Smishing - jak się chronić przed fałszywymi SMSami?

Każdego dnia dostajemy różnego rodzaju wiadomości SMS, nie tylko od osób, które mamy zapisane w kontaktach, ale także z innych źródeł. Bardzo często są to powiadomienia o promocjach, dostawie zamówionych produktów, informacje z banku lub od firm, z których usług korzystamy (np. dostawca energii, operator sieci komórkowej).

Niestety może też się zdarzyć, że otrzymamy wiadomość od osoby podszywającej się pod przedstawiciela znanej instytucji lub znajomego. Jeśli potraktujemy ją poważnie, może to doprowadzić do utraty naszych pieniędzy.
Najpopularniejszym rodzajem oszustwa stosowanego przez cyberprzestępców jest phishing, czyli próba wykradzenia danych. Warto wiedzieć, że ma on swoje „odmiany", w zależności od tego, jakie działania podejmują oszuści. Jedną z nich jest wysyłanie fałszywych wiadomości tekstowych na telefon ofiary. Każdy użytkownik telefonu komórkowego jest narażony na takie wiadomości. Jest to tzw. smishing. Nazwa smishing pochodzi od skrótu SMS, czyli krótkich wiadomości tekstowych, i słowa phishing. Większość z nas korzysta z SMS-ów niemalże codziennie w kontaktach z rodziną czy znajomymi. Przed erą komunikatorów typu Messenger lub WhatsApp był to najpopularniejszy sposób przesyłania np. życzeń świątecznych.

Najpopularniejsze tematy fałszywych wiadomości to:
- nieopłacony rachunek czy faktura np. za prąd;
- dopłata do przesyłki
- problemy z rachunkiem bankowym (zablokowane konto, informacja o złożeniu wniosku na pożyczkę);
- wygrane w loteriach, informacje o oczekującej nagrodzie.

Co powinno wzbudzić naszą czujność?
- Ton wiadomości wywołujący silne emocje (np. strach), a także ponaglanie (np. poprzez odłączenie usługi czy zablokowanie środków na naszym koncie);
- wszelkiego rodzaju prośby o poufne dane (np. data urodzenia, numer PESEL) oraz dane do logowania;
- linki i załączniki, które mogą przekierować na fałszywą stronę np. płatności;
- nakłanianie do pobrania dodatkowej aplikacji lub programu;
- nagła wygrana, zadziwiająco atrakcyjna promocja.

Jak się chronić przed fałszywymi wiadomościami?
- Nie działaj pochopnie i nie podejmuj decyzji pod wpływem emocji i presji czasu;
- zweryfikuj nadawców, zadzwoń pod numer instytucji, od której rzekomo dostaliśmy wiadomość bądź odwiedźmy jej oddział;
- nie klikaj w linki i załączniki, które otrzymasz w wiadomości;
- nie udostępniaj danych osobowych nieznanym nadawcom;

- stosuj silne hasła oraz weryfikację dwuetapową; jeśli nie wiesz, jak to zrobić, poproś o pomoc kogoś bliskiego;
- zwracaj uwagę na komunikaty i ostrzeżenia, które otrzymujesz od banku;
- jeśli otrzymasz podejrzaną wiadomość, zgłoś ją do zespołu CERT Polska. Poproś zaufaną osobę, aby pomogła Ci wypełnić formularz i przesłać zgłoszenie. Podejrzane wiadomości SMS możesz bezpośrednio przekazać na bezpłatny numer 8080.

Podcast „3 grosze o ekonomii"

Internetowe love. Jak zadbać o swoje cyberbezpieczeństwo w relacjach online? Link do audycji: 3 grosze o ekonomii – Internetowe love. Jak zadbać o swoje cyberbezpieczeństwo w relacjach online (google.com)

***

Materiał przygotowany w ramach kampanii pt. *#Halo! Tu cyberbezpieczny Senior*! przygotowanej przez NASK, Centralne Biuro Zwalczania Cyberprzestępczości w Policji oraz Warszawski Instytut Bankowości.

***