Nie bądź ryba, nie daj się złowić

Polacy szturmują sklepy! Za 15 zł wynoszą koszyki pełne zakupów! Wiemy jak to robią! **Przyznajcie, że mielibyście ochotę kliknąć w taki link…? Wiedzą o tym cyberprzestępcy, którzy tylko na to czekają. Poznajcie phishing.**

Zanim jednak przejdziemy do wytłumaczenia Wam, czym jest phishing, najpierw wytłumaczymy o co chodziło ze szturmem na sklepy.

Rybobranie

Ten sensacyjny tytuł miał zachęcać nie tylko do kliknięcia. Dalej znajdowała się „oferta" bonów zniżkowych o wartości kilkuset złotych. Wszystko to było opatrzone nazwą i logo jednej z najpopularniejszych w Polsce sieci sklepów. Żeby było jasne – nie było żadnych bonów. Chodziło o to, by wyłudzić dane kart płatniczych, a dodatkowo zapisać tych, którzy dali się nabrać, na drogą subskrypcję.

Na szczęście domena, na której znajdowała się ta „oferta" jest już na liście ostrzeżeń. Nie zmienia to faktu, że w sieci takich wędek jest zdecydowanie więcej. Dlatego dobrze jest wiedzieć, jak nie dać się złowić.

Nazwa phishing 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 żebyśmy podjęli działania zgodne z ich zamierzeniami. To dlatego kuszą nas sensacyjnymi tytułami, rzekomymi niepowtarzalnymi ofertami, czy promocjami, które nigdy więcej się nie powtórzą* – tłumaczy minister cyfryzacji Marek Zagórski, pełnomocnik rządu ds. cyberbezpieczeństwa. - *Są bezwzględni. Często podszywają się np. pod firmy kurierskie, urzędy, operatorów telekomunikacyjnych, czy nawet naszych znajomych. Coraz częściej wykorzystują do tego komunikatory i portale społecznościowe – dodaje szef MC.*

A robią to wszystko po to, by wyłudzić nasze dane do logowania np. do kont bankowych lub używanych przez nas kont w mediach społecznościowych. Jak się nie dać?

Nie klikaj

Pierwsze i najważniejsze - NIE klikaj w podejrzane linki. Jeśli otrzymasz wiadomość e-mail lub SMS, a nie masz pewności, że ich nadawca jest prawdziwy - nie odpowiadaj i nie klikaj w umieszczone w wiadomościach linki. Żeby Cię podejść, w tego rodzaju wiadomościach przestępcy wykorzystują tzw. skrócone adresy stron internetowych. Bądź czujny, nie daj się nabrać.

Zwracaj uwagę na - wykorzystane w linku - nazwy stron internetowych. Twoją czujność powinny wzbudzić wszystkie literówki i przejęzyczenia. Czasem może chodzić o jedną przestawioną literę w adresie. Wiele wiadomości phishingowych ma niepoprawną gramatykę, interpunkcję, pisownię, czy też brak w nich polskich znaków np. „ą", „ę" itd. Dlatego zwracaj uwagę na pisownię!

Inne rady, które trzeba znać:

- Oceń, czy wygląd i ogólna jakość e-maila może pochodzić ze znanej Ci organizacji/firmy. Zwróć uwagę na np. użyte logotypy, stopki z danymi nadawcy itd.
- Sprawdź, czy e-mail na pewno jest adresowany do Ciebie (z imienia i nazwiska). Zdarza się tak, że podejrzane maila są adresowane do „cenionego klienta", „przyjaciela" lub „współpracownika". A to znak, że nadawca tak naprawdę Cię nie zna i że może to być część oszustwa.
- Bądź podejrzliwy w stosunku do zwrotów typu „wyślij dane w ciągu 24 godzin" lub „padłeś ofiarą przestępstwa, kliknij tutaj natychmiast". Właśnie takie sformułowania mają wymusić Twoją szybką reakcję. Przestępcy tylko na to czekają.

- Twój bank lub jakakolwiek inna instytucja nigdy nie powinny prosić Cię o podanie w wiadomości e-mail danych osobowych.
- Urzędy administracji publicznej w SMSach czy mailach nigdy nie proszą o dopłatę do szczepionki, czy uregulowanie należności podatkowych.
- Sprawdź wszelkie polecenia lub pytania zawarte w np. mailu. Jeśli mail rzekomo pochodzi z banku, zadzwoń do swojego banku i zapytaj, czy taki e-mail był do Ciebie wysłany.

Bez litości

Phishing to nie tylko maile i SMSy. Coraz częściej to także działania w mediach społecznościowych. Pewnie słyszeliście o osobach, którym włamano się na profil i później wysyłano z niego wiadomości do znajomych z np. prośbami o szybki przelew pieniędzy. Przestępcy w takich sytuacjach próbują nas podejść grając na naszych emocjach. Kto odmówi, jeśli pisze do niego siostra, brat lub najlepszy przyjaciel/przyjaciółka twierdząc, że następnego dnia zrobi przelew...? Jeśli otrzymacie taką wiadomość, zanim zrobicie przelew, zadzwońcie do osoby, od której rzekomo pochodzi ta wiadomość i upewnijcie się, że na pewno jest w potrzebie.

Kolejna ważna sprawa - zwracajcie uwagę na linki wymieniane między znajomymi w mediach społecznościowych. Kliknięcie w podejrzany link może grozić utratą kontroli nad swoim profilem w mediach społecznościowych.

- *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 cyfryzacji Marek Zagórski.

A gdzie i jak to zgłosić?

Wystarczy wejść na stronę https://incydent.cert.pl/phishing i wypełnić dostępny tam formularz. To tutaj możecie zgłosić stronę, która wyłudza dane osobowe, dane uwierzytelniające do kont bankowych lub serwisów społecznościowych.

Na liście ostrzeń jest już niemal 2,2 tysiąca stron!

Inne internetowe incydenty zgłaszajcie na https://incydent.cert.pl/.

O projekcie

Projekt **„Kampanie edukacyjno-informacyjne na rzecz upowszechniania korzyści z wykorzystywania technologii cyfrowych”** realizowany jest przez Ministerstwo Cyfryzacji we współpracy z Państwowym Instytutem Badawczym NASK. Kampanie mają na celu promowanie wykorzystywania technologii w codziennym życiu przez osoby w różnym wieku, przełamywanie barier z tym związanych oraz wzrost cyfrowych kompetencji społeczeństwa. Projekt obejmuje cztery obszary: jakość życia, e-usługi publiczne, bezpieczeństwo w sieci i programowanie.

za: www.gov.pl