Nie daj się złowić w sieci

Internet już na dobre trafił pod nasze strzechy. Według raportu Głównego Urzędu Statystycznego[1], ponad 90 proc. polskich gospodarstw domowych miało do niego dostęp. Pandemia przyspieszyła ten trend i doprowadziła do raptownej cyfryzacji zarówno sektora publicznego (dla przykładu, w 2020 r. ok 3,4 mln użytkowników założyło profil zaufany), jak i prywatnego. Gdy zamknięte były sklepy stacjonarne, powszechnie robiliśmy zakupy w sieci. Jak wynika z raportu „E-commerce w Polsce. Gemius dla e-Commerce Polska", aż 73 proc. respondentów zrobiło w 2020 r. zakupy w sieci. To o 13 proc. więcej niż rok wcześniej.

Odwrotu od cyfrowego świata już nie ma. Tym bardziej warto zwrócić uwagę na to, czy jesteśmy w nim bezpieczni i czy umiemy się w nim poruszać.

Przestępstwa w sieci to nie tylko miejska legenda

Rok do roku zagrożenie ze strony cyberprzestępców staje się bardziej realne. Jak wynika z badania, które na potrzeby swojej kampanii przeprowadził właśnie mBank[2], już co drugi z nas zetknął się z jakąś formą oszustwa w Internecie. To bardzo niepokojące dane, bo oznaczają, że sieci zastawione przez przestępców są dosłownie wszędzie. Potwierdzają je także statystyki polskiej Policji. W ciągu ostatnich czterech lat liczba zarejestrowanych cyberprzestępstw wzrosła o połowę, sięgając w 2020 r. aż 55 tys. przypadków. A to tylko dane zarejestrowane.

CERT Orange w swoim raporcie[3] podkreśla, że pomysłowość przestępców w sieci nie zna granic. Dopasowują oni swoje metody do najbardziej aktualnych trendów i zdarzeń po to, żeby jak najbardziej uśpić naszą czujność. I tak w ubiegłym, pandemicznym roku, najczęściej zdarzały się właśnie przestępstwa związane z handlem elektronicznym. Mieliśmy do czynienia z podszywaniem się pod sklepy, urzędy, firmy telekomunikacyjne i wreszcie – firmy kurierskie. Wiele z przestępstw dotyczyło też stron z zapisami na szczepienia, profilu zaufanego czy innych informacji o koronawirusie. Wszystko po to, żeby wywołać w nas poczucie pilności sprawy, konieczności jej załatwienia. Gdy jesteśmy pod presją, łatwiej ulegamy socjotechnikom stosowanym przez przestępców.

Nasza waluta online, czyli co chcą nam ukraść?

W realnym świecie dokładnie wiemy, co chcemy zabezpieczyć przed złodziejami.

Chronimy swoje domy i samochody, zakładając alarmy. Gdy jedziemy tramwajem, trzymamy torbę z portfelem i telefonem blisko siebie. Gdy zgubimy portfel – zastrzegamy karty i dowody.

Ale co interesuje przestępców najbardziej w świecie Internetu? To proste. Ich celem są nasze dane. Im ich więcej i bardziej wrażliwe – tym bardziej łakomym kąskiem się stają. Do tej kategorii należy zaliczyć dane osobowe czyli: imię i nazwisko, PESEL, adres zamieszkania, nazwisko panieńskie matki, nr dowodu osobistego czy paszportu i nr telefonu. Przestępcy chętnie też wykradają nasze adresy mailowe, profile na mediach społecznościowych i hasła do nich.

Szczególną kategorią danych są tzw. dane wrażliwe, zwłaszcza nr rachunków bankowych, PIN-y do kart i aplikacji, nr kart płatniczych i kody CVC/CVV (znajdują się na odwrocie kart), a także najbardziej interesujące dla złodziei: loginy i hasła do bankowości internetowej.

Podczas próby kradzieży złodzieje wyłudzają te dane po to, żeby przejąć kontrolę nad naszym kontem i ostatecznie „wyczyścić" rachunek ze wszystkich pieniędzy. Często też kradną naszą tożsamość, żeby wyłudzić kredyt czy użyć naszych danych do założenia konta „na słupa" – czyli rachunku, który posłuży im do wyprowadzenia pieniędzy od faktycznej ofiary.

Banki i inne instytucje dwoją się i troją, żeby jak najlepiej zabezpieczyć swoje usługi. Jednak w walce z cyberprzestępczością udział musimy brać także my, użytkownicy. Możemy to robić, zachowując czujność na każdym etapie. Warto więc pamiętać, że w sieci najlepszym towarem dla przestępców są właśnie nasze dane. Jeśli będziemy mieć tego świadomość, z większą rezerwą będziemy je podawać w różnych nietypowych miejscach i podczas rozmów telefonicznych.

