silne. Najlepiej o długości minimum 12 znaków, z małymi i wielkimi literami, cyframi i znakami specjalnymi. Nie powtarzaj w haśle nazwy użytkownika, ani prostych ciągów znaków - np. 12345 czy abcde. Nie używaj informacji, którymi można Cię zidentyfikować: miasto, imię, nazwisko, data urodzenia, świadczona usługa. Pamiętaj, że można się wiele o Tobie dowiedzieć, zbierając informacje z różnych źródeł. Wykorzystaj skojarzenia, przeplataj frazy cyframi i znakami specjalnymi. Oto przykład silnego hasło, które zapamięta entuzjasta harcerstwa: **letni820b#z++H@@rcerski**.

Czas potrzebny na złamanie skomplikowanego hasła rośnie wykładniczo wraz z jego złożonością i długością.

letni820b#z++H@@rcerski

NASZ PROTIP

Nie musisz pamiętać wszystkich swoich haseł. **Skorzystaj z menedżera haseł np. KeePass, Bitwarden, LastPass, 1Password czy Kaspersky PURE**. To programy, które w zaszyfrowanej postaci zachowają hasła w pamięci, ale także je wygenerują. Aby mieć do nich dostęp, musisz pamiętać tylko jedno, bardzo silne hasło tzw. master password.

Stosuj dwustopniowe zabezpieczenie. Dodatkowym sposobem jest tzw. 2FA - *two factor authentication*. Aby potwierdzić swoją tożsamość poza hasłem, musisz podać kod, który otrzymasz SMSem lub wygenerujesz w przeznaczonej do tego aplikacji do uwierzytelniania dwuetapowego np. Authy, Google Authenticator, LastPass, Microsoft Authenticator.

Czy Twoja przeglądarka jest bezpieczna?

Zacznijmy od ciasteczek (*cookies*) i pamięci podręcznej (*cache*). **Dlaczego powinny być regularnie "keszowane"?** Ciasteczka to pliki tekstowe, które zapisują się na Twoim urządzeniu, kiedy korzystasz z przeglądarki. Tymczasowo zapamiętują ustawienia przeglądarki, zapisują dane logowania oraz produkty, które dodałeś do koszyka w e-sklepie. Dzięki nim strona szybciej się ładuje.

Jednak to pliki cookies, z których korzysta niemal każdy serwis www i na których wykorzystywanie z reguły się zgadzasz, mogą narazić Cię na wiele niebezpieczeństw. Działają nieinwazyjnie i są niewidoczne, ale zapamiętują dane o Tobie, **w tym również dane wrażliwe**. Hakerzy właśnie za pomocą zapisanych plików cache, mogą włamać się do Twojego komputera czy smartfona.

NASZ PROTIP

Obsługę ciasteczek możesz zawsze wyłączyć. Możesz również włączyć tryb prywatny (incognito) w przeglądarce, który pozwala surfować po sieci z zachowaniem prywatności. Tryb incognito chroni dane o Twojej aktywności, które dodatkowo nie są zapisywane po zamknięciu karty. Zapobiega również przechowywaniu plików cookies i **nie pozwala na śledzenie historii pod kątem wysyłania reklam**.

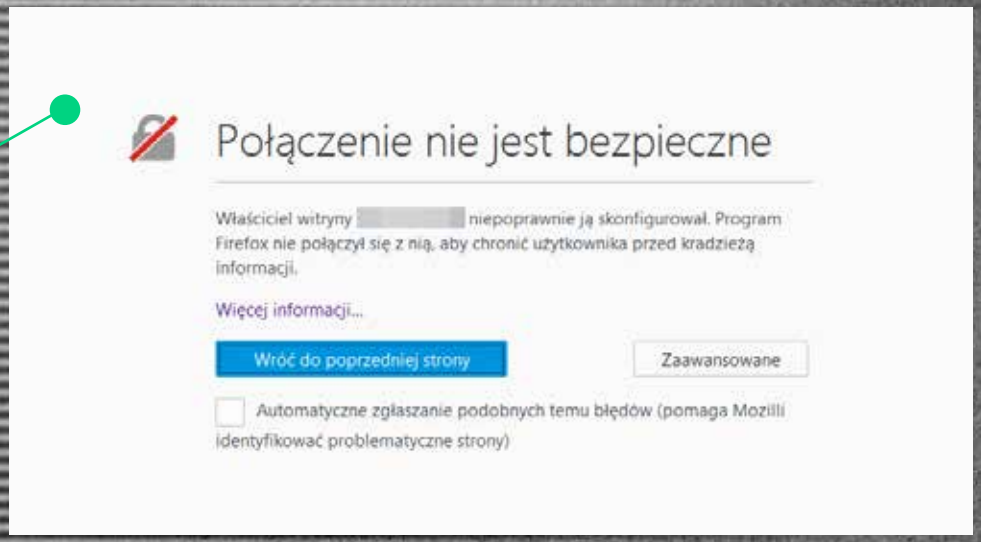
ALE, ALE...
Pamiętaj jednak, że tryb prywatny **nie gwarantuje całkowitej anonimowości**. O Twojej aktywności wie dostawca internetu lub pracodawca. Sam tryb prywatny nie ochroni Cię także przed atakami hakerskimi, ani nie zabezpieczy danych, które przesyłasz w internecie.

