Ile można stracić - czyli czym jest phishing? - Rok XVI nr 9 (188) Wrzesień 2022 r.

Coraz więcej osób pada ofiarą cyberprzestępców, a jedną z najbardziej popularnych metod oszustwa jest właśnie phishing, który polega na podszywaniu się pod osobę, instytucję lub firmę w celu:

- wyłudzenia cennych danych,
- nakłonienia do określonych działań, najczęściej transakcji płatniczych,
- zainfekowania urządzenia w celu uzyskania do niego nieautoryzowanego dostępu umożliwiającego pobranie danych.

Chociaż phishing uznawany jest za oszustwo internetowe, to przestępcy posługują się różnymi kanałami komunikacji: wiadomościami e-mail, smsami, poprzez komunikatory takie jak messanger czy whatsapp, wiadomościami prywatnymi wysyłanymi poprzez media społecznościowe (facebook, instagram), na platformach sprzedażowych (olx.pl, vinted.pl) czy nawet rozmowami telefonicznymi.

Informacje podawane nam przez przestępców wydają się bardzo autentyczne i prawdziwe, a treść łatwa do zaakceptowania. Jednak zawsze działanie odbywa się pod presją czasu („proszę się pośpieszyć, promocja się kończy") i naleganiem na podjęcie natychmiastowej decyzji. Jednak nie ma „super okazji" - zbyt niska cena może sugerować oszustwo.

Nierzadko informacje te napisane są niepoprawną polszczyzną, zawierają błędy językowe i literówki.

Niestety przestępcom często udaje się uzyskać potrzebne im dane, których nie powinno się udostępniać:

- loginy i hasła do systemów bankowych,
- numery kart płatniczych i kredytowych ,
- numery PESEL,
- seria i numer dowodów osobistych i dokumentów tożsamości,
- data i miejsce urodzenia,
- nazwisko panieńskie matki,
- dane logowania do poczty elektronicznej, mediów społecznościowych i innych serwisów internetowych.

Aby zabezpieczyć się przed phishingiem nie należy:

- Logować się z obcego komputera (ponieważ nie wiemy czy komputer jest dostatecznie chroniony).
- Podawać wielu informacji o sobie, rodzinie, bliskich, znajomych, miejscu pracy, itp.
- Klikać w podejrzane linki (np. wysyłane rzekomo z banku czy też przez operatorów telefonicznych lub dostawców prądu i gazu z prośbą o zalogowanie się przez kliknięcie w link podany w wiadomości, podanie hasła czy jego zmianę) - bank, operatorzy i dostawcy nigdy takich próśb i linków nie wysyłają.

Logując się do kont należy wybierać stronę z zakładek przeglądarki lub wpisywać adres w pasku adresu, nie należy klikać w linki z wiadomości.

• Logować się do bankowości internetowej na stronach, które nie są zabezpieczone symbolem KŁÓDKI:

Jeśli strona poprosi o podanie poufnych informacji, należy sprawdzić, czy jej adres URL zaczyna się od „HTTPS", a nie tylko „HTTP". „S" oznacza „bezpieczeństwo". Nie jest to gwarancja, że witryna jest zgodna z prawem, ale większość legalnych witryn korzysta z protokołu HTTPS, ponieważ jest on bardziej bezpieczny. Strony HTTP, nawet te legalne, są podatne na ataki hakerów.

Zawsze należy zachować ostrożność przy podawaniu danych w odpowiedzi na zapytania serwisów internetowych.

• Pomijać dodatkowych zabezpieczeń ze strony banku (np. kodu przesyłanego smsem) kiedy dokonujemy płatności.

• Podawać nikomu kodów PIN do kart płatniczych.

• Zamieszczać zdjęć, które mogą być podstawą szantażu lub mogą pomóc w uwiarygodnieniu podszywania się pod nas.

• Przelewać pieniędzy, jeżeli nie jesteśmy pewni sprzedawcy lub danego konta bankowego.

• Instalować na komputerze czy telefonie żadnych programów czy aplikacji nieznanego źródła.

• Logować się i podawać swojego hasła w miejscach korzystania z publicznego internetu (tzw. hot-spotach). Barbara Dobija-Herda / UG

Nie udostępniaj swoich danych Nie daj się złowić!

Jeśli podejrzewasz, że ktoś próbuje wyłudzić Twoje dane lub pieniądze, podszywa się pod Ciebie lub, że doszło już do przestępstwa, niezwłocznie skontaktuj się z najbliższym komisariatem lub posterunkiem policji!

Głos Gminy Wilkowice