Najczęstsze rodzaje przestępstw i sposoby, jak się przed nimi chronić

Poniżej opiszę kilka pojęć ze świata cyberbezpieczeństwa, które należy znać, żeby łatwo rozróżnić sytuację, z którą mamy do czynienia. Do najczęstszych rodzajów przestępstw należą:

– PHISHING. Choć może się kojarzyć z wędkarstwem, to jedna z najbardziej powszechnych metod wyłudzania danych i kradzieży pieniędzy. Jak to działa? Dziecinnie prosto! Przestępcy rozsyłają nam maile lub SMS-y, w których umieszczają linki prowadzące do fałszywych stron lub załączniki, które mają zainfekować nasz komputer/telefon.

Bardzo często są to wiadomości, w których podszywają się pod banki, operatorów

komórkowych, kurierów, dostawców usług, jak np. gazownia czy nawet… urzędy skarbowe i inne instytucje państwowe. Wiadomości te łączy jedna rzecz: właściwie wszystkie są „BARDZO WAŻNE”, „PILNE” i każda z nich straszy nas „KONSEKWENCJAMI”. W ostatnim roku szczególnie popularne były SMS-y z informacją o konieczności dopłaty do paczki, żeby ją zdezynfekować…

W większości przypadków gdy klikniemy w taki link, zostaniemy przeniesieni na stronę www łudząco podobną do oryginalnej – może mieć niemalże ten sam adres, zieloną kłódkę, te same grafiki. Może to być strona urzędu, banku czy integratora płatności. Na tej stronie zostaniemy poproszeni o podanie danych – bardzo często danych do logowania do banku lub danych naszej karty kredytowej. Wszystkie informacje, jakie wpiszemy na fałszywej stronie, trafią do złodziei a ci wypłacają pieniądze z naszego konta bez naszej wiedzy.

Możemy też paść ofiarą przestępców, którzy chcą na naszych komputerach/smartfonach zainstalować złośliwe oprogramowanie, które albo zaszyfruje nam dane na komputerze, albo będzie nas śledzić, albo „wstrzyknie” nieprawdziwe informacje na stronę www, którą właśnie przeglądamy i w ten sposób wyłudzi nasze dane. Tak może się stać, jeśli otworzymy załączniki zawarte w tych fałszywych mailach.

Warto pamiętać, że wiadomości te to nie tylko e-maile ale także SMS-y, czy nawet… prywatne wiadomości na Facebooku czy innych mediach społecznościowych. Zasada działania jest taka sama, choć sam „przekręt” może zaczynać się inaczej.

Jak się przed tym ochronić?

Przede wszystkim, zawsze i w każdej sytuacji trzeba zachować czujność. Jeśli nie znamy adresata, najlepiej po prostu zignorować wiadomość, nie otwierać jej i usunąć. Jeśli jednak otworzymy wiadomość, bo wydaje nam się, że zawiera ważne dla nas informacje albo pochodzi od firmy, z którą współpracujemy, to uważnie przyjrzyjmy się treści. Czy to nas w ogóle dotyczy? Czy nie ma w niej błędów ortograficznych, stylistycznych, błędnego logotypu? Za każdym razem, kiedy sprawa jest nietypowa, lepiej zadzwonić do firmy i wyjaśnić, o co może chodzić. Pod żadnym pozorem nie otwierajmy załączników ani nie klikajmy w linki zawarte w wiadomości.

Naczelną zasadą jest także korzystanie z programów antywirusowych, które pomogą chronić nasz komputer przed różnego rodzaju wirusami.

– VISHING – czyli łowienie przez telefon. To coraz częstsza metoda oszustów. Dzwonią do nas, podając się za pracownika banku, pracownika Policji, doradcę inwestycyjnego. Co możemy usłyszeć?

Metoda „na wnuczka” – dotyczy zwłaszcza starszych osób. Przestępcy dzwonią i podają się za członka bliskiej rodziny lub jego znajomego. Tłumaczą, że pilnie potrzebują pomocy, bo znaleźli się w trudnej sytuacji zdrowotnej czy finansowej. Podają kilka szczegółów, żeby się uwiarygodnić i naciskają na rozmówcę tworząc dramatyczną atmosferę. A potem… proszą o przelew na nr konta, który podają. Nie trzeba dalej tłumaczyć, że członek rodziny, o którym mowa, nie ma pojęcia, że ktoś wyłudził od ich bliskich pieniądze.

