UWAGA NA PHISHING!

Gdy ktoś podstępnie próbował uzyskać dostęp do środków zgromadzonych na twoim rachunku bankowym lub wyłudzić inne twoje dane, powiadom policję.
Wyłudzenie danych za pośrednictwem sieci internet stanowi przestępstwo

Kiedy dostaniesz maila z prośbą o weryfikację twoich danych bankowych, pilne uregulowanie rachunku telefonicznego lub należności za przesyłkę kurierską, z linkiem do dokonania płatności, nie reaguj na niego. To może być phishing!

Nie daj się złowić

Phishing (Password Harvesting Fishing) potocznie oznacza łowienie haseł i jest jedną z form oszustwa komputerowego. Polega na podszywaniu się pod inną osobę lub instytucję i wysyłaniu w jej imieniu fałszywych wiadomości elektronicznych. Wiadomości te zawierają zwykle link, który przekierowuje na stronę internetową łudząco przypominającą stronę twojego banku, sklepu internetowego, w którym często robisz zakupy, lub innego podmiotu, z którym wiążą cię jakieś relacje – zwykle finansowe. Link ma rzekomo ułatwić dokonanie płatności. W rzeczywistości chodzi natomiast o wyłudzenie poufnych informacji (na przykład danych logowania, danych karty kredytowej), za pomocą których oszust uzyskuje dostęp do twojego konta, następnie opróżniając je do zera.
Przyjmuje się, że określenie phishing pochodzi od nazwiska Briana Phishinga. To podobno pierwsza osoba stosująca techniki psychologiczne do wykradania numerów kart kredytowych. Podobno, bo niektórzy twierdzą, że to postać fikcyjna, stworzona przez spamerów w celu ich wzajemnego rozpoznawania się w sieci.
Według raportu CERT Polska, phishing zdecydowanie wyprzedza inne oszustwa komputerowe. Odsetek zgłoszonych w 2018 roku incydentów phishingowych stanowi około 44 procent spośród nich. Dlatego zawsze należy z dużą ostrożnością podchodzić do wszelkich wiadomości e-mail zawierających prośbę o płatność lub o podanie w celu weryfikacji danych, zwłaszcza danych związanych z dostępem do środków pieniężnych.

Zachowaj czujność

Pamiętaj! Żaden bank ani żadna inna instytucja nigdy nie powinny prosić cię o podanie twojego identyfikatora, hasła do rachunku bankowego lub numeru PIN, a już na pewno nie mailowo. Co zrobić, gdy mimo to do twojej skrzynki wpłynął e-mail z taką prośbą? Jeżeli masz wątpliwości, czy wiadomość pochodzi z legalnego źródła, w żadnym wypadku nie stosuj się do zawartych w niej instrukcji. W pierwszej kolejności skontaktuj się z podmiotem, od którego ma ona rzekomo pochodzić. Można to zrobić telefonicznie, dzwoniąc na infolinię, osobiście udać się do jego placówki lub przesłać mu podejrzanego maila z prośbą o weryfikację jego prawdziwości. Najszybsze efekty przynieść powinna rozmowa telefoniczna lub kontakt osobisty. Od razu uzyskasz konkretne informacje.
Banki, a także inne podmioty funkcjonujące na rynku (operatorzy sieci komórkowych, sklepy internetowe etc.), czuwają nad bezpieczeństwem swoich klientów. Dlatego, gdy otrzymują informację, że ktoś, podszywając się pod nie, próbuje wyłudzić dane, szybko reagują, powiadamiając o zaistniałym procederze policję. Często umieszczają również ostrzeżenia o próbach wyłudzenia danych na swoich stronach internetowych lub w komunikatach prasowych, a także organizują akcje mailingowe, w których ostrzegają przed oszustami. Warto je czytać.

