ik › internetowykantor.pl

PORADNIK

Czy bezpiecznie zarządzasz swoimi finansami w sieci?

2019

Spis treści

Wstęp

To, w jaki sposób korzystamy z naszych oszczędności, w ciągu ostatnich kilku lat uległo ogromnej zmianie. Coraz chętniej zarządzamy nimi za pośrednictwem bankowości internetowej lub mobilnej. Wydajemy pieniądze na platformach e-commerce i aukcyjnych. Z większym entuzjazmem podchodzimy też do kupowania w Internecie dostępu do rozrywki, wiedzy i kultury. Słowem, wiemy już, że w Internecie można załatwić prawie wszystko i coraz odważniej z tego korzystamy.

Niestety, wraz z przeniesieniem do Internetu tak dużej części naszego życia, wzrosła liczba przestępstw, polegających na wyłudzeniach danych, przechwytywaniu haseł i włamaniach na konta serwisów instytucji finansowych, społecznościowych, zakupowych itd. Konsekwencje phishingu, czyli podszycia się pod inną osobę lub instytucję w celu wyłudzenia danych, są jednym z największych zagrożeń dla naszych oszczędności, a bronienie się przed atakami staje się coraz większym wyzwaniem.

Celem poradnika jest zwiększenie świadomości zagrożeń czyhających w sieci oraz dostarczenie internautom wiedzy, która pozwoli się przed nimi bronić. Impulsem do jego stworzenia był Światowy Dzień Oszczędzania przypadający 31 października. Uznaliśmy, że święto to warto wykorzystać nie tylko po to, by zachęcić Polaków do pomnażania oszczędności, ale i przypominać o tym, że należy dbać o ich bezpieczeństwo.

Zespół Internetowykantor.pl

Co to jest phishing?

Phishing to atak socjotechniczny polegający na wyłudzaniu informacji lub przekonaniu ofiary do wykonania czynności sprzecznych z jej interesem. Jego celem jest najczęściej kradzież haseł, danych logowania do bankowości internetowej i numerów kart, ale bywa i tak, że zdobyczą phishera są poufne informacje z naszego komputera lub przelewy, które sami zleciliśmy.

Możemy wyróżnić kilka rodzajów phishingu:

- masowy - kierowany do przypadkowych użytkowników,
- spear phishing - skierowany do konkretnego odbiorcy i często bardziej wiarygodny, bo opierający się na informacjach, jakie oszust posiada na temat ofiary,
- whaling - skierowany do konkretnej grupy osób: decyzyjnych, zarządzających dużymi organizacjami lub posiadających cenne informacje,
- pharming - polega na tym, że nawet, gdy wpiszemy prawidłowy adres danego serwisu internetowego, zostajemy przekierowani na fałszywą stronę, na której oszust zamierza wykraść nasze dane.

Na czym polega phishing?

Duża część phishingu opiera się na przekazywaniu potencjalnym ofiarom fałszywych linków: w mailach, SMS-ach czy ogłoszeniach. Odnośniki zamiast prowadzić np. na stronę internetową banku, wysyłają ofiarę na stronę łudząco podobną, gdzie dobrowolnie podaje ona swoje dane. Zdarza się też, że oszuści po prostu podszywają się pod kogoś, komu ufamy i proszą o podanie wrażliwych danych lub przelanie określonej kwoty pieniędzy. Trzecią, bardzo popularną metodą jest sprawienie, aby ofiara, razem z pozornie bezpiecznym załącznikiem czy aplikacją, pobrała na swoje urządzenie złośliwe oprogramowanie.

"Ataki phishingowe są bardziej wyrafinowane i dopracowane, niż jeszcze kilka lat temu. Oszuści dbają o poprawność językową, której brak kiedyś ich zdradzał, sprawiają, że wygląd strony jest maksymalnie zbliżony do oryginału, uwiarygodniają otrzymanie wiadomości związanej np. z zamieszczonym przez nas ogłoszeniem, podszywają się pod znajomych na portalach społecznościowych. Innymi słowy, ataki są coraz bardziej wiarygodne, przez co trudniej jest je rozpoznać i skutecznie się przed nimi bronić."

Dariusz Polaczyk
Risk and Security Manager w Currency One

Na co liczy oszust?