Metoda „na Policjanta” – jest, niestety, coraz częstsza. Złodzieje przedstawiają się jako policjanci i tłumaczą, że prowadzą operację przeciwko zorganizowanej grupie przestępczej. Podają nawet nr jednostki i telefon do niej, żeby się uwiarygodnić. Jak można się domyślić, nawet jeśli ofiara zadzwoniłaby pod podany numer – będzie znów rozmawiać z przestępcą. Potem „Policjant” tłumaczy, że prosi o pomoc w akcji i wręczenie podejrzanym gotówki albo zrobienie przelewu na podany nr rachunku. Jak można się domyślać, złodzieje tłumaczą, że cała operacja jest tajna i nikomu nie można o niej mówić. Gdy ofiara pojawia się w banku po pieniądze, też ma „nic nie mówić”, bo – jak tłumaczy „Policjant” – pracownicy banku są w zmowie z grupą przestępczą. Naturalnie gdy tylko dostaną pieniądze, przestępcy znikają. Znane są przypadki oszustw nawet na kilkaset tysięcy złotych, w których ofiary zaciągały nawet kredyty w bankach, żeby „pomóc Policji”.

Jak można się przed tym chronić? Jeszcze raz: zachować zdrowy rozsądek. Jeśli odbierzemy taki telefon, to najlepiej sprawdzić później osobiście w jednostce, czy faktycznie taki „Policjant” tam pracuje i prowadzi konkretną sprawę. Policja nie nakłania obywateli do pomocy przy takich sprawach, bo dysponuje innymi metodami. Pamiętajmy, żeby nikomu nie podawać naszych prywatnych haseł do banku ani na nikogo nie zaciągać kredytów.

Metoda „na pracownika banku lub innej instytucji finansowej” – odbieramy telefon, w którym ktoś podaje się za pracownika banku i mówi, że na naszym koncie doszło do nietypowej sytuacji: jest zablokowane, ktoś przelał z niego jakieś pieniądze, zerwał lokatę itd. „Pracownik” chce, żebyśmy mu podali dane identyfikacyjne albo zainstalowali dodatkową aplikację na swoim smartfonie, która ma nas „ochronić”. Tak naprawdę, oszust chce uzyskać nasze dane, żeby przejąć kontrolę nad kontem i nas okraść lub zadłużyć. Natomiast „aplikacja”, która ma nas chronić, w efekcie uzyska dostęp do naszych danych na telefonie, w tym do aplikacji bankowej. Rozpoznać oszustów jest tym trudniej, że dzięki różnym programom mogą oni wyświetlić nam nr telefonu, który znamy i pod którym zazwyczaj kontaktujemy się z bankiem.

Co można zrobić w tej sytuacji?

Znów: warto zachować zdrowy rozsądek. Przede wszystkim gdy ktoś do nas dzwoni – nie

podawać żadnych haseł ani innych wrażliwych danych. To nie my dzwonimy do banku, warto o tym pamiętać! Nie instalujmy żadnych aplikacji, jeśli nie pochodzą one ze znanego źródła, bo najprawdopodobniej są to aplikacje ze złośliwym oprogramowaniem. Jeśli jednak już coś zatwierdzamy, to uważnie czytajmy komunikaty, które przychodzą z banku – czy na pewno dotyczą tego, na co się zgodziliśmy? Nigdy nie potwierdzajmy transakcji, których sami nie zaczęliśmy – żadnego dodania odbiorcy do zaufanych czy wykonania przelewu! Warto pamiętać, że pracownicy banków nigdy nie będą prosić o podanie hasła do banku czy innych wrażliwych danych. Nie będą też przesyłać żadnych aplikacji do zainstalowania, bo oficjalne aplikacje dostępne są w sklepach GooglePlay czy AppStore.

– PODSZYWANIE SIĘ POD ZNAJOMEGO na Facebooku lub innych portalach społecznościowych. To także coraz bardziej powszechna metoda oszustwa. Oszuści przejmują konto znajomego i zaczynają rozmowę z nami. Często dość trudno jest zorientować się, że rozmawiamy ze złodziejem, bo dopasowuje się on do stylu naszego znajomego, może nawet wspominać wspólnych znajomych. Bardzo często proszą o przelew na niską kwotę i wysyłają link do płatności – po jej kliknięciu jesteśmy przekierowani na fałszywą stronę, która wyłudzi nasze dane. Inną metodą jest prośba o wsparcie finansowe. Złodzieje proszą o niewielki przelew i potwierdzenie płatności naszym kodem BLIK. W obu przypadkach stracimy pieniądze.

Co zrobić?

Jeśli znajomy prosi Cię o przelew na komunikatorze, zadzwońmy do niego i potwierdźmy, że to faktycznie on. Jeśli okaże się, że jednak o nic nie prosił, polećmy mu zmianę hasła i przeskanowanie komputera i telefonu programem antywirusowym.