HTTPS, czyli bezpiecznie odwiedzaj strony

Protokół HTTPS zabezpiecza połączenie na całej drodze do odwiedzanej witryny. Dziś większość stron internetowych obsługuje ten protokół. Na pasku adresu www pojawia się symbol zamkniętej kłódki. Gdy w nią klikniesz, poznasz szczegóły dotyczące certyfikatu bezpieczeństwa SSL (Secure Socket Layer). Szyfrowanie SSL to uniwersalne rozwiązanie, które **ma na celu "zakodowanie" informacji przesyłanych pomiędzy Tobą, jako użytkownikiem danej strony www, a jej serwerem**.

UWAGA: HTTPS minimalizuje ryzyko, ale niestety nie chroni przed przechwyceniem i kradzieżą danych podczas ich przesyłania.

To przykład komunikatu ostrzegawczego o braku certyfikatu SSL.

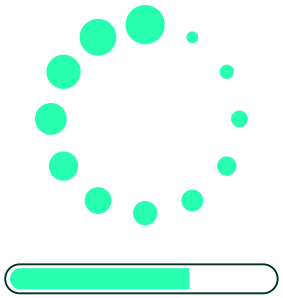


Czy surfując po Internecie spotkałeś się z podobnym komunikatem?

NASZ PROTIP

Czy SSL daje nam gwarancję bezpieczeństwa? Niestety nie. Wchodząc na strony, które mają certyfikat SSL, zawsze weryfikuj czy nazwa strony i domena nie posiadają podejrzanych znaków. Cyberprzestępcy **coraz częściej tworzą fałszywą stronę z SSL, na której będzie widoczna zielona kłódka i komunikacja nadal będzie szyfrowana, ale mimo to i tak może dojść do wyłudzenia Twoich danych**. Niemal wszystkie przeglądarki mają funkcję ostrzegania użytkownika w momencie próby odwiedzenia potencjalnie złośliwego adresu www. Pamiętaj jednak, że nie uchroni Cię to przed phishingiem, kradzieżą danych itd.

Aktualizuj system i pakiet oprogramowania antywirusowego



Aby zabezpieczyć się przed atakiem hakerskim i wyłudzeniem danych, dobry, **zaktualizowany program antywirusowy to minimum**. Zdarza się, że przypomnienie o konieczności aktualizacji systemu operacyjnego lub programu odkładamy do momentu, gdy samo urządzenia ją wymusza i następuje nagły reset. Traktujemy aktualizację jako zbędną czynność, a lekceważąc ją - **narażamy się na potencjalne niebezpieczeństwo**. Skuteczność złośliwych programów wynika z tego, że wykorzystują starsze wersje oprogramowania lub niezałatane luki. Dlatego aktualizacje programów wprowadzane są, aby poprawić błędy i zwiększyć ochronę komputera. Czasami ma to związek z wykryciem tzw. krytycznych luk bezpieczeństwa np. w przeglądarce, dzięki którym można niepostrzeżenie włamać się do komputera. Poważne zagrożenie odkryte np. w wyniku ataku hakerów - firma usuwa i **informuje użytkowników o konieczności aktualizacji programu**.

