materiał prasowy, 02.05.2023 r.

**Nowe sposoby oszustów na wyłudzenie naszych pieniędzy!**

**Duże technologiczne koncerny i małe start-upy nieustannie pracują nad rozwijaniem rozwiązań, które mają nam ułatwić życie. Za pomocą kilku kliknięć możemy zamówić zakupy, które w kilka dni trafią do nas
z drugiego końca świata. Nasze smartfony są coraz „mądrzejsze”. Stają się naszymi osobistymi centrami dowodzenia – pozwalają na prowadzenie biznesu „bez wychodzenia z domu”. Ale postęp i ciągłe bycie online mają też swoje konsekwencje. Cyberprzestępcy również starają się być na czasie i wymyślają coraz to nowsze sposoby, by wyłudzić nasze dane, które są im potrzebne do dokonywania kolejnych przestępstw. Głównie do kradzieży naszych pieniędzy. W 2022 roku zarejestrowano 322 tys. zgłoszeń naruszeń bezpieczeństwa
w polskiej sieci. Rok wcześniej było ich 116 tys., czyli mamy do czynienia ze wzrostem o 178% r./r.(!), co pokazuje skalę problemu[[1]](#footnote-1). W ostatnim czasie wśród oszustów „modne” stały się dwie metody: „na fałszywe
 e-recepty” i „na rezerwowe rachunek bankowy”. Chociaż scenariusze tych oszust są nowe, to jednak cyberzłodzieje bazują na tym, co zawsze: braku dbania internautów o bezpieczne poruszanie się po sieci
i zastraszaniu swych „ofiar”. Podpowiadamy, walczyć z cyberprzestępcami i na czym polegają ich „najnowsze” metody działania”.**

**Fałszywe e-recepty, czyli nowa metoda phishingowców[[2]](#footnote-2)**

E-recepty, czyli internetowe wersje tradycyjnych recept są coraz częściej stosowane. W związku z tym zwrócili na nie uwagę cyberprzestępcy, czyniąc z nich nowy sposób wyłudzania danych osobowych. Problem stał się na tyle poważny, że przed oszustwem ostrzega Ministerstwo Zdrowia, co nie dziwi, bo wizerunek Ministerstwa jest wykorzystywany przez oszustów do przeprowadzenia tzw. scamu. Jak wygląda w praktyce scenariusz oszustwa?

Rozsyłane są fałszywe wiadomości e-mail lub smsy. Zazwyczaj w ich treści znajduje się informacja o wystawieniu
e-recepty, do której ma prowadzić załączony link. Problem polega na tym, że link może zawierać w sobie elementy złośliwego oprogramowania, które zainstaluje na naszym komputerze wirusa czy aplikacje, poprzez które przestępcy będą śledzić nasze działania w sieci i/lub przekierowywać do strony, gdzie zostaną wyłudzone nasze dane.

– *W tym przypadku cyberprzestępcy wykorzystują to, że coraz więcej osób, dzięki nowym technologiom
i nowoczesnym rozwiązaniom chce ułatwić sobie życie, zaoszczędzić czas. Przykładem są e-recepty. Jeżeli często
z nich korzystamy, nasza czujność może zostać uśpiona – myślimy: „przecież tyle razy klikałam w te załączniki i nic złego się nie stało, dlaczego więc tym razem miało być coś pójść nie tak?”. To jednak błąd. Właśnie takie podejście liczą oszuści. Dlatego warto na co dzień stosować metodę ograniczanego zaufania. Dzięki temu nie staniemy się ofiarą cyberprzestępców i nie wpadniemy w problemy finansowe* – radzi **Jakub Baumgart, ekspert Intrum**.

Co zatem można zrobić, by nie paść ofiarą oszustwa „na e-receptę”? Przede wszystkim trzeba wiedzieć, jak wygląda e-recepta i jakimi kanałami może do nas dotrzeć.

1. **SMS z 4-cyfrowym kodem** – przesyłany przez lekarza; jako nadawca wiadomości będzie widnieć
„e-zdrowie” – informacja jest generowana przez państwowy, ogólnopolski system, ale uwaga! – w takim smsie nigdy nie znajdziemy dodatkowych linków czy próśb o rejestrację do zewnętrznych stron internetowych!,
2. **e-mail z załączoną w PDF-ie informacją o e-recepcie** – wysyłana przez rządowy system (w nadawcy powinna znaleźć się domena gov.pl); taką informację możemy otrzymać również bezpośrednio od lekarza czy jednostki, w której odbyła się wizyta lekarska, a która ma wprowadzony elektroniczny obieg dokumentami czy sposób kontaktu z pacjentami,
3. **powiadomienie/kod w aplikacji mojeIKP.**