– FAŁSZYWE SKLEPY internetowe. Trudno nam rozpoznać to przestępstwo od razu, bo na pierwszy rzut oka wszystko wygląda odpowiednio. Gdy szukamy jakiejś rzeczy w Internecie, często porównujemy ceny w różnych miejscach. I nagle trafiamy na wyjątkową okazję! Niższa cena, szybsza dostawa. Nic, tylko kupować. Płacimy więc za towar, który… nigdy do nas nie przychodzi. Zostaliśmy oszukani, ale pieniędzy najprawdopodobniej już nie odzyskamy.

Co zrobić?

Przed zakupem uważnie sprawdźmy sklep. Poszukajmy, co inni piszą na jego temat na forach czy w social mediach. Warto zwrócić uwagę na jakość i różnorodność komentarzy. Same pozytywy to też niewłaściwy sygnał, bo oszuści mogą te komentarze stworzyć samodzielnie. Sprawdźmy firmę w KRS-ie, czy faktycznie jest zarejestrowana. A jeśli okazja jest naprawdę spora, zadzwońmy pod numer podany na stronie sklepu

i zapytajmy, skąd taka atrakcyjna cena. Kontakt telefoniczny może czasem wiele wyjaśnić.

Metody, które wymieniłam powyżej, to tylko najpopularniejsze scenariusze oszustw w sieci. A wyobraźnia złodziei naprawdę nie zna granic. Dlatego na każdym kroku trzeba zachować czujność i dbać o własne dane i pieniądze. Pamiętajmy, że ich poufność zależy głównie od nas, a przestępcy zrobią wszystko, byle je tylko dostać.

Higiena życia online

Wielu stresujących sytuacji możemy uniknąć, jeśli tylko będziemy pamiętać o kilku podstawowych zasadach funkcjonowania w sieci. Jest ich naprawdę niewiele, a warto, żeby stały się naszym nawykiem, bo mogą ochronić nas przed kosztownymi błędami i stresem z nimi związanymi.

Pamiętajmy, żeby:

– zachować czujność wobec maili i SMS-ów, zwłaszcza, jeśli nie znamy nadawcy lub sprawa wydaje się nam podejrzana. Nie klikajmy w żadne zawarte w takich wiadomościach linki, nie otwierajmy załączników. Jeśli możemy, zadzwońmy do instytucji, z której przyszła wiadomość i wyjaśnijmy sprawę;

– nie podawać nikomu swoich poufnych danych. Nasze dane osobowe, ale także PINy do kart, hasła i identyfikatory, nr kart czy ich kody CVV (widoczne na rewersie karty) należą tylko do nas. Nikomu ich nie przekazujmy;

– uważać, z kim rozmawiamy. Jeśli znajomy wysyła nam link lub prośbę o kod BLIK, potwierdźmy telefonicznie, że to faktycznie on. Jeśli dzwoni do nas ktoś podający się za policjanta, pracownika banku czy innej instytucji, również zachowajmy czujność. Nie instalujmy nic, sprawdźmy tożsamość rozmówcy i sprawę, z jaką do nas dzwoni;

– przed kliknięciem bardzo uważnie przeczytać, na co się zgadzamy lub jaką operację wykonujemy. Pośpiech to bardzo zły doradca;

– korzystać z programów antywirusowych i firewalli. One pomogą obronić się przed złośliwym oprogramowaniem;

– używać tylko oryginalnego, legalnego oprogramowania i pamiętać o tym, żeby je regularnie aktualizować. Aktualizacje są niezbędne, działają jak łatki na podartym swetrze. Dzięki nim przestępcy nie będą mogli wykorzystać luk w oprogramowaniu;

– nie instalować aplikacji z linków czy innych nieznanych źródeł. Jeśli chcemy mieć

aplikację, zainstalujmy ją z oficjalnego sklepu GooglePlay, Appstore lub Huawei AppGallery;

– nie używać tego samego hasła do wszystkich serwisów. Im trudniejsze i rzadsze hasło, tym większą mamy gwarancję, że będzie bezpieczniejsze;

– sprawdzać strony www, na jakich jesteśmy. Szukajmy zielonej kłódki oznaczającej szyfrowane połączenie, szukajmy certyfikatów stron.

To tylko kilka dobrych rad, które nie zastąpią zdrowego rozsądku. Pamiętajmy, że większość oszustw w sieci opartych jest na socjotechnice, co oznacza, że przestępcy chcą wykorzystać naszą nieuwagę, pośpiech i strach. Nie dajmy się na to nabrać. Na szali są nasze pieniądze i spokój.

