Urząd Komunikacji Elektronicznej | UKE

Phishing – kradzież informacji

Redakcja:

Departament Polityki Konsumenckiej 2018

Urząd Komunikacji Elektronicznej (UKE)

Phishing to oszustwo, przez które całkiem nieświadomie możemy przekazać obcym swoje osobiste, istotne dane takie jak loginy, hasła czy numery kart kredytowych. Co więcej, będziemy przekonani, że informacji tych udzielamy instytucji, którą dobrze znamy - naszemu bankowi czy operatorowi.

Na czym polega przekręt?

Najczęściej wiadomości phishingowe to fałszywe powiadomienia z banków, komunikaty od dostawców systemów e-płatności, urzędów i innych organizacji. Czytając e-mail lub SMS, odbiorca zawsze jest zachęcany, aby pilnie wprowadził czy zaktualizował swoje poufne dane. W przeciwnym razie „grozi mu" utrata konta, pieniędzy, zablokowanie systemu itp. Wiadomości mogą też sugerować konieczność potwierdzenia danych w celu ochrony przed pishingiem. Aby uzupełnić wymagane informacje, wystarczy kliknąć w przesłany link, który przekieruje bezpośrednio w odpowiednie miejsce na stronę instytucji. Problem w tym, że strona łudząco przypomina oryginalną. Wszystko, co tam wpiszemy zostanie wysłane do twórcy, wraz
z loginem i hasłem do zaufanej, prawdziwej strony. Phisher uzyskując dostęp do konta, może wykorzystać go na różne sposoby, zależnie od typu konta.

Na co trzeba zwrócić uwagę?

Często wiadomości nie są skierowane do nas personalnie. Możemy spotkać się z formą bezosobową typu „Drogi użytkowniku" lub „Dear user". Nadawca z reguły nie wie do kogo pisze, więc wiadomość ma być jak najbardziej uniwersalna. Haker liczy, że odruchowo odbiorca kliknie w link, skoro przychodzi on od instytucji, którą zna.

Innym sposobem wyłudzenia jest informacja, że należy dopłacić 1 zł, gdyż przesyłka pod wskazany adres jest droższa. Oszuści chcą wykorzystać to, że coraz więcej konsumentów robi zakupy przez internet i korzysta z usług różnych doręczycieli. Osoba, która faktycznie czeka na przesyłkę być może nie zweryfikuje wiadomości, kliknie przesłany link i zaloguje się na konto bankowe. W tym czasie haker może zalogować się do prawdziwej domeny bankowej i zlecić przelew pieniędzy lub wykonać operacje, które doprowadzą do utraty środków. Często transakcję należy potwierdzić kodem SMS. Ofiara phishingu

skupia się na szeregu cyfr do przepisania i nie zawsze sprawdza, na jaką kwotę jest przelew.

Istotna jest także sama weryfikacja adresu strony, na którą odbiorca jest przekierowany. Zazwyczaj nieznacznie różni się ona od oryginału. Może się np. zdarzyć, że adres rozpoczyna się od numeru IP. Różnica może być także w samej nazwie adresu URL – z dodatkowymi znakami czy wyrazami (np. "www.logowanie-mojbank.pl" zamiast „www.mojbank.pl” lub „adresstrony.com” zamiast „adresstrony.pl”).

Smishing

Szczególnym rodzajem oszustwa jest smishing. Nazwa powstała z połączenia dwóch słów: SMS i phishing. Oznacza nic innego jak kradzież z wykorzystaniem spreparowanych wiadomości SMS. Użytkownik otrzymuje SMS w tonie, który ma go zaniepokoić i namówić do podjęcia natychmiastowego działania. Oszuści najczęściej korzystają z internetowych bramek umożliwiających spoofing SMS. Dzięki nim mogą tak skonfigurować wysyłaną wiadomość, żeby na ekranie naszego telefonu w polu nadawcy ukazał się wybrany przez nich tekst. W ten sposób podszywają się pod banki czy operatorów telekomunikacyjnych.
Z raportu opracowanego w 2018 roku przez Symantec wynika, że smishing może być znacznie groźniejszy niż phishing z wykorzystaniem e-maili. Jesteśmy bowiem bardziej świadomi zagrożeń wynikających z klikania w linki znajdujące się w mailach. W przypadku wiadomości SMS działamy szybciej i pochopniej, często nie zdając sobie sprawy z niebezpieczeństwa.