Słysząc historie o wyłudzeniach w Internecie, przypadkowym ściągnięciu złośliwego oprogramowania czy stracie wszystkich oszczędności, większość z nas myśli o ofiarach, jako o ludziach bardzo naiwnych. Problem w tym, że czasy ataków phishingowych polegających na wysyłaniu maili, które aż kłują w oczy brakiem wiarygodności, mamy już w dużej mierze za sobą. Dziś oszukać jest trudniej, ale zostać oszukanym - znacznie łatwiej. Co powoduje, że tak wielu z nas pada ofiarą ataków phishingowych?

1. Strach i pośpiech - niebezpieczna para

Wiadomości będące wstępem do phishingu nierzadko bazują na obawie przed utratą czegoś cennego: dostępu do konta, wyczekiwanej przesyłki, atrakcyjnej okazji. Otrzymując informację o tym, że rachunek z naszymi oszczędnościami zostanie zablokowany albo coś, na co czekamy od miesiąca, zostanie zwrócone nadawcy, jesteśmy skłonni w to uwierzyć i szybko zrobić wszystko, o co poprosi nas oszust.

2. Nie zwracamy uwagi na szczegóły

Ataki phishingowe często polegają na tym, że fałszywe strony są uderzająco podobne do prawdziwych i to, co daje im szansę na sukces, to nasza nieostrożność. Gdy korzystamy z bankowości mobilnej na co dzień, przestajemy zwracać uwagę na szczegóły i robimy wszystko automatycznie - a to czyni nas łatwym celem. Podekscytowani atrakcyjną ofertą albo w pośpiechu odpisując na maile, ignorujemy niepokojące sygnały i wpadamy prosto w sidła oszustów.

3. Ufamy oszustowi

Oszuści skutecznie podszywają się pod podmioty, którym ufamy - banki, instytucje rządowe, organizacje non profit czy nawet naszych znajomych i współpracowników. Zakładamy ich dobre intencje (gdy kolega prosi o szybkie wsparcie finansowe), boimy się konsekwencji (gdy otrzymujemy ponaglenie od urzędu skarbowego) albo nie widzimy w danej prośbie nic nadzwyczajnego (gdy szef dopytuje o poufne dane).

4. Jesteśmy łasi na okazje

Oszust oferuje korzyści, na które normalnie nie mamy szansy. Raz jest to nagroda w loterii, innym razem opowieść o spadku wujka z Ameryki albo jedyna w swoim rodzaju oferta na portalu ogłoszeniowym. Skuszeni perspektywą szybkiego zarobku lub zaoszczędzenia kilku tysięcy złotych podajemy dane, wysyłamy zaliczki i logujemy się na podejrzane portale, zapominając o podstawowych zasadach bezpieczeństwa w sieci.

5. Nie wiemy wszystkiego

Często jesteśmy zupełnie bezbronni wobec oszustów, bo nie jesteśmy pewni, jakich danych nigdy nie powinniśmy podawać. Nie zdajemy sobie sprawy z zagrożeń, a nawet nie możemy sobie wyobrazić, że można nas oszukać w taki sposób. Nie wiemy też, co warto sprawdzać, by upewnić się, że jesteśmy na bezpiecznej stronie, aukcji lub czy czytamy maila od prawdziwej instytucji.

Gdzie polują cyberoszuści?

Wiesz już, na jakich mechanizmach psychologicznych bazują oszuści i dlaczego tak łatwo jest im dotrzeć nawet do tych, którzy wydają się być świadomi niebezpieczeństw czających się w Internecie. W tym rozdziale pokażemy Ci, jak ataki phishingowe mogą wyglądać, podamy przykłady oszustw i udzielimy mnóstwa wskazówek, które pomogą Ci uchronić się nawet przed tymi bardziej wyrafinowanymi podstępami.

1. Zakupy w sieci

Przez Internet kupujemy już niemal wszystko, a oferta platform e-commercowych stale rośnie - podobnie jak liczba ataków phishingowych, wykorzystujących nieostrożność konsumentów. Jakimi metodami oszuści wyłudzają dane i pieniądze za pośrednictwem sklepów internetowych?

Sklepy widmo i imitacje gigantów

Choć trudno to sobie wyobrazić, tuż przed najgorętszym okresem zakupowym, w okolicach tzw. Czarnego Piątku, oszuści często tworzą całe platformy e-commerce. Ofiara wybiera, co chce kupić, płaci, a potem czeka na przesyłkę, która do niej nie dociera - bo sklep ten nigdy nie istniał. Drugą metodą ataku phishingowego jest tworzenie stron do złudzenia przypominających największe platformy np. Allegro czy Aliexpress. Konsument, zachęcony reklamą, klika w link, który przekierowuje go do fałszywej strony.