Katarzyna Rulkiewicz

Panaceum 7-8/2021

[1] Społeczeństwo informacyjne w Polsce w 2020 r., GUS

[2] Ogólnopolskie badanie CAWI na panelu badawczym Norstat.pl na próbie N=1000 dorosłych Polaków

[3] https://cert.orange.pl/raporty-cert

Internet już na dobre trafił pod nasze strzechy. Według raportu Głównego Urzędu Statystycznego[1], ponad 90 proc. polskich gospodarstw domowych miało do niego dostęp. Pandemia przyspieszyła ten trend i doprowadziła do raptownej cyfryzacji zarówno sektora publicznego (dla przykładu, w 2020 r. ok 3,4 mln użytkowników założyło profil zaufany), jak i prywatnego. Gdy zamknięte były sklepy stacjonarne, powszechnie robiliśmy zakupy w sieci. Jak wynika z raportu „E-commerce w Polsce. Gemius dla e-Commerce Polska", aż 73 proc. respondentów zrobiło w 2020 r. zakupy w sieci. To o 13 proc. więcej niż rok wcześniej.

Odwrotu od cyfrowego świata już nie ma. Tym bardziej warto zwrócić uwagę na to, czy jesteśmy w nim bezpieczni i czy umiemy się w nim poruszać.

Przestępstwa w sieci to nie tylko miejska legenda

Rok do roku zagrożenie ze strony cyberprzestępców staje się bardziej realne. Jak wynika z badania, które na potrzeby swojej kampanii przeprowadził właśnie mBank[2], już co drugi z nas zetknął się z jakąś formą oszustwa w Internecie. To bardzo niepokojące dane,

bo oznaczają, że sieci zastawione przez przestępców są dosłownie wszędzie. Potwierdzają je także statystyki polskiej Policji. W ciągu ostatnich czterech lat liczba zarejestrowanych cyberprzestępstw wzrosła o połowę, sięgając w 2020 r. aż 55 tys. przypadków. A to tylko dane zarejestrowane.

CERT Orange w swoim raporcie[3] podkreśla, że pomysłowość przestępców w sieci nie zna granic. Dopasowują oni swoje metody do najbardziej aktualnych trendów i zdarzeń po to, żeby jak najbardziej uśpić naszą czujność. I tak w ubiegłym, pandemicznym roku, najczęściej zdarzały się właśnie przestępstwa związane z handlem elektronicznym. Mieliśmy do czynienia z podszywaniem się pod sklepy, urzędy, firmy telekomunikacyjne i wreszcie – firmy kurierskie. Wiele z przestępstw dotyczyło też stron z zapisami na szczepienia, profilu zaufanego czy innych informacji o koronawirusie. Wszystko po to, żeby wywołać w nas poczucie pilności sprawy, konieczności jej załatwienia. Gdy jesteśmy pod presją, łatwiej ulegamy socjotechnikom stosowanym przez przestępców.

Nasza waluta online, czyli co chcą nam ukraść?

W realnym świecie dokładnie wiemy, co chcemy zabezpieczyć przed złodziejami. Chronimy swoje domy i samochody, zakładając alarmy. Gdy jedziemy tramwajem, trzymamy torbę z portfelem i telefonem blisko siebie. Gdy zgubimy portfel – zastrzegamy karty i dowody.

Ale co interesuje przestępców najbardziej w świecie Internetu? To proste. Ich celem są nasze dane. Im ich więcej i bardziej wrażliwe – tym bardziej łakomym kąskiem się stają. Do tej kategorii należy zaliczyć dane osobowe czyli: imię i nazwisko, PESEL, adres zamieszkania, nazwisko panieńskie matki, nr dowodu osobistego czy paszportu i nr telefonu. Przestępcy chętnie też wykradają nasze adresy mailowe, profile na mediach społecznościowych i hasła do nich.

Szczególną kategorią danych są tzw. dane wrażliwe, zwłaszcza nr rachunków bankowych, PIN-y do kart i aplikacji, nr kart płatniczych i kody CVC/CVV (znajdują się na odwrocie kart), a także najbardziej interesujące dla złodziei: loginy i hasła do bankowości internetowej.

Podczas próby kradzieży złodzieje wyłudzają te dane po to, żeby przejąć kontrolę nad naszym kontem i ostatecznie „wyczyścić” rachunek ze wszystkich pieniędzy. Często też kradną naszą tożsamość, żeby wyłudzić kredyt czy użyć naszych danych do założenia konta „na słupa” – czyli rachunku, który posłuży im do wyprowadzenia pieniędzy od faktycznej ofiary.

Banki i inne instytucje dwoją się i troją, żeby jak najlepiej zabezpieczyć swoje usługi.

Jednak w walce z cyberprzestępczością udział musimy brać także my, użytkownicy. Możemy to robić, zachowując czujność na każdym etapie. Warto więc pamiętać, że w sieci najlepszym towarem dla przestępców są właśnie nasze dane. Jeśli będziemy mieć tego świadomość, z większą rezerwą będziemy je podawać w różnych nietypowych miejscach i podczas rozmów telefonicznych.