Najczęstszym scenariuszem jest próba podszycia się pod bank:

- Użytkownik dostaje wiadomość z informacją o rzekomej blokadzie karty płatniczej ze względów bezpieczeństwa. Aby ją odblokować, musi zadzwonić pod podany w wiadomości numer. Jeśli nawiąże połączenie, usłyszy nagraną wiadomość, po której będzie musiał podać dane karty, by ją odblokować.
- SMS może zawierać prośbę o zmianę danych logowania do bankowości internetowej. Swój dotychczasowy login i hasło – rzekomo w celu weryfikacji – trzeba będzie podać, dzwoniąc pod podany numer.

Oba przypadki kończą się przekazaniem oszustom swoich prywatnych danych, dzięki którym otrzymają bezpośredni dostęp do naszych pieniędzy.

Możemy także dostać SMS informujący, że kończy się darmowy okres jakiejś usługi (np. wideo na życzenie, serwisu streamingowego, portalu randkowego). Aby zrezygnować z dalszej – płatnej – subskrypcji, musimy kliknąć w link. Przenosi nas na stronę, gdzie rzekomo anulujemy usługę poprzez podanie danych karty płatniczej, której nie chcemy obciążać płatnościami. Pamiętajmy, że takie dane podaje się jedynie przy rejestracji, nigdy przy rezygnacji z usług.

Vishing

Vishing, czyli voice phishing, to kolejny rodzaj oszustwa. Cyberprzestępcy wyłudzają dane wykorzystując połączenia głosowe. Często są to nieświadomi zagrożenia rozmówcy.

Podobnie jak w smishingu chodzi o kradzież osobistych, bardzo istotnych informacji. Naciągacz podający się np. za pracownika banku poprosi o hasła dostępu, loginy czy numery kart kredowych bądź debetowych. Przykładowo przekonuje, że ktoś w danym momencie podjął próbę wypłaty czy transakcji internetowej za pośrednictwem naszej karty.

Częstym przykładem vishingu jest wyłudzenie kodu Blik. Po jego otrzymaniu oszust pobiera pieniądze z bankomatu.

Oszuści podszywają się nie tylko pod pracowników banków. W danej chwili mogą przedstawić się jako pracownik urzędu czy po prostu przedstawiciel handlowy.

Słysząc miły głos, informujący o blokadzie naszego konta trudno nam zweryfikować czy dzwoniąca osoba jest na pewno tą, za którą się podaje. Oszuści brzmią przekonująco, są przygotowani. Należy zachować rozsądek. Jeśli rozmówca budzi naszą wątpliwość, rozłączmy się. Zadzwońmy do danej placówki i potwierdźmy przekazane informacje.

Urząd Komunikacji Elektronicznej | UKE

Jak ustrzec się phishingu?

- Klikaj z głową, zachowaj czujność;
- Aktualizuj przeglądarkę, z której korzystasz do najnowszej oferowanej przez producenta wersji;
- Sprawdź czy znasz nadawcę, który wysyła wiadomość z linkiem, w który masz kliknąć;
- Podchodź z dystansem do otrzymywanych wiadomości, maili;
- Jeśli masz wątpliwości, co do wiarygodności osoby dzwoniącej nie podawaj żadnych poufnych informacji;
- Zweryfikuj u źródła (np. w placówce banku) czy wysłał do nas wiadomość z koniecznością aktualizacji danych.