Phishing jako najczęściej spotykana forma cyberataków

Phishing to termin pochodzący od angielskiego słowa fishing, które oznacza łowienie ryb. Analogicznie do łowienia, cyberprzestępcy stosują „przynętę", by nakłonić użytkowników do ujawnienia poufnych danych, takich jak kody PIN lub numery kart kredytowych. Phishing często przyjmuje formę wiadomości e-mail imitujących komunikaty od banków lub innych instytucji, z prośbą o potwierdzenie danych lub kliknięcie linka do fałszywej strony. Ofiarą phishingu mogą stać się także właściciele firm, którym przesyła się fałszywe wezwania do zapłaty za usługi lub zaległe faktury.

W 2023 roku podobnie jak w latach poprzednich, phishing był najczęstszym typem cyberataków. Zarejestrowano 41 423 takie przypadki, co stanowiło ponad połowę wszystkich incydentów obsłużonych przez CERT Polska. To wzrost o 61% w porównaniu do roku 2022. Najczęściej wykorzystywano wizerunek serwisów takich jak Allegro (11 161 przypadków), Facebook (5 308) oraz OLX (4 753).

Jak chronić się przed oszustem?

Naszą czujność powinny wzbudzać wszelkie wiadomości, które wywierają presję czasu, proszą o pilne działania lub zawierają błędy językowe. Ważne jest sprawdzenie samego adresu URL oraz adresu nadawcy e-maila. W większości przypadków są one źle napisane lub wykorzystują rozszerzenia charakterystyczne dla darmowych domen z egzotycznych krajów. Nie należy klikać w podejrzane załączniki, szczególnie te, które pochodzą od nieznanego odbiorcy albo informują o atrakcyjnej wygranej w konkursie, w którym nigdy nie braliśmy udziału. Niebezpieczne załączniki często przypominają dokumenty PDF, Microsoft Word lub Excel. Podejrzenia powinny wzbudzać w szczególności ich rozszerzenia, takie jak .exe, js, .iso, .img, .htm, .html. Pamiętajmy również, że przedstawiciele banku nigdy nie poproszą o podanie kodu PIN do karty ani na stronie internetowej, ani podczas rozmowy telefonicznej.

W przypadku podejrzenia, że padło się ofiarą phishingu (uruchomiło się podejrzany załącznik lub odwiedziło fałszywą stronę), należy natychmiast zmienić hasła do swoich kont. W sytuacji podania danych finansowych należy skontaktować się ze swoim bankiem. Konieczne jest również zgłoszenie incydentu – w Polsce istnieje kilka instytucji zajmujących się oszustwami internetowymi.

Oprócz policji można skontaktować się z CERT Polska (poprzez https://incydent.cert.pl/ lub w aplikacji mObywatel – usługa Bezpiecznie w sieci – podejrzane wiadomości SMS z linkami można zgłosić na nr 8080). Należy również przeskanować urządzenia programem antywirusowym, ponieważ kliknięcie podejrzanego linka mogło spowodować pobranie złośliwego oprogramowania.

Zaleca się także uruchomienie uwierzytelnienia dwuskładnikowego (np. w postaci kluczy sprzętowych) we wszystkich serwisach internetowych, które oferują takie rozwiązanie.

Nowe funkcje w aplikacji mObywatel 2.0

Ministerstwo Cyfryzacji, wychodząc naprzeciw potrzebom użytkowników, wprowadziło w aplikacji mObywatel 2.0 nową funkcję zgłaszania incydentów cyberbezpieczeństwa. Umożliwia ona raportowanie podejrzanych stron internetowych, e-maili czy SMS-ów. Zgłoszenia trafiają bezpośrednio do ekspertów z CERT Polska, którzy zajmują się analizą i eliminacją zagrożeń.