Najczęstsze rodzaje przestępstw i sposoby, jak się przed nimi chronić

Poniżej opiszę kilka pojęć ze świata cyberbezpieczeństwa, które należy znać, żeby łatwo rozróżnić sytuację, z którą mamy do czynienia. Do najczęstszych rodzajów przestępstw należą:

– PHISHING. Choć może się kojarzyć z wędkarstwem, to jedna z najbardziej powszechnych metod wyłudzania danych i kradzieży pieniędzy. Jak to działa? Dziecinnie prosto! Przestępcy rozsyłają nam maile lub SMS-y, w których umieszczają linki prowadzące do fałszywych stron lub załączniki, które mają zainfekować nasz komputer/telefon.

Bardzo często są to wiadomości, w których podszywają się pod banki, operatorów komórkowych, kurierów, dostawców usług, jak np. gazownia czy nawet… urzędy skarbowe i inne instytucje państwowe. Wiadomości te łączy jedna rzecz: właściwie wszystkie są „BARDZO WAŻNE", „PILNE" i każda z nich straszy nas „KONSEKWENCJAMI". W ostatnim roku szczególnie popularne były SMS-y z informacją o konieczności dopłaty do paczki, żeby ją zdezynfekować…

W większości przypadków gdy klikniemy w taki link, zostaniemy przeniesieni na stronę www łudząco podobną do oryginalnej – może mieć niemalże ten sam adres, zieloną kłódkę, te same grafiki. Może to być strona urzędu, banku czy integratora płatności. Na tej stronie zostaniemy poproszeni o podanie danych – bardzo często danych do logowania do banku lub danych naszej karty kredytowej. Wszystkie informacje, jakie wpiszemy na fałszywej stronie, trafią do złodziei a ci wypłacają pieniądze z naszego konta bez naszej wiedzy.

Możemy też paść ofiarą przestępców, którzy chcą na naszych komputerach/smartfonach zainstalować złośliwe oprogramowanie, które albo zaszyfruje nam dane na komputerze, albo będzie nas śledzić, albo „wstrzyknie" nieprawdziwe informacje na stronę www, którą właśnie przeglądamy i w ten sposób wyłudzi nasze dane. Tak może się stać, jeśli otworzymy załączniki zawarte w tych fałszywych mailach.

Warto pamiętać, że wiadomości te to nie tylko e-maile ale także SMS-y, czy nawet… prywatne wiadomości na Facebooku czy innych mediach społecznościowych. Zasada działania jest taka sama, choć sam „przekręt" może zaczynać się inaczej.

Jak się przed tym ochronić?

Przede wszystkim, zawsze i w każdej sytuacji trzeba zachować czujność. Jeśli nie znamy adresata, najlepiej po prostu zignorować wiadomość, nie otwierać jej i usunąć. Jeśli jednak otworzymy wiadomość, bo wydaje nam się, że zawiera ważne dla nas informacje albo pochodzi od firmy, z którą współpracujemy, to uważnie przyjrzyjmy się treści. Czy to nas w ogóle dotyczy? Czy nie ma w niej błędów ortograficznych, stylistycznych, błędnego logotypu? Za każdym razem, kiedy sprawa jest nietypowa, lepiej zadzwonić do firmy i wyjaśnić, o co może chodzić. Pod żadnym pozorem nie otwierajmy załączników ani nie klikajmy w linki zawarte w wiadomości.

Naczelną zasadą jest także korzystanie z programów antywirusowych, które pomogą chronić nasz komputer przed różnego rodzaju wirusami.

– VISHING – czyli łowienie przez telefon. To coraz częstsza metoda oszustów. Dzwonią do nas, podając się za pracownika banku, pracownika Policji, doradcę inwestycyjnego. Co możemy usłyszeć?

Metoda „na wnuczka” – dotyczy zwłaszcza starszych osób. Przestępcy dzwonią i podają się za członka bliskiej rodziny lub jego znajomego. Tłumaczą, że pilnie potrzebują pomocy, bo znaleźli się w trudnej sytuacji zdrowotnej czy finansowej. Podają kilka szczegółów, żeby się uwiarygodnić i naciskają na rozmówcę tworząc dramatyczną atmosferę. A potem… proszą o przelew na nr konta, który podają. Nie trzeba dalej tłumaczyć, że członek rodziny, o którym mowa, nie ma pojęcia, że ktoś wyłudził od ich bliskich pieniądze.

