Internauto – uważaj na podejrzane maile!

Otrzymałeś maila rzekomo od Poczty Polskiej z żądaniem odebrania paczki pod rygorem zapłaty kary finansowej oraz wskazówką, że więcej szczegółów znajduje się w linku lub załączniku? Uważaj – tego maila nie wysłał żaden pracownik poczty. Internauto, właśnie padłeś ofiarą próby cyberataku.

W dzisiejszym mobilnym świecie e-mail to podstawowe narzędzie komunikacyjne. Znaczenie poczty elektronicznej docenili także cyberprzestępcy, którzy za pomocą e-maili próbują wykraść poufne dane. Cyberatak to tak groźne i częste zjawisko, że doczekało się własnej terminologii – to tzw. phishing.

Mechanizm jest prosty: atak rozpoczyna się w momencie odebrania wiadomości e-mail, która wydaje się być od osoby lub instytucji, której ufamy np. banku, operatora telefonii komórkowej czy ulubionego sklepu internetowego. Treść takiej wiadomości zazwyczaj zachęca użytkownika do podjęcia jakiegoś działania np. kliknięcia w link, otwarcia załącznika albo wysłania odpowiedzi na wiadomość. Co się stanie, gdy nieroztropny internauta wykona polecenie? To zależy od celu ataku, ale generalnie – nic dobrego. Ataki typu phishing mają za zadanie:

- wyłudzenie informacji: zamiarem atakującego jest zmanipulowanie internauty tak, aby kliknął na link, który zabierze go na stronę pytającą o login i hasło. Takie witryny bliźniaczo przypominają znane strony banku, jednak są zaprojektowane tylko po to, żeby wykraść dane potrzebne do uzyskania dostępu do konta bankowego. Nieroztropny użytkownik traci wówczas kontrolę nad swoim kontem oraz pieniędzmi.

- przejęcie kontroli nad komputerem poprzez złośliwy link lub załącznik – w tym przypadku, po otwarciu linku/załącznika cyberprzestępca zyskuje dostęp do naszego komputera.

Phishing to bardzo groźne zjawisko. Możemy się przed nim bronić – kiedy po przeczytaniu wiadomości podejrzewasz, że jest to phishing, po prostu skasuj tę wiadomość. **PAMIĘTAJ, by pod żadnym pozorem nie otwierać linków lub załączników!** Ponadto cyberprzestępcy popełniają błędy, które powstają najczęściej przy tworzeniu fałszywych stron banków czy innych instytucji. Oto garść wskazówek, która uchroni Cię przed atakiem:

Po pierwsze: Działaj roztropnie!

Bądź podejrzliwy, jeśli jakikolwiek e-mail wymaga natychmiastowego działania lub potęguje wrażenie pilności. Akurat w tym przypadku pośpiech jest bardzo złym doradcą. Na chłodno przeanalizuj treść maila: jeśli zwarty we wiadomości link wydaje się podejrzany, najedź na niego myszką (nie klikając). Wówczas ukaże się prawdziwy adres strony – a ta często jest zupełnie inna, niż sugeruje link lub też zawiera błędy w nazwie np. www.ipko.com. Ponadto zwróć uwagę na adres nadawcy – przestępcy podszywają się pod pracownika danej firmy, jednak maile często zawierają błędy w nazwie. Nierzadko jednak zdarzają się sytuacje, gdy atakujący nawet nie silą się na zachowanie pozorów – tak więc gdy dostaniesz informację rzekomo z banku, a adres nadawcy złożony jest ze zbioru znaków – od razu kasuj maila!

Po drugie: czytaj uważnie!

Należy zwiększyć czujność, jeśli w mailu znajdują się błędy gramatyczne lub w pisowni. Większość firm bardzo dokładnie formułuje swoje wiadomości, a przestępcy często korzystają z niedokładnych, automatycznych translatorów, stąd maile z lapsusami językowymi.

Po trzecie: orientuj się w prawie!

Wiadomości phishingowe z reguły informują odbiorców o zmianie infrastruktury lub polityki bezpieczeństwa przez bank, w związku z czym wszyscy klienci są proszeni o powtórne potwierdzenie podanych przez siebie informacji. Jednak po kliknięciu zawartego w mailu linku zostają przekierowani na fałszywą stronę, na której są nakłaniani do ujawnienia poufnych danych. PAMIĘTAJ! Banki nigdy nie żądają podawania jakichkolwiek danych mailowo. Jeżeli masz wątpliwości, zadzwoń i sprawdź!

Nie wypełniaj mailowych formularzy, w których należy podać informacje osobiste. Wprowadzaj takie dane tylko za pośrednictwem bezpiecznej strony internetowej. Sprawdź, czy adres URL zaczyna się od „https://”, a nie

„http://”. Poszukaj symbolu kłódki w prawym dolnym rogu przeglądarki i kliknij go dwukrotnie, aby sprawdzić ważność certyfikatu cyfrowego lub skontaktuj się z bankiem telefonicznie.

Po czwarte: zadbaj o swoje bezpieczeństwo!

By uchronić się przed cyberatakami, używaj najnowszej wersji przeglądarki internetowej i stosuj wszystkie łaty bezpieczeństwa. Porządne oprogramowanie antywirusowe jest wręcz wskazane.

Pamiętajmy, że phisherzy ciągle udoskonalają sposoby wyłudzania danych. Internauta nie jest jednak bezbronny – wiedza i zdrowy rozsądek uchronią nas przed atakiem.

Katarzyna Nikołajuk

źródło: Biuletyn Bezpieczeństwa komputerowego OUCH!, grudzień 2011

phishing.jpg

Image not found or type unknown