Fałszywa strona pośrednika płatności

Zdarza się też, że choć sama platforma sprzedażowa jest prawdziwa, to strona płatności wręcz przeciwnie. Po zaakceptowaniu koszyka, zamiast bezpiecznie zapłacić za towar, jesteśmy przenoszeni na fałszywą stronę pośrednika płatności, gdzie wpisujemy dane do logowania. Następnie jesteśmy proszeni o autoryzację transakcji i to najczęściej dwukrotnie, bo oszust w tle przeprowadza operacje, które mają na celu wyprowadzenie z naszego konta wszystkich oszczędności.

Komunikaty o dopłacie

"Modnymi" atakami phishingowymi są SMS-y, w których oszuści podszywający się pod najpopularniejszych dostawców, informują o tym, że, aby nasza przesyłka dotarła na miejsce, musimy dopłacić niewielką kwotę. Podobny schemat występuje przy płatnych ogłoszeniach w sieci, w których wystawcy podają swoje numery telefonu - otrzymują oni wiadomość, że należy uiścić dodatkową, drobną opłatę, aby ich ogłoszenie nadal było aktywne. Uważać należy również na oferowanie rzeczy za darmo, z koniecznością zapłacenia jedynie za przesyłkę. Linki w powyżej wymienionych sytuacjach mogą kierować do specjalnie stworzonych paneli, gdzie podajemy dane do logowania do banku, a przestępcy je przejmują. Następnie oszuści logują się na nasze konto bankowe i generują płatność lub założenie odbiorcy zaufanego, co wymaga dodatkowej autoryzacji, którą wykonujemy dobrowolnie, nie zwracając uwagi na treść komunikatów autoryzacyjnych.

Jak bezpiecznie kupować w sieci?

1. Zwracaj uwagę na szczegóły i upewnij się, że robisz zakupy na właściwej stronie.
2. Na każdym etapie płatności sprawdzaj, czy zgadza się adres URL, a cała strona wygląda tak samo jak zwykle.
3. Gdy kupujesz coś w nowym miejscu, sprawdź, jak długo dany sklep internetowy działa i czy na pewno jest bezpieczny.
4. Jeśli chcesz zachować szczególną ostrożność, możesz założyć konto przeznaczone specjalnie na zakupy internetowe i nie trzymać na nim dużych kwot.

Zwracaj uwagę na szczegóły i upewnij się, że robisz zakupy na właściwej stronie.

2. Media społecznościowe

Media społecznościowe są obecne w wielu obszarach naszego życia - szukamy w nich rozrywki, śledzimy poczynania naszych znajomych, dzielimy się swoimi opiniami, podtrzymujemy kontakt z naszymi bliskimi, a nawet nawiązujemy znajomości. Niewielu z nas ma jednak świadomość, co może nam grozić.

Jak oszuści wykorzystują media społecznościowe?

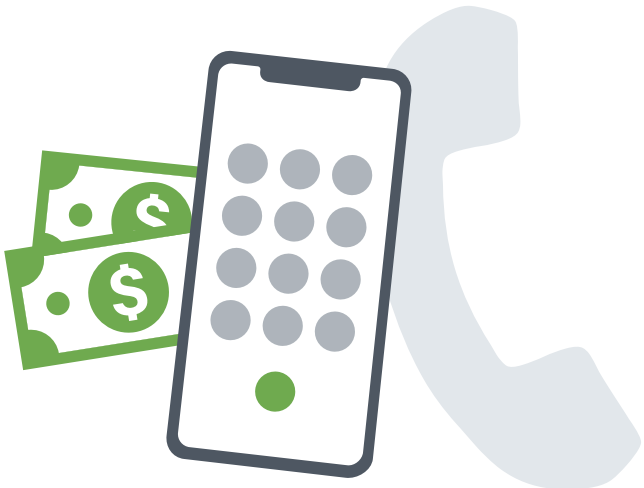
Oprócz wycieku wrażliwych danych czy udostępnianych przez nas informacji, źródłem niebezpieczeństwa jest również nasze zaufanie do znajomych. Ich konta, tak samo zresztą jak nasze, mogą być bowiem wykorzystane do wyłudzenia mniejszych lub większych kwot pieniężnych. W jaki sposób?