Zdarza się, że do ataku dochodzi, zanim twórcy oprogramowania dowiedzą się lub zidentyfikują lukę w zabezpieczeniach przeglądarki lub programu pocztowego. **Mówimy wówczas o ataku *zero-day***. Taka niewykryta luka umożliwia instalację złośliwego oprogramowania - *malware*; szpiegowskiego - spyware czy takiego, które szyfruje dane, aby wyłudzić okup - *ransomware*.

NASZ PROTIP

Zawsze **aktualizuj posiadany pakiet zabezpieczeń i system operacyjny na swoich urządzeniach**.

Program antywirusowy pomoże Cię ochronić (ale pamiętaj, że nie daje 100% gwarancji bezpieczeństwa) przed zainfekowanymi załącznikami, podejrzanymi linkami czy stronami i atakami hakerów. Musisz wiedzieć, że przestępca bez Twojej wiedzy potrafi uruchomić nawet Twoją kamerę internetową lub mikrofon w laptopie!

Łącz się bezpiecznie przez Wi-Fi

Dziś z internetem łączymy się zazwyczaj bezprzewodowo. Często bez świadomości, że sieć Wi-Fi jest również narażona na cyberataki. Dotyczy to danych poufnych, udostępnianych i przechowywanych w sieci: numerów kart płatniczych, danych do poczty, social media, komunikatorów czy systemów bankowości internetowej.

Upewnij się, że zarówno domowa jak i firmowa sieć Wi-Fi jest zaszyfrowana, zabezpieczona solidnym hasłem i najwyższym, dostępnym w routerze poziomem zabezpieczeń. Najlepiej, gdy będzie także ukryta.

NASZ PROTIP

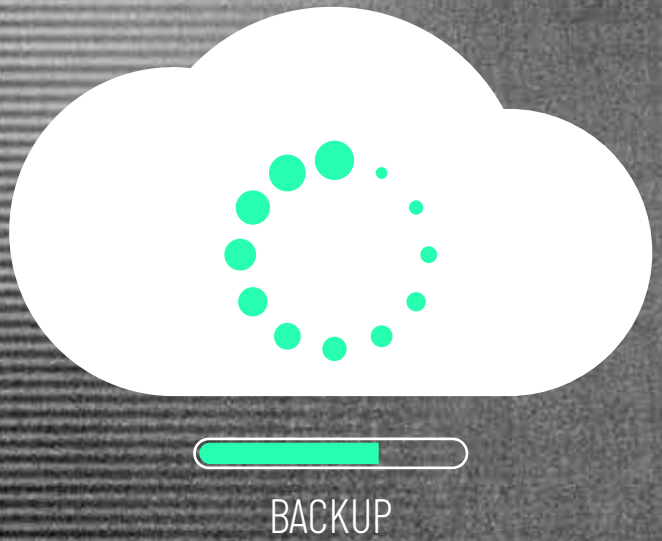
Nigdy nie loguj się do swojego konta bankowego lub innych aplikacji za pośrednictwem publicznej sieci Wi-Fi. Jeśli chcesz skorzystać z Internetu, łącząc się przez publiczne Wi-FI, np. spędzając czas w kawiarni - upewnij się, że udostępniona sieć rzeczywiście do niej należy. Dlatego korzystając z Wi-Fi w miejscu publicznym, korzystaj z VPN, który szyfruje komunikację.

Zwiększ prywatność w sieci używając VPN

W sieci każdy Twój ruch może być śledzony. Jeśli chcesz zachować prywatność, skorzystaj z VPN (*Virtual Private Network*). Wirtualna sieć prywatna to program, który **szyfruje całą komunikację, informacje o Twoim adresie IP czy lokalizacji w trakcie ich przesyłania**. Dzięki VPN Twoje informacje nie wpadną w niepowołane ręce, niezależnie od tego, w jakim miejscu aktualnie się znajdujesz.
Aby mieć pewność co do jakości usługi, warto sięgnąć po komercyjne rozwiązania (np. SurfShark, ExpressVPN, PureVPN).
Z VPN skorzystasz również, kupując program antywirusowy, który oferuje taką usługę (np. Norton). Jednak, jak mówi nasz spec od bezpieczeństwa danych:
niczemu nie możesz ufać bezgranicznie.