Metoda „na Policjanta” – jest, niestety, coraz częstsza. Złodzieje przedstawiają się jako policjanci i tłumaczą, że prowadzą operację przeciwko zorganizowanej grupie przestępczej. Podają nawet nr jednostki i telefon do niej, żeby się uwiarygodnić. Jak można się domyślić, nawet jeśli ofiara zadzwoniłaby pod podany numer – będzie znów rozmawiać z przestępcą. Potem „Policjant” tłumaczy, że prosi o pomoc w akcji i wręczenie podejrzanym gotówki albo zrobienie przelewu na podany nr rachunku. Jak można się domyślać, złodzieje tłumaczą, że cała operacja jest tajna i nikomu nie można o niej mówić. Gdy ofiara pojawia się w banku po pieniądze, też ma „nic nie mówić”, bo – jak tłumaczy „Policjant” – pracownicy banku są w zmowie z grupą przestępczą. Naturalnie gdy tylko dostaną pieniądze, przestępcy znikają. Znane są przypadki oszustw nawet na kilkaset tysięcy złotych, w których ofiary zaciągały nawet kredyty w bankach, żeby „pomóc Policji”.

Jak można się przed tym chronić? Jeszcze raz: zachować zdrowy rozsądek. Jeśli odbierzemy taki telefon, to najlepiej sprawdzić później osobiście w jednostce, czy faktycznie taki „Policjant” tam pracuje i prowadzi konkretną sprawę. Policja nie nakłania

obywateli do pomocy przy takich sprawach, bo dysponuje innymi metodami. Pamiętajmy, żeby nikomu nie podawać naszych prywatnych haseł do banku ani na nikogo nie zaciągać kredytów.

Metoda „na pracownika banku lub innej instytucji finansowej" – odbieramy telefon, w którym ktoś podaje się za pracownika banku i mówi, że na naszym koncie doszło do nietypowej sytuacji: jest zablokowane, ktoś przelał z niego jakieś pieniądze, zerwał lokatę itd. „Pracownik" chce, żebyśmy mu podali dane identyfikacyjne albo zainstalowali dodatkową aplikację na swoim smartfonie, która ma nas „ochronić". Tak naprawdę, oszust chce uzyskać nasze dane, żeby przejąć kontrolę nad kontem i nas okraść lub zadłużyć. Natomiast „aplikacja", która ma nas chronić, w efekcie uzyska dostęp do naszych danych na telefonie, w tym do aplikacji bankowej. Rozpoznać oszustów jest tym trudniej, że dzięki różnym programom mogą oni wyświetlić nam nr telefonu, który znamy i pod którym zazwyczaj kontaktujemy się z bankiem.

Co można zrobić w tej sytuacji?

Znów: warto zachować zdrowy rozsądek. Przede wszystkim gdy ktoś do nas dzwoni – nie podawać żadnych haseł ani innych wrażliwych danych. To nie my dzwonimy do banku, warto o tym pamiętać! Nie instalujmy żadnych aplikacji, jeśli nie pochodzą one ze znanego źródła, bo najprawdopodobniej są to aplikacje ze złośliwym oprogramowaniem. Jeśli jednak już coś zatwierdzamy, to uważnie czytajmy komunikaty, które przychodzą z banku – czy na pewno dotyczą tego, na co się zgodziliśmy? Nigdy nie potwierdzajmy transakcji, których sami nie zaczęliśmy – żadnego dodania odbiorcy do zaufanych czy wykonania przelewu! Warto pamiętać, że pracownicy banków nigdy nie będą prosić o podanie hasła do banku czy innych wrażliwych danych. Nie będą też przesyłać żadnych aplikacji do zainstalowania, bo oficjalne aplikacje dostępne są w sklepach GooglePlay czy AppStore.

– PODSZYWANIE SIĘ POD ZNAJOMEGO na Facebooku lub innych portalach społecznościowych. To także coraz bardziej powszechna metoda oszustwa. Oszuści przejmują konto znajomego i zaczynają rozmowę z nami. Często dość trudno jest zorientować się, że rozmawiamy ze złodziejem, bo dopasowuje się on do stylu naszego znajomego, może nawet wspominać wspólnych znajomych. Bardzo często proszą o przelew na niską kwotę i wysyłają link do płatności – po jej kliknięciu jesteśmy przekierowani na fałszywą stronę, która wyłudzi nasze dane. Inną metodą jest prośba o wsparcie finansowe. Złodzieje proszą o niewielki przelew i potwierdzenie płatności naszym kodem BLIK. W obu przypadkach stracimy pieniądze.

Co zrobić?

Jeśli znajomy prosi Cię o przelew na komunikatorze, zadzwońmy do niego i potwierdźmy, że to faktycznie on. Jeśli okaże się, że jednak o nic nie prosił, polećmy mu zmianę hasła i przeskanowanie komputera i telefonu programem antywirusowym.