Przestępcy połączyli jeden z najwygodniejszych sposobów wykonywania przelewów - BLIK oraz ufność, jaką pokładamy w mediach społecznościowych i komunikatorach, by stworzyć nową metodę phishingu. Podszywając się pod znajomego, dzięki przejęciu lub stworzeniu fałszywego profilu takiej osoby, kontaktują się z ofiarą i proszą o pilny przelew określonej kwoty. Argumentują swoją potrzebę sytuacją losową: kradzieżą portfela, problemem z powrotem do domu itp. Z reguły prośby te dotyczą małych kwot, wiążą się z naciskami na szybką reakcję i są uzupełniane zapewnieniami o zwrocie pożyczonych środków już następnego dnia. Oszuści proszą nas o przekazanie kodu BLIK, a po zatwierdzeniu przez nas transakcji w aplikacji bankowej (czasami kilkukrotnego z powodu rzekomego niezadziałania poprzedniego kodu) szybko wypłacają gotówkę z bankomatu.

Jak dbać o bezpieczeństwo w mediach społecznościowych?

1. Jeśli Twój znajomy prosi Cię o przelew przez Internet lub podanie wrażliwych danych, skontaktuj się z nim w inny sposób, na przykład zadzwoń, aby upewnić się, że to on jest nadawcą danej wiadomości.
2. Zadbaj o silne hasło i, jeśli jest to możliwe, ustaw dwuetapowe uwierzytelnienie.
3. Nigdy nie loguj się do swojego konta na obcych urządzeniach. Jeśli nie masz innego wyjścia, najlepiej ustaw wcześniej podwójne uwierzytelnienie i otwórz stronę logowania w trybie incognito.
4. Nie udostępniaj swojej lokalizacji w social mediach - może to być dla złodzieja wskazówka, że nie ma Cię w domu.
5. W Internecie można znaleźć wszystko, ale to nie znaczy, że warto publikować każdy szczegół swojego życia. Uważaj przede wszystkim na takie kwestie jak wysokość zarobków, adresy czy zdjęcia dokumentów, na których mogą znajdować się Twoje dane.

Znajomy prosi Cię o przelew przez Internet lub podanie wrażliwych danych? Skontaktuj się z nim, aby upewnić się, że to na pewno on.



3. Fałszywe oferty pracy

Phishing może przyjąć również formę fałszywej, najczęściej bardzo atrakcyjnej oferty pracy. Naszą podejrzliwość powinny wzbudzić:

- bardzo atrakcyjne warunki łączące się z brakiem oczekiwań i gwarancją pracy jedynie kilka godzin w tygodniu,
- zakres obowiązków, który obejmuje wykorzystanie naszego prywatnego konta i pośredniczenie przy przelewach pieniężnych,
- brak opisu wymagań i zakresu obowiązków,
- otrzymanie niespodziewanej wiadomości od rekrutera. W dobie bezpośredniej rekrutacji zdarza się to coraz częściej, ale jeśli oferta nie jest związana z naszym doświadczeniem zawodowym, a za nadawcą nie stoi żadna znana nam firma, lepiej mieć się na baczności,
- linki lub pliki w wiadomości od rekrutera, w których rzekomo znajduje się opis stanowiska,
- e-mail rekrutacyjny przychodzący z adresu bez domeny firmowej - szczególnie, gdy po firmie nie ma śladu w Internecie i brakuje podstawowych informacji o przedsiębiorstwie, tj. adresu, numeru KRS lub telefonu,
- wiadomości pisane łamaną polszczyzną lub bez polskich znaków,
- żądania skanu dowodu, poufnych informacji lub numeru konta jeszcze przed podpisaniem umowy,
- prośby o opłacenie szkolenia lub wykonanie próbnego przelewu.

Pytanie jednak, jaki jest cel oszusta, który publikuje fałszywe oferty pracy?

"Oszust może liczyć na pozyskanie naszych danych osobowych, w tym numer PESEL czy adresu zamieszkania, m.in. w celu zaciągnięcia pożyczki; zmanipulowania nas do przelania pieniędzy na podane konto lub uruchomienia płatnej subskrypcji np. poprzez potwierdzenie konta kodem SMS. Jeszcze niebezpieczniejsze są jednak te ataki, które sprawiają, że zostajemy wplątani w działalność związaną z praniem pieniędzy - jeśli jesteśmy proszeni o pośrednictwo w przelewaniu, wypłacaniu/wpłacaniu środków lub użyczenie prywatnego konta bankowego, jak najszybciej wycofajmy się z takiej współpracy i rozważmy zgłoszenie tego do organów ścigania."

