

Phishing - widzisz, zgłaszaj

Oszuści łapią się różnych sposobów, by wyłudzić nasze dane i pieniądze. Podszywają się pod firmy kurierskie, energetyczne, portale ogłoszeniowe, a nawet Policję. Wysyłają maile i SMSy. Jeśli takie wiadomości dotrą także do Ciebie - reaguj.

Niemal 15 tysięcy adresów znalazło się do dziś na liście ostrzeżeń przed fałszywymi stronami, którą w marcu ubiegłego roku uruchomiliśmy wspólnie z NASK, UKE oraz we współpracy z operatorami telekomunikacyjnymi. Cel: ostrzegać użytkowników przed nadużyciami, w tym przed fałszywymi stronami internetowymi. Zgłaszać można też podejrzane SMSy.

Nie daj się podejść tzw. phishing.

Ta nazwa nie przez przypadek budzi dźwiękowe skojarzenia z fishingiem, czyli - po angielsku - łowieniem ryb. Przestępcy, podobnie jak wędkarze, stosują bowiem odpowiednio przygotowaną „przynętę”. - Phishing to jeden z najpopularniejszych typów ataków opartych o wiadomości e-mail lub SMS. Stosujący go cyberprzestępcy wykorzystują znaną technikę, która ma spowodować, że podejmiemy działania zgodne z ich zamierzeniami. To dlatego kuszą nas sensacyjnymi tytułami, rzekomymi niepowtarzalnymi ofertami, czy promocjami, które nigdy więcej się nie powtórzą. Straszą niezapłaconym mandatem czy rachunkiem. Są przy tym bezwzględni. Często podszywają się np. pod firmy kurierskie, urzędy, operatorów telekomunikacyjnych, czy nawet naszych znajomych. Coraz częściej wykorzystują do tego komunikatory i portale społecznościowe - mówi minister Marek Zagórski, pełnomocnik rządu ds. cyberbezpieczeństwa. Ostatnie miesiące to czas wzmożonej aktywności cyberprzestępców. Aby okraść wykorzystują m.in. nasz lęk, niepokój o bliskich i chęć zadbania o zdrowie. Dlatego tak ważne, aby zachować czujność i... działać! Jeśli widzisz podejrzaną stronę lub trafiła do Ciebie podejrzana wiadomość SMS - zgłoś to. Oto, jak to zrobić.

Zgłaszaj - dla siebie i innych

Zacznijmy od podejrzanych stron. To takie, które wyłudniają dane osobowe i dane uwierzytelniające. Linki do nich przesyłane są różnymi kanałami - SMSem, mailem lub przez media społecznościowe. Ich adresy mogą znajdować się w różnych domenach, nie tylko w domenie krajowej *.pl.

W przypadku takich stron kluczowe jest szybkie działanie - rozpoznawanie, raportowanie oraz współdzielenie informacji o złośliwych domenach. Wszystko po to, by jak najszybciej zablokować do nich dostęp. Pomaga w tym uruchomiona przez nas lista ostrzeżeń, która jest dostępna publicznie. Do dziś znalazło się na niej niemal 15 tysięcy adresów: https://www.cert.pl/posts/2020/03/ostrezenia_phishing/

Kto może zgłosić podejrzaną stronę? Każdy. Wystarczy wypełnić internetowy formularz: <https://incydent.cert.pl/domena#!/lang=pl>

- Na listę trafiają strony wyłudzające dane lub pieniądze. Każde zgłoszenie jest weryfikowane w CSIRT NASK. Kiedy podejrzenia okazują się prawdziwe - strona trafia na listę ostrzeżeń, użytkownicy są ostrzegani przed wejściem na taką stronę, a operatorzy mogą ograniczać jej obsługę. W niektórych wypadkach powiadamiane są też organy ścigania - prokuratura i policja - tłumaczy minister Marek Zagórski, pełnomocnik rządu ds. cyberbezpieczeństwa.

Zgłaszać można też podejrzane, zawierające linki, SMSy. Wystarczy przesłać je na numer 799 448 084, wykorzystując w swoim telefonie funkcję „przekaż” albo „udostępnij”.

Wiadomość trafi bezpośrednio do analityków CSIRT NASK, którzy zdecydują o dopisaniu podejrzanej domeny do listy ostrzeżeń. Z jednego numeru można zgłosić maksymalnie trzy wiadomości w ciągu czterech godzin.

WAŻNE! Numer służy wyłącznie do SMSowego zgłaszania prób wyłudzeń internetowych (phishingu, fałszywych aplikacji). Jeśli chcesz zadzwonić i zgłosić incydent - odpowiedni numer znajdziesz na stronie CSIRT NASK:

<https://www.cert.pl/kontakt/>

Włącz czujność

- Cyberprzestępcy nie ustają w wysiłkach, by stale tworzyć nowe metody oszukiwania nas, czy wyłudzenia naszych pieniędzy lub danych. Dlatego my także nieustannie musimy być czujni. Weryfikujmy informacje, nie działajmy w emocjach, a jeśli mamy pewność, że jesteśmy świadkami przestępstwa, zgłaszajmy to - radzi minister Marek Zagórski.

Oto kilka prostych sposobów, jak zadbać o swoje bezpieczeństwo w sieci i nie stać się ofiarą phishingu:

- Dokładnie sprawdzajcie wygląd i adres strony, na której podajecie dane logowania, dane osobowe czy karty płatniczej (na pierwszy rzut oka może nie różnić się od tego oficjalnego, ale wystarczy się przyjrzeć, by znaleźć np. drobną literówkę).
- Nie działajcie pod presją czasu, uważajcie na maile, SMS-y, strony internetowe, aplikacje i telefony, które skłaniają do natychmiastowego działania.
- Uważajcie na sensacyjne wiadomości, strony wymagające dodatkowego logowania, również te udostępniane z kont znajomych w mediach społecznościowych.
- Weryfikujcie źródła informacji zanim podejmiecie działania na ich podstawie lub je powielicie.
- Jeśli nie jesteście pewni, że dana informacja jest prawdziwa - skontaktujcie się z rzekomym nadawcą innym znanym kanałem i/lub poszukajcie potwierdzenia informacji w innych źródłach.
- Zgłaszajcie do CSIRT NASK każdą podejrzaną stronę, a także wiadomości e-mail i SMSy, które mogą wyłudzać dane.
- Formularz znajdziecie na stronie <https://incydent.cert.pl>

Jeśli chcecie poznać więcej wskazówek jak chronić się przed cyberatakami – koniecznie zajrzyjcie do naszego poradnika: <https://www.gov.pl/web/cyfryzacja/bezpieczni-w-mediach-spoecznościowych--praktyczne-wskazowki>

Informacja: Ministerstwo Cyfryzacji