Wiadomości

2021-09-13

Kosztowne wiadomości

Rekordowa wygrana w loterii jest Twoja? A może – daleki krewny właśnie przepisał Ci swój liczony w milionach majątek? Nie daj się nabrać. Każda podejrzana wiadomość, którą dostajesz - to może być phishing.

Zaintrygowanie, krótki impuls, który podpowiada, żeby sprawdzić o co chodzi, kliknięcie w link… tyle wystarczy, żeby stać się ofiarą phishingu. Cyberprzestępcy to wiedzą – i korzystają. Jak się nie dać?

Różne sposoby

Zacznijmy od krótkiego wyjaśnienia, czym jest phishing. To jeden z najpopularniejszych typów ataków opartych o wiadomości e-mail lub SMS, a coraz częściej także – te przesyłane w mediach społecznościowych. Ta metoda ma sprawić, żebyśmy podjęli działania zgodne z zamierzeniami cyberprzestępców, mówiąc inaczej – złapali się na rzuconą przynętę (stąd skojarzenie ze słowem fishing – ang. łowienie ryb).

To dlatego kusi rzekomymi niepowtarzalnymi ofertami, sensacyjnymi nagłówkami, dosłownym lub przysłowiowym „zwycięskim losem” - wywołuje poczucie, że jesteśmy szczęśliwcami. W rzeczywistości jest zupełnie odwrotnie.

Jaki jest cel phishingu? To np. wyłudzenie naszych danych do logowania do kont bankowych lub w mediach społecznościowych. Jak możecie się domyślać – stąd już tylko krok do poważnych problemów. Wykorzystując nasze dane cyberprzestępcy mogą przejąć pieniądze z naszych kont bankowych, czy też zaciągnąć pożyczkę podszywając się pod nas. Mogą też wykorzystać nasze konta w mediach społecznościowych do złapania kolejnych ofiar. Dlatego – nie dajcie się „złowić”.

Na chłodno

Najważniejsza zasada – nigdy nie klikaj w podejrzane linki lub takie, które pochodzą od nieznanych nadawców. Zwracaj uwagę na nazwy stron internetowych, a także na treść wiadomości.

Cyberprzestępcy dbają o jak największą wiarygodność, ale zdarzają im się błędy i przejęzyczenia. Czasem może chodzić o literówkę, czy jedną przestawioną literę, innym razem o niepoprawną gramatykę, interpunkcję, pisownię, czy też brak polskich znaków np. „ą”, „ę” itd. Na co jeszcze warto zwrócić uwagę?

Oto kilka wskazówek:

- Sprawdź, czy e-mail na pewno jest adresowany do Ciebie (z imienia i nazwiska). Jeśli występujesz w roli np. „przyjaciela”, czy „zwycięzcy” – to podejrzane.
- Zweryfikuj oznakowania i ogólny wygląd wiadomości. Jeśli np. mail pochodzi z banku, powinny być w nim odpowiednie logotypy, stopki, itp. Masz wątpliwości? Zadzwoń do danej instytucji i zapytaj, czy jesteś adresatem takiej wiadomości.
- Dokładnie zweryfikuj adres, z którego przysłana została wiadomość. Często będzie się on zbliżony do prawdziwego adresu, ale szczegóły będą się różniły, np. znajdziesz w nim dodatkową cyfrę lub literę.
- Bądź podejrzliwy w stosunku do zwrotów: „kliknij natychmiast”, „odpowiedz w ciągu 24h” – i innych, które mają wymusić szybką reakcję.

Pamiętaj też, że banki i inne instytucje nigdy nie proszą o podanie hasła lub innych wrażliwych danych za pośrednictwem maila czy sms-a. W przypadku, gdy wiadomość zawiera prośby o takie informacje, najprawdopodobniej jest ona phishingiem. W każdej sytuacji zachowaj czujność – to Twoja przewaga.

Działaj - zgłoś

- Cyberprzestępcy stale tworzą nowe metody wyłudzania danych lub pieniędzy. Dlatego – postępujmy

ostrożnie, weryfikujmy informacje, zastanówmy się kilka razy, zanim uznamy, że dana wiadomość nie budzi naszych zastrzeżeń. A jeśli mamy pewność, że jesteśmy świadkami przestępstwa, zgłaszajmy to – mówi minister Janusz Cieszyński, pełnomocnik rządu ds. cyberbezpieczeństwa.

A gdzie i jak można to zgłosić?

Wystarczy wejść na stronę https://incydent.cert.pl/ i wypełnić dostępny tam formularz. Tu możecie zgłosić stronę, która wyłudza dane osobowe, dane uwierzytelniające do kont bankowych lub serwisów społecznościowych. Warto to robić!

Źródło: Cyfryzacja KPRM

Źródło: https://paliwa.pl/strona-startowa/archiwum/kosztowne-wiadomosci