Maciej Pawlak
Chief Information Security Officer w Currency One

Oferty pracy mogą być też wykorzystane do typowych ataków phishingowych, takich jak niebezpieczne linki lub zainfekowane pliki. Tego typu oszustw przestępcy dopuszczają się nie tylko poprzez udostępnianie ogłoszeń na portalach rekrutacyjnych czy na grupach na Facebooku (proponując najczęściej pracę bez wychodzenia z domu i ogromne prowizje), ale też w bezpośrednich, nierzadko bardzo przekonujących mailach lub wiadomościach na Linkedinie czy innych portalach zawodowych.

Jak uchronić się przed oszustwami?

1. Nie otwieraj plików od nieznanych nadawców. Dotyczy to zarówno wiadomości mailowych, jak i serwisów społecznościowych.
2. Dokładnie czytaj treści wysłanych przez potencjalnego pracodawcę lub agencję zatrudnienia regulaminów i umów - nie daj się złapać na drobny druczek.
3. Jeśli otrzymasz ofertę od firmy znanej na rynku, ale coś wzbudzi Twoje wątpliwości, zadzwoń do działu HR i upewnij się, że nikt nie podszywa się pod danego pracodawcę (zadzwoń pod numer telefonu znaleziony na oficjalnej stronie internetowej, nie w otrzymanej wiadomości).
4. Nie odpowiadaj na podejrzane oferty pracy - szczególnie, gdy nigdy nie aplikowałeś na podobne stanowisko.

Nie otwieraj plików od nieznanych nadawców. Dotyczy to zarówno wiadomości mailowych, jak i serwisów społecznościowych.

4. Niebezpieczne wiadomości

Częstą praktyką phishingową jest wysyłanie maili i SMS-ów w imieniu podmiotów cieszących się zaufaniem: instytucji finansowych, serwisów ogłoszeniowych czy organów państwowych. Pomysłowość przestępców w tym zakresie nie zna granic, a jej efektem są niezwykle wiarygodne komunikaty, których przykłady zostały opisane poniżej.

Wiadomości o blokadzie konta

Oszuści, podszywając się pod banki, wysyłają na losowo wybrane adresy e-mail komunikaty o blokadzie konta, karty płatniczej lub aplikacji mobilnej. W wiadomości znajduje się link, który kieruje nas na stronę panelu transakcyjnego. W rzeczywistości użytkownik trafia na witrynę do złudzenia przypominającą oryginał i, aby uratować rzekomo zablokowane konto, loguje się do serwisu - a złodzieje zyskują jego hasło i login. Jedyne, czego im brakuje, by ograbić ofiarę z oszczędności, to kod SMS lub autoryzacja przez aplikację mobilną, którymi zatwierdzą transakcję.

Niebezpieczne załączniki

W imieniu różnych instytucji i przedsiębiorstw oszuści wysyłają do swoich ofiar e-maile z plikami, które mają na celu zainfekowanie ich urządzeń. Załącznik jest najczęściej spakowany lub zawiera nietypowe rozszerzenie. Złośliwe oprogramowanie, atakujące komputer lub telefon, po otwarciu pliku może podmieniać linki do stron bankowości internetowej, przechwytywać hasła lub wyświetlać komunikaty, sugerujące konieczność zainstalowania specjalnego oprogramowania antywirusowego. W rzeczywistości jest to kolejny wirus, który infekuje urządzenie użytkownika w celu przekierowania kodów SMS, przechwytywania informacji wrażliwych czy wręcz jego przejęcia.

Prośby o przelewy

Bardzo popularną metodą phishingu jest podszywanie się pod firmy telekomunikacyjne czy kurierskie, a nawet instytucje rządowe, aby poprosić użytkowników o uregulowanie rachunku lub dopłatę do usługi. Z pozornie wiarygodnego adresu otrzymujemy wtedy fałszywy numer konta albo link do panelu, w którym mamy zatwierdzić przelew. Przykładem tego są SMS-owe prośby o uiszczenie opłaty za przesyłkę w okresie przedświątecznym. Znane są też sytuacje podszywania się pod Ministerstwo Finansów i prośby o wpłatę za wpis do rejestru REGON lub podanie danych karty kredytowej celem zwrotu nadpłaty podatku.