Informacje z e-receptą powinniśmy otrzymać w krótkim czasie po jej wystawieniu, oczywiście po odbytej wizycie lekarskiej. – *Dlatego, jeżeli w ogóle nie oczekujemy na receptę, nie klikajmy w żadne wiadomości czy to sms,
czy mailowe, które sugerują, że są e-receptą, bo prawdopodobnie będzie to próba wyłudzenia naszych pieniędzy*
– komentuje **Jakub Baumgart, ekspert Intrum.** Jeżeli korzystamy z aplikacji mojeIKP czy np. z aplikacji/portalu internetowego danego ośrodka zdrowia, to prawdopodobnie musieliśmy wcześniej wyrazić zgodę na otrzymywanie informacji, w tym e-recept (po stronie nadawcy także leży obowiązek dbania o dane osobowe „klientów”). Dlatego najlepiej przyjąć ogólną zasadę nieotwierania linków, których pochodzenie nie jest dla nas jasne.

Gdy nadal będziemy mieć wątpliwości dotyczące otrzymanej e-recepty, możemy sprawdzić te informacje na oficjalnej stronie Ministerstwa Zdrowia lub kontaktując się z Telefoniczną Informację Pacjenta, dzwoniąc pod numer 800 190 590.

**Metoda na „konto rezerwowe”**

Oszuści bardzo często chcą uzyskać bezpośredni dostęp do naszych pieniędzy, poddając się za pracowników banku czy wysyłając drogą mailową czy smsem informacje zmuszające do takiego działania, które do złudzenia przypominają te stosowane przez banki. Przestępcy sukcesywnie opracowują kolejne metody oszustw. Kiedy wypływają one na światło dzienne, a media dokładnie opisują sposób ich działania, znajdują oni kolejne taktyki.

Ostatnio coraz częściej słyszy się o metodzie „na konto rezerwowe/zapasowe”. Ta taktyka wyjątkowo skutecznie usypia czujność konsumenta, bo oszuści dzwoniąc, podają się za pracownika banku i sami informują o zajściu przestępstwa, czym wzbudzają zaufanie potencjalnej ofiary.

Metoda działania jest następująca: odbieramy telefon – bardzo często od „znajomego” numeru swojego banku
z informacją, że np. zaobserwowano na naszym rachunku podejrzaną transakcję na wysoką sumę lub dokonano jednego dnia wielu wypłat z bankomatu. Osoba podająca się za pracownika banku będzie chciała potwierdzić te działania. Nie miały one realnie miejsca, nie dokonywaliśmy ich, więc dzwoniący informuje nas, że prawdopodobnie doszło do przestępstwa i ktoś wykradł nasze dane i otrzymał dostęp do naszego internetowego konta bankowego lub karty płatniczej. Przestępca – „pracownik banku” oferuje wtedy pomoc w założeniu nowego rachunku, abyśmy przelali na nie swoje pieniądze. Słyszymy jednak, że ze względów bezpieczeństwa, musimy zostać zweryfikowani.
Dokładnie w tym momencie zaczyna się „prawdziwe” przestępstwo. Oszust otrzymuje informacje o naszym numerze PESEL, ustala ze swoją „ofiarą” nowe hasło do bankowości elektronicznej. W dalszej kolejności dyktuje albo przesyła smsem numer do „nowego” rachunku bankowego i przekazuje instrukcje jak przelać na nie środki, aby były już bezpieczne. Jeżeli „ofiara” wykona ten krok, z dużym prawdopodobieństwem straci swoje pieniądze w kilka minut. Dlaczego ta metoda jest wyjątkowo skuteczna?

– *Przestępcy wzbudzają nasze emocje, a one obiorą górę nad rozsądkiem. Bardzo często to wygląda tak, że osoba, która pada ofiarą przestępstwa, dostaje w pracy telefon niby z banku o zajściu przestępstwa – że ktoś włamał się
na konto bankowe lub dokonał nieuprawnionej transakcji. W pierwszym momencie ofiara jest w szoku, ale potem wręcz cieszy się, że otrzymuje pomoc. Uważa, że założenie nowego konta, a przed tym podanie kluczowych, wrażliwych informacji rozwiąże problem. A to dopiero początek problemów* – komentuje **Jakub Baumgart, ekspert Intrum.**

Czy w takim razie w ogóle da się uchronić, przez metodą „na konto rezerwowe”? Tak, ale jeśli będziemy przestrzegać kilku wskazówek.

– *Po pierwsze, jeżeli korzystamy z bankowości elektronicznej, możemy samodzielnie zmienić login i hasło do naszego internetowego konta bankowego z poziomu platformy banku. O to w pierwszej kolejności prawdopodobnie poprosi „prawdziwy” pracownik banku, który będzie chciał nas poinformować o zajściu przestępstwa. Cały proces odbywa się bez ingerencji osoby z zewnątrz. Gdy otrzymujemy telefon o włamaniu się na nasze konto w portalu transakcyjnym banku, jeszcze lepszym pomysłem będzie pilne zablokowanie wszelkich dostępów, także transakcji kartą płatniczą, BLIKiem, itp. To też możemy wykonać samodzielnie. Warto następnie niezwłocznie udać się do placówki banku
i wyjaśnić całą sytuację. Pracownik banku rozwieje wszelkie nasze wątpliwości* – podpowiada **Jakub Baumgart, ekspert Intrum**.