Twórz regularnie kopię zapasową danych

Kopia zapasowa, czyli tzw. *back-up* jest kopią danych, która pozwoli odzyskać dostęp do nich po awarii dysku lub zainfekowaniu komputera wirusem, w tym np. zaszyfrowaniu wszystkich danych (*ransomware*). **Tworzenie zabezpieczenia danych na urządzeniach firmowych jest obowiązkowe**. W razie pojawienia się kryzysu możesz (nie ponosząc większych strat), zapewnić biznesowi płynne funkcjonowanie. Jeśli nie robisz jeszcze kopii zapasowych swoich danych, albo lekceważysz ryzyko ich utraty - zmienisz zdanie, gdy dotknie Cię to osobiście.



NASZ PROTIP

Jak często powinieneś robić backup? Pytanie powinno brzmieć: **na utratę danych, z jakiego okresu możesz sobie pozwolić?** Kopie danych wykonuj najlepiej codziennie, wykorzystując do tego dedykowane narzędzia i programy. Możesz kopiować automatycznie dane do chmury korzystając z usług GDrive, iCloud, OneDrive czy Dropbox. Dane możesz archiwizować również na dysku zewnętrznym. Pamiętaj jednak, aby zaszyfrować dane. Jeśli pracujesz na komputerze Apple, skorzystaj z rozwiązania TimeMachine, które tworzy kopie aplikacji, zdjęć, e-maili i dokumentów.

Komu zależy na Twoich danych?

Z kradzieżą tożsamości (*identity theft*) mamy do czynienia wtedy, gdy **osoba trzecia otrzyma dostęp do danych i wykorzysta je wbrew Twojej woli, najczęściej w celu przyjęcia korzyści majątkowej**. O jakich danych mówimy? To dane logowania do poczty e-mail, serwisów social media, ale także dane osobowe: numer dowodu osobistego, karty, telefonu. Oszust, posiadając takie dane, może wyłudzić kredyt na Twoje nazwisko.

Dane mogą wpaść w ręce przestępców nie z naszej winy - np. w sytuacji wycieku danych w wyniku włamania lub ludzkiego błędu. Najczęściej są to:

- **loginy i hasła klientów,**
- **informacje o kartach kredytowych,**
- **numery PESEL,**
- **adresy,**
- **numery telefonów.**

Cenne informacje, gdy wpadną w ręce przestępców, **mogą być użyte do wyłudzania okupu, zaciągnięcia kredytów czy wyczyszczenia konta bankowego**. Cyberprzestępcy próbują złamać hasła do poczty e-mail, a następnie sprawdzają te dane logowania w innych popularnych witrynach. Dlaczego? Niestety, wiele osób używa tych samych danych logowania i haseł dla wielu kont. A to kardynalny błąd!

Komu zależy na Twoich danych?

Na stronie **haveibeenpwned.com** możesz sprawdzić czy Twoje dane nie wyciekły do Sieci. To zaufana witryna, możesz więc bezpiecznie podać tam swój e-mail lub numer telefonu. Serwis publikuje **613 584 246** prawdziwych haseł (czerwiec 2021), które wcześniej zostały ujawnione w wyniku naruszenia danych.

Warto skorzystać z usługi Biura Informacji Kredytowej (**www.bik.pl**), dzięki której otrzymasz natychmiastowy alert o próbie wyłudzenia kredytu na Twoje dane i możesz reagować natychmiast, aby zapobiec wyłudzeniu. Usługa jest płatna (tylko 24zł/rok), ale bardzo wartościowa.

Ataki cybernetyczne stanowią również globalne zagrożenie dla firm technologicznych. Należący do Colonial Pipeline rurociąg z paliwem w USA, czy instytucji: szpitale w Irlandii, metro w NYT. Stoją za nimi **zorganizowane grupy przestępcze specjalizujące się w przeprowadzaniu ataków czy szyfrowaniu danych przy użyciu oprogramowania typu *ransomware***, aby uzyskać okup. W momencie zarażenia komputera dochodzi do zaszyfrowania i blokady dostępu do danych zawartych na dyskach. Aby te dane odzyskać, hakerzy informują o możliwościach usunięcia blokady, zazwyczaj w postaci zapłacenia okupu (najczęściej przy użyciu kryptowaluty, co pozwala achować im anonimowość).