Oszustwa na konkursy

Któż z nas nie dostał SMS-a o treści "Gratulacje, wygrałeś XYZ! Aby odebrać nagrodę, wyślij SMS na numer…"? Odesłanie SMS-a będzie nie tylko bardzo kosztowne, ale i rozpocznie serię kolejnych, dodatkowo płatnych wiadomości np. z odpowiedziami na zadawane pytania. Równie popularne są konkursy wyskakujące nam w okienkach na stronach internetowych lub przychodzące za pośrednictwem poczty elektronicznej - zaangażowanie się w nie, poza stratą pieniędzy, może wiązać się z wgraniem złośliwego oprogramowania. Należy również uważać z oddzwanianiem na numery, od których mamy nieodebrane połączenia. Oszuści podszywają się pod numer przypominający numer krajowy, ale w rzeczywistości jest to numer egzotycznego kraju, gdzie połączenia są bardzo kosztowne.

Jak uchronić się przed takimi oszustwami?

1. Żadna instytucja finansowa nie poprosi Cię w wiadomości o podanie danych do logowania, hasła, kodów autoryzacyjnych lub danych kart płatniczych, więc nigdy ich nie wysyłaj.

2. Loguj się na swoje konto bankowe tylko przez stronę banku lub aplikację, nigdy z linków przesyłanych w wiadomościach.
3. Nie otwieraj załączników od nieznajomych ani tych, które znajomi wysłali Ci niespodziewanie - ich poczta elektroniczna mogła zostać zainfekowana.
4. Dokładnie sprawdzaj adres nadawcy, porównuj korespondencję z wcześniejszymi mailami.
5. Jeśli coś wzbudzi Twój niepokój, zadzwoń do instytucji, która rzekomo wysłała wiadomość i wyjaśnij wątpliwości. Numer telefonu sprawdź na oficjalnej stronie internetowej, zamiast dzwonić pod numer podany w komunikacie.
6. Nie odpowiadaj na maile o nagrodach, których nie starałeś się wygrać.
7. Jeśli z takowych nie korzystasz, zablokuj u swojego operatora telekomunikacyjnego wiadomości i połączenia głosowe o podwyższonej opłacie (tzw. usługi PREMIUM), a także wychodzące połączenia międzynarodowe. Usługa ta jest bezpłatna, a operator nie może odmówić jej wykonania.

Loguj się na swoje konto bankowe tylko przez stronę banku lub aplikację, nigdy z linków przesyłanych w wiadomościach.

5. Oszustwa "sezonowe"

Ataki phishingowe bardzo często opierają się na aktualnych wydarzeniach i trudno się dziwić, bo dzięki temu zyskują na wiarygodności. Przykładowo, w okolicach ostatecznego terminu rozliczania podatku PIT pojawiają się maile, rzekomo od Urzędu Skarbowego, nawołujące do szybkiej dopłaty i grożące poważnymi konsekwencjami. Gdy wybucha skandal związany z niewypłacaniem odszkodowań przez ubezpieczalnie, dostajemy podejrzane wiadomości, które gwarantują nam wsparcie i odzyskanie pieniędzy.

Ostatnio oszuści wykorzystali kampanie medialne dotyczące unijnej dyrektywy PDS2, która weszła w życie 14 września 2019 roku. Jednym z elementów owej dyrektywy jest konieczność skorzystania z tzw. silnego uwierzytelnienia podczas logowania do serwisu finansowego czy dokonywania transakcji. Jak to wygląda w praktyce? Musimy zostać zweryfikowani przez 2 z 3 elementów:

- „wiedzę", czyli kod lub hasło, które jest znane tylko nam,
- „posiadanie", czyli coś, co posiadamy na własność np. telefon,
- „cecha", czyli nasza wyjątkowość np. odcisk palca.

"Pomysłowi złodzieje postanowili wykorzystać to, że wszyscy mówili o PSD2 i zorganizować na jej podstawie próbę wyłudzenia. Do klientów jednego z największych banków dzwoniono i proszono o zainstalowanie specjalnego oprogramowania, które miało na celu kradzież danych. Wniosek? Zawsze warto zachować czujność i nie tracić głowy, nawet kiedy podejrzana wiadomość wydaje się mieć poparcie w rzeczywistości."