– FAŁSZYWE SKLEPY internetowe. Trudno nam rozpoznać to przestępstwo od razu, bo na pierwszy rzut oka wszystko wygląda odpowiednio. Gdy szukamy jakiejś rzeczy w Internecie, często porównujemy ceny w różnych miejscach. I nagle trafiamy na wyjątkową okazję! Niższa cena, szybsza dostawa. Nic, tylko kupować. Płacimy więc za towar, który… nigdy do nas nie przychodzi. Zostaliśmy oszukani, ale pieniędzy najprawdopodobniej już nie odzyskamy.

Co zrobić?

Przed zakupem uważnie sprawdźmy sklep. Poszukajmy, co inni piszą na jego temat na forach czy w social mediach. Warto zwrócić uwagę na jakość i różnorodność komentarzy. Same pozytywy to też niewłaściwy sygnał, bo oszuści mogą te komentarze stworzyć samodzielnie. Sprawdźmy firmę w KRS-ie, czy faktycznie jest zarejestrowana. A jeśli okazja jest naprawdę spora, zadzwońmy pod numer podany na stronie sklepu i zapytajmy, skąd taka atrakcyjna cena. Kontakt telefoniczny może czasem wiele wyjaśnić.

Metody, które wymieniłam powyżej, to tylko najpopularniejsze scenariusze oszustw w sieci. A wyobraźnia złodziei naprawdę nie zna granic. Dlatego na każdym kroku trzeba zachować czujność i dbać o własne dane i pieniądze. Pamiętajmy, że ich poufność zależy głównie od nas, a przestępcy zrobią wszystko, byle je tylko dostać.

Higiena życia online

Wielu stresujących sytuacji możemy uniknąć, jeśli tylko będziemy pamiętać o kilku podstawowych zasadach funkcjonowania w sieci. Jest ich naprawdę niewiele, a warto, żeby stały się naszym nawykiem, bo mogą ochronić nas przed kosztownymi błędami i stresem z nimi związanymi.

Pamiętajmy, żeby:

– zachować czujność wobec maili i SMS-ów, zwłaszcza, jeśli nie znamy nadawcy lub sprawa wydaje się nam podejrzana. Nie klikajmy w żadne zawarte w takich wiadomościach linki, nie otwierajmy załączników. Jeśli możemy, zadzwońmy do instytucji, z której przyszła wiadomość i wyjaśnijmy sprawę;

– nie podawać nikomu swoich poufnych danych. Nasze dane osobowe, ale także PINy do kart, hasła i identyfikatory, nr kart czy ich kody CVV (widoczne na rewersie karty) należą

tylko do nas. Nikomu ich nie przekazujmy;

– uważać, z kim rozmawiamy. Jeśli znajomy wysyła nam link lub prośbę o kod BLIK, potwierdźmy telefonicznie, że to faktycznie on. Jeśli dzwoni do nas ktoś podający się za policjanta, pracownika banku czy innej instytucji, również zachowajmy czujność. Nie instalujmy nic, sprawdźmy tożsamość rozmówcy i sprawę, z jaką do nas dzwoni;

– przed kliknięciem bardzo uważnie przeczytać, na co się zgadzamy lub jaką operację wykonujemy. Pośpiech to bardzo zły doradca;

– korzystać z programów antywirusowych i firewalli. One pomogą obronić się przed złośliwym oprogramowaniem;

– używać tylko oryginalnego, legalnego oprogramowania i pamiętać o tym, żeby je regularnie aktualizować. Aktualizacje są niezbędne, działają jak łatki na podartym swetrze. Dzięki nim przestępcy nie będą mogli wykorzystać luk w oprogramowaniu;

– nie instalować aplikacji z linków czy innych nieznanych źródeł. Jeśli chcemy mieć aplikację, zainstalujmy ją z oficjalnego sklepu GooglePlay, Appstore lub Huawei AppGallery;

– nie używać tego samego hasła do wszystkich serwisów. Im trudniejsze i rzadsze hasło, tym większą mamy gwarancję, że będzie bezpieczniejsze;

– sprawdzać strony www, na jakich jesteśmy. Szukajmy zielonej kłódki oznaczającej szyfrowane połączenie, szukajmy certyfikatów stron.

To tylko kilka dobrych rad, które nie zastąpią zdrowego rozsądku. Pamiętajmy, że większość oszustw w sieci opartych jest na socjotechnice, co oznacza, że przestępcy chcą wykorzystać naszą nieuwagę, pośpiech i strach. Nie dajmy się na to nabrać. Na szali są nasze pieniądze i spokój.

Katarzyna Rulkiewicz

Panaceum 7-8/2021

[1] Społeczeństwo informacyjne w Polsce w 2020 r., GUS

[2] Ogólnopolskie badanie CAWI na panelu badawczym Norstat.pl na próbie N=1000 dorosłych Polaków

[3] https://cert.orange.pl/raporty-cert