Złóż zawiadomienie o przestępstwie

Gdy ktoś podstępnie próbował uzyskać dostęp do środków zgromadzonych na twoim rachunku bankowym, złóż zawiadomienie o popełnieniu przestępstwa. Wyłudzenie danych za pośrednictwem sieci internet stanowi przestępstwo z art. 287 Kodeksu karnego. Zgodnie ze wskazanym przepisem, kto, w celu osiągnięcia korzyści majątkowej lub wyrządzenia innej osobie szkody, bez upoważnienia, wpływa na automatyczne przetwarzanie, gromadzenie lub przekazywanie danych informatycznych lub zmienia, usuwa albo wprowadza nowy zapis danych informatycznych, podlega karze pozbawienia wolności od 3 miesięcy do lat 5. W wypadku mniejszej wagi, sprawca podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do roku.
Zawiadomienie można złożyć zarówno, gdy doszło do wyłudzenia danych, a więc gdy podałeś swoje dane oszustowi, jak również, gdy próbowano je wyłudzić. Karalne jest bowiem także usiłowanie popełnienia tego przestępstwa.
Zawiadomienie o popełnieniu przestępstwa można złożyć na piśmie lub ustnie do protokołu. W piśmie należy wskazać:
- **Dane organu**, do którego składasz zawiadomienie (jednostka policji lub prokuratury właściwa według miejsca popełnienia przestępstwa).
- **Swoje dane:** imię, nazwisko, adres korespondencyjny, numer telefonu.
- **Opis zdarzenia**, o którym zawiadamiasz, w tym kiedy i gdzie miało ono miejsce.
- **Wysokość szkody**, jeżeli wskutek opisanego w zawiadomieniu zdarzenia ją poniosłeś (zwykle będzie to kwota, jaka została przelana na rachunek bankowy wskazany przez oszusta lub jaką oszust sam bezprawnie pobrał z twojego konta).
- **Dane ewentualnych świadków**.
- **Dowody wskazujące na popełnienie przestępstwa** – koniecznie załącz e-mail, w którym próbowano od ciebie wyłudzić dane. Pamiętaj, żeby nie usuwać go ze swojej skrzynki.

W zawiadomieniu zazwyczaj podaje się również dane sprawcy, jeżeli jest on znany, lub jego cechy charakterystyczne. W przypadku przestępstw popełnianych w sieci, sprawca pozostaje jednak zwykle anonimowy. W takim przypadku organy ścigania podejmują próbę ustalenia jego tożsamości na podstawie numeru IP lub poprzez weryfikację informacji wynikających z wiadomości e-mail zawierającej prośbę o podanie danych. Gdy zawiadomienie wysyłasz pocztą, wyślij je listem poleconym, najlepiej za potwierdzeniem odbioru.
Jeśli chcesz złożyć zawiadomienie o przestępstwie w formie ustnej, musisz udać się do jednostki policji lub prokuratury. Zostaniesz wówczas poproszony o podanie informacji takich samych, jakie musiałbyś podać w zawiadomieniu pisemnym. Pamiętaj, żeby zabrać ze sobą wydrukowany e-mail, w którym próbowano wyłudzić od ciebie dane. Będzie on stanowił najważniejszy dowód w sprawie.

Co dalej?

Wskutek twojego zawiadomienia organy ścigania będą prowadziły postępowanie przygotowawcze między innymi w celu wykrycia i w razie potrzeby ujęcia sprawcy. Jeżeli sprawca nie zostanie ustalony, postępowanie zostanie umorzone – taką decyzję możesz zaskarżyć! Jeśli natomiast uda się ustalić jego tożsamość, sprawa trafi do sądu.
Pamiętaj, że w postępowaniu sądowym aż do zamknięcia przewodu sądowego możesz zgłosić wniosek o naprawie szkody, jaka została ci wyrządzona wskutek przestępstwa. W takim przypadku sąd ukarze sprawcę, zobowiązując go jednocześnie do pokrycia szkody. Jeżeli nie zgłosisz takiego wniosku w postępowaniu karnym albo sąd karny nie orzeknie co do całości żądanej przez ciebie kwoty, nic straconego. Możesz jeszcze wnieść pozew do sądu cywilnego.
Gdy sąd – karny lub cywilny – zasądzi na twoją rzecz żądaną kwotę odszkodowania, sprawca przestępstwa powinien ją niezwłocznie uregulować. Jeżeli nie zrobi tego dobrowolnie, w celu jej wyegzekwowania możesz skorzystać z pomocy komornika.