Maciej Pawlak
Chief Information Security Officer w Currency One

Jak zadbać o swoje bezpieczeństwo w sieci?

1. Nie lekceważ siły hasła

Pomimo podniesionych, m.in. dzięki dyrektywie PSD2, standardów bezpieczeństwa w bankowości internetowej i mechanizmowi podwójnego zabezpieczenia, wybierane przez nas hasło wciąż jest istotnym elementem obrony przed atakiem phishingowym. Każdy z nas ma w Internecie dziesiątki lub nawet setki kont i teoretycznie wszyscy powinniśmy zdawać sobie sprawę z tego, że ustawione przez nas hasła są jedynym, co możemy zrobić, by je zabezpieczyć. Mimo to, ustawianie jako hasła imion swoich pupili lub dat urodzenia naszych bliskich to wciąż norma - tak samo jak włamania na konta w serwisach, z których korzystamy.

Co tworzy dobre hasło?

Na siłę hasła składają się 4 elementy: długość, złożoność, unikalność oraz miejsce, w którym je przechowujemy. Poza tym trzeba mieć na uwadze własne ograniczenia - nie jesteśmy przecież w stanie zapamiętać 80 przypadkowych haseł. Dobrym pomysłem jest bazowanie na skojarzeniach lub łączenie kilku słów np. Ania-czyta.2poradniki albo 3kwiatY!w.doniczce. Takie hasła są proste do zapamiętania, a niemożliwe do odgadnięcia. Wskazane jest, aby hasło składało się z minimum 8 znaków.

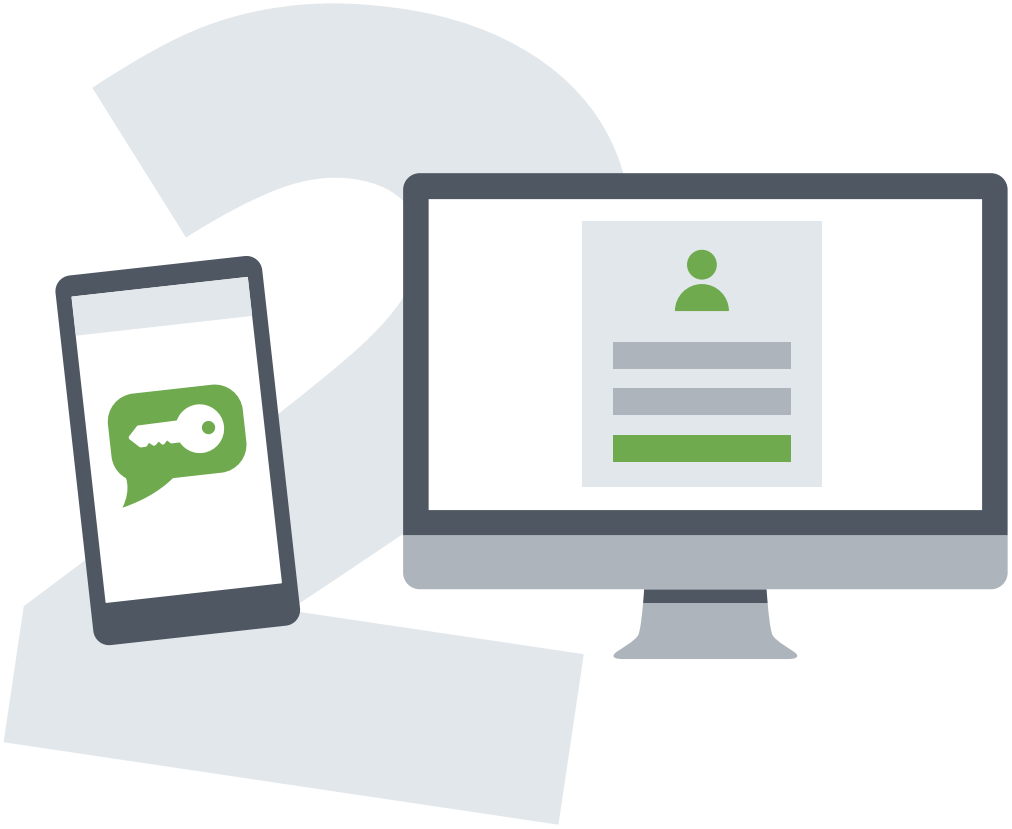
Jak dbać o bezpieczeństwo haseł?