Pilnuj telefonu jak oka w głowie

Poza komputerem na celowniku przestępców jest także Twój smartfon czy tablet. Używasz go do bankowości online czy robienia zakupów, a zatem w **grę może wchodzić duża ilość danych osobowych**. Telefon jest łatwiejszym celem niż komputer. Łatwiej go ukraść, rzadziej instalujemy na nim program antywirusowy czy zabezpieczamy. Jednocześnie wymieniamy szereg informacji przez komunikatory czy SMSy i łatwiej jest przemycić wiadomość z fałszywym linkiem, poprzez który ściągniemy złośliwe oprogramowanie. Zadbaj o mocne hasło albo **dwustopniowe zabezpieczenie przy logowaniu do kont w serwisach społecznościowych**. Gdy przestępca włamie się na takie konto, rozsyła do wszystkich kontaktów wiadomości z niebezpiecznymi linkami. Gdy sądzimy, że wiadomość przyszła od znajomego i nie wygląda na podejrzaną, chętniej w nią klikniemy. Dodatkowo, poważnym zagrożeniem jest zdolność przestępców do **podszywania się pod numery telefonów i maskowanie prawdziwego numeru nadawcy**.
Przestępcy wykorzystują natłok wiadomości w komunikatorach, e-mailach, aby uśpić Twoją czujność.

Bądź na bieżąco z informacjami o bezpieczeństwie

Media regularnie informują o atakach hakerskich i nowych pomysłach na wyłudzenia danych. Oszuści próbowali wyłudzić pieniądze lub dane, **podszywając się pod OLX**, gdy platforma wprowadziła nową usługę Przesyłek i Płatności. Wysyłali wiadomości od rzekomego kupującego, że zakupiony przedmiot został opłacony, prosząc o wejście w link do fałszywego potwierdzenia płatności OLX i podanie danych karty płatniczej.

Dziś każdy musi mieć świadomość nie tylko istniejących, ale potencjalnych zagrożeń. Musisz wiedzieć, skąd może nadejść zagrożenie i jakie formy przybiera. Dlatego śledzenie informacji o bezpieczeństwie, to niezbędny element internetowej higieny. Informacje i ostrzeżenia o zagrożeniach publikują banki, platformy aukcyjne, sklepy internetowe czy serwisy popularyzujące wiedzę o bezpieczeństwie jak Niebezpiecznik.pl

Zwracaj uwagę, jakie prywatne informacje zostawiasz w internecie np. dzieląc się zdjęciami w social mediach.
Pamiętaj, że mogą zostać wykorzystane przeciwko Tobie.

PODSUMOWANIE

- Bezpieczeństwo w internecie jest jak talia kart. Dlatego, aby rozegrać bezpieczną grę każda z kart pełni swoją określoną rolę.
- Silne hasło, a zwłaszcza weryfikacja dwupoziomowa (2FA) chronią Twoje zasoby: pocztę, konta w social mediach, dane lub programy w chmurze.
- Program antywirusowy będzie zaporą przed złośliwymi wirusami, których celem jest dziś wyłudzanie lub kradzież danych lub tożsamości. Szyfrowanie danych przesyłanych w sieci przy pomocy VPN zagwarantuje Ci, że nie wpadną w niepowołane ręce. Stosując się do naszych zaleceń, nie zapominaj także o regularnych kopiach zapasowych ważnych danych!
- Gdy wiesz, że cyberprzestępcy, niczym karciani iluzjoniści nagminnie wykorzystują zarówno proste jak i wyrafinowane triki, aby złowić Twoje dane (phishing), musisz krytycznie traktować nietypowe komunikaty: alerty, ponaglenia, informacje o konieczności weryfikacji danych, itd.
- Generalnie, stosuj Zasadę Ograniczonego Zaufania i niczym doświadczony pokerzysta z założenia nie ufaj innym i nie ulegaj emocjom.
- W długim łańcuchu bezpieczeństwa każde ogniwo ma znaczenie, ale najwięcej zależy od Twojej wiedzy i podejścia! Nie pozwól, aby Twoje bezpieczeństwo runęło jak domek z kart.

SARE°
DIGITREE GROUP

Bezpieczny kontakt:

kontakt@sare.pl

www.sare.pl

ZOSTAŃ ASEM BEZPIECZEŃSTWA!

E-BOOK O BEZPIECZEŃSTWIE W SIECI Bo chcemy, abyś był bezpieczny.