Jeżeli bank zarejestruje sytuację, że na koncie danego klienta zaszły jakieś podejrzanie działania, może dokonać automatycznej blokady na koncie. To jedna z opcji zabezpieczeń stosowana przez banki. Jednak właśnie ze względów bezpieczeństwa nie mają one w swojej polityce proszenia klientów o zakładanie „zapasowych” rachunków, szczególnie zdalnie, przez telefon.

Istnieje także zestaw kilku podstawowych zasad, których warto przestrzegać na co dzień, by nie stać się ofiarą cyberprzestępców i zadbać o bezpieczeństwo swoich pieniędzy.

**10 zasad Intrum bezpiecznego korzystania z sieci, które powinien znać każdy internauta.**

1. **Nie otwieraj wiadomości e-mail i sms nieznanego pochodzenia oraz zawierających podejrzaną treść.** Zwróć szczególną uwagę na wiadomości nakazujące zapłatę zaległych (w tym przypadku fikcyjnych) faktur lub podanie dostępu do konta bankowego albo danych z karty płatniczej.
2. **Zadbaj o bezpieczeństwo haseł dostępu**. Hasła powinny składać się z różnych znaków (wielkie i małe litery, znaki specjalne i cyfry) oraz być odpowiednio długie (min. 8 znaków), wtedy będą trudniejsze do złamania. Co nie mniej ważne – nie posługuj się tym samym hasłem dostępu do wielu kont i pamiętaj,
aby zmieniać je co jakiś czas.
3. **Nigdy nie podawaj haseł i loginów osobom trzecim.**
4. **Sprawdzaj, czy bank lub sklep internetowy, z którego korzystasz, wykorzystuje szyfrowaną wersję protokołu http.** Innymi słowy, sprawdź, czy adres strony poprzedza fraza „https” (np. https://www.abc.pl). Jeżeli nie, to takie połączenie nie jest szyfrowane, co znacząco obniża poziom zaufania do takiej witryny
i warto rozważyć, czy istnieje potrzeba przekazywać tam swoje dane.
5. **Wybieraj tylko bezpieczne i sprawdzone sklepy internetowe,** czyli takie, o których wiadomo,
że przestrzegają zasad bezpieczeństwa i stosują odpowiednie zabezpieczenia, dzięki którym dane osobowe ich klientów nie staną się łatwym łupem dla oszustów.
6. **Wykonując przelew bankowy on-line, nigdy nie kopiuj numeru rachunku bankowego z zewnętrznych źródeł**, tylko za każdym razem wpisuj go ręcznie.
7. **Dokonuj płatności internetowych tylko przy udziale certyfikowanych pośredników.**
8. **Nie korzystaj z otwartych, niezabezpieczonych sieci Wi-Fi, czyli tzw. hotspotów, dostępnych
w miejscach publicznych**, takich jak restauracje, galerie handlowe czy lotniska, nawet jeżeli musisz skorzystać z aplikacji bankowej, aby wykonać szybki przelew. W celu zwiększenia ochrony naszych urządzeń, zasadne wydaje się rozważenie nabycia usługi VPN (z ang. Virtual Private Network), dzięki której przeglądanie Internetu, w tym także korzystanie z usług bankowych czy robienie zakupów, będzie odpowiednio zabezpieczone i niedostępne dla osób trzecich.
9. **Używaj sprawdzonych programów antywirusowych.** Dzięki temu dodatkowemu zabezpieczeniu możesz mieć pewność, że zarówno Twoje dane, które udostępniasz w Internecie, jak i informacje, które przechowujesz lokalnie na komputerze lub w smartfonie, będą bezpieczne. Korzystaj tylko
z oprogramowania pochodzącego z autoryzowanych, legalnych źródeł.
10. **Dokonuj regularnych aktualizacji oprogramowania na Twoim komputerze i smartfonie.**
1. Dane CERT Polska. Podmiot działający w strukturach NASK, jest jednym z trzech CSIRT-ów na poziomie krajowym,
który odpowiada za monitorowanie polskiej cyberprzestrzeni pod kątem cyberzagrożeń. [↑](#footnote-ref-1)
2. Metoda oszustów działających w sieci, która polega na tym, że cyberprzestępca podszywa się pod inną osobę lub instytucję
w celu wyłudzenia poufnych informacji (np. danych osobowych) lub wykonania określonych działań, by zdobyć te informacje. [↑](#footnote-ref-2)