1. Przechowuj je w bezpiecznym miejscu - najlepiej w pamięci. Nie udostępniaj nikomu swoich haseł i nie zapisuj ich otwartym tekstem w telefonie czy w notesie, bo w przypadku kradzieży torby, złodziej zyska dostęp do wszystkich Twoich kont.
2. Ustawiaj zróżnicowane hasła. Pamiętaj, że hasło może być wykradzione nie tylko w wyniku phishingu, ale także włamania np. do słabo zabezpieczonego sklepu internetowego. Jeśli wszędzie posługujesz się tym samym hasłem, otwierasz złodziejom drzwi do dużo cenniejszych zasobów.
3. Nie lekceważ siły hasła np. gdy kupujesz coś w sieci lub zakładasz konto w serwisie, z którego skorzystasz tylko raz. Twoje hasło i dane mogą zostać przechwycone wszędzie, więc zachowaj czujność nawet w przypadku kont, które niewiele dla Ciebie znaczą.
4. Gdy zaczniesz bardziej dbać o bezpieczeństwo w sieci, liczba haseł do zapamiętania będzie rosła w zatrważającym tempie: konta bankowe, w mediach społecznościowych, na serwisach e-commerce i aukcyjnych, w systemach potrzebnych do pracy zawodowej. Jeśli obawiasz się, że pamięć Cię zawiedzie, zamiast obniżać stopień skomplikowania haseł, zainstaluj na swoim urządzeniu menedżera haseł.

Liczba haseł do zapamiętania rośnie w zatrważającym tempie? Zamiast obniżać stopień ich skomplikowania, zainstaluj na swoim urządzeniu menedżera haseł.

2. Jak zabezpieczyć swoje urządzenie?

Po przeczytaniu całego e-booka potrafisz już odróżnić phishing od bezpiecznych operacji, wiesz, na co uważać i umiesz tworzyć dobre hasła. Niestety, to wszystko może nie wystarczyć, jeśli nie zabezpieczysz urządzeń, z których korzystasz.
I pamiętaj - dotyczy to nie tylko komputerów, ale i wszelkich urządzeń mobilnych.



Korzystaj z dwustopniowej weryfikacji. Podwójna ochrona utrudni oszustom uzyskanie dostępu do Twojego konta.

Co możesz zrobić, by zabezpieczyć swoje urządzenie?

1. Aktualizuj oprogramowanie, z którego korzystasz - wszystkie systemy mają luki i są one chętnie wykorzystywane przez hackerów, więc warto korzystać z wersji z wprowadzonymi poprawkami.
2. Korzystaj z dwustopniowej weryfikacji. Podwójna ochrona utrudni oszustom uzyskanie dostępu do Twojego konta.
3. Korzystaj z mocnych haseł i stosuj unikatowe hasła do różnych systemów.
4. Do przechowywania haseł używaj menedżerów haseł np. https://keepass.info.
5. Zaszyfruj cały twardy dysk w laptopie i smartfonie, aby uchronić swój sprzęt przed nieuprawnionym dostępem do danych.
6. Instaluj tylko oprogramowanie ze znanych źródeł - nie ściągaj programów z nieoficjalnych i niezaufanych stron.
7. Sprawdzaj, czy Twoje połączenie ze stroną jest szyfrowane. Jednym z wyznaczników bezpieczeństwa jest m.in. słynna zielona kłódka, ale i ona nie daje 100% pewności - trzeba sprawdzić, dla kogo został wystawiony certyfikat.
8. Zainstaluj i odświeżaj program antywirusowy, który wyłapie znane i masowo wysyłane zagrożenia.
9. Nie wykonuj transakcji i nie loguj się do serwisów internetowych korzystając z publicznych i otwartych sieci typu hotspot np. w McDonalds czy w autobusach. Prawdopodobieństwo przechwycenia poufnych danych w takich sieciach jest bardzo duże.
10. Uważaj na to, co wrzucasz do sieci, bo cyberoszuści mogą to wykorzystać przeciwko Tobie i Twoim bliskim.
11. Nie zapomnij o ochronie swojego urządzenia mobilnego - zabezpiecz telefon hasłem lub odciskiem biometrycznym i nie instaluj aplikacji niewiadomego pochodzenia.