„Według raportu CERT Polska, phishing zdecydowanie wyprzedza inne oszustwa komputerowe. Odsetek zgłoszonych w 2018 roku incydentów phishingowych stanowi około 44% spośród nich. Dlatego zawsze należy z dużą ostrożnością podchodzić do wszelkich wiadomości e-mail zawierających prośbę o płatność lub o podanie w celu weryfikacji danych, zwłaszcza danych związanych z dostępem do środków pieniężnych".

Natalia Gaweł
Adwokat w Kancelarii Andersen Tax & Legal, autorka tekstu

RÓŻNE OBLICZA PHISHINGU

Phishing może występować w różnych odmianach:
- **Spear phishing** jest atakiem wymierzonym w konkretną osobę. Przed jego dokonaniem przestępca gromadzi szczegółowe informacje na temat ofiary, tworząc jej profil. Następnie wysyła do niej spersonalizowaną wiadomość, która jest często na tyle wiarygodna, że adresat się do niej stosuje.
- **Clone phishing** jest atakiem polegającym na stworzeniu wiadomości e-mail stanowiącej kopię (klon) innej, wcześniejszej wiadomości otrzymanej przez ofiarę. Wiadomość taka zawiera zazwyczaj załączniki lub linki. Otwierasz je, a oszust uzyskuje dostęp do twojego systemu.
- **Whaling** (wielorybnictwo) to proceder, którego celem są osoby zajmujące najwyższe stanowiska. Kierowana do nich wiadomość email zawiera zwykle wezwanie do podjęcia określonego działania, na przykład zainstalowania oprogramowania w celu otwarcia załączonego do niej dokumentu i często przypomina pismo z kancelarii prawnej lub urzędu. Instalujesz oprogramowanie, a oszust za jego pośrednictwem ma dostęp do wszystkiego, co masz w komputerze.
- **Pharming** polega na tym, że ofiara, wpisując w wyszukiwarkę prawidłowy adres WWW, na przykład swojego banku, zostaje przekierowana na fałszywą stronę internetową, do złudzenia przypominającą prawdziwą. Dzieje się tak po uprzednim zainstalowaniu na twoim komputerze wirusa. Gdy próbujesz zalogować się do swojego konta za pośrednictwem fałszywej strony, oszust pozyskuje twoje hasła oraz inne poufne dane.
- **Smishing**, czyli nakłanianie do podjęcia określonych działań za pośrednictwem wiadomości SMS, oraz **vishing**, czyli wyłudzanie danych za pomocą automatycznego systemu głosowego, który telefonicznie prosi nas o podanie danych poufnych.

NIE DAJ SIĘ OSZUSTOWI!

1. Zainstaluj na swoim komputerze oprogramowanie antywirusowe i antyspamowe.
2. Nigdy nie klikaj na podejrzane linki. Zamiast tego wpisz adres WWW ręcznie do wyszukiwarki.
3. Sprawdź, czy adres strony internetowej, na którą przekierował cię link, zawiera w pasku adresowym protokół https oznaczający połączenia szyfrowane zamiast protokołu http. Jedynie protokół https pozwala na bezpieczne przesyłanie danych.
4. Filtruj wiadomości – twoją czujność powinny wzbudzić e-maile zawierające błędy językowe.
5. Sprawdź nadawcę – skontaktuj się z podmiotem, od którego ma pochodzić wiadomość, i ustal, czy rzeczywiście ją do ciebie wysłał. Zanim nie potwierdzisz jego tożsamości, nie otwieraj przesłanych ci załączników.
6. W miarę możliwości zmieniaj dane logowania do stron, z których oszuści mogą wykraść twoje dane.

Fot. BrianAJackson /iStockphoto.com