OSTRZEŻENIE W SPRAWIE OSZUKAŃCZYCH LINKÓW W WIADOMOŚCIACH SMS

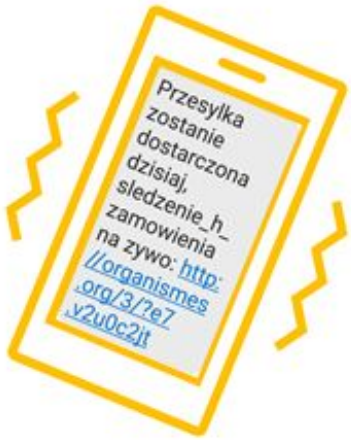
Data publikacji 22.12.2021

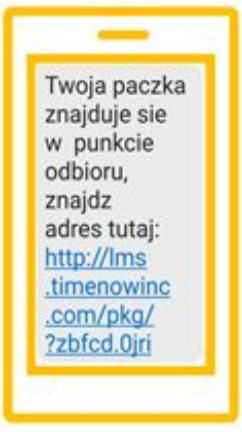
Komenda Główna Policji i FinCERT.pl – Bankowe Centrum Cyberbezpieczeństwa ZBP ostrzegają klientów banków przed oszukańczymi linkami w wiadomościach SMS. Oszuści stosując socjotechnikę i licząc na naszą nieuwagę podsyłają do nas między innymi wiadomości SMS rzekomo zawierające informację o przesyłce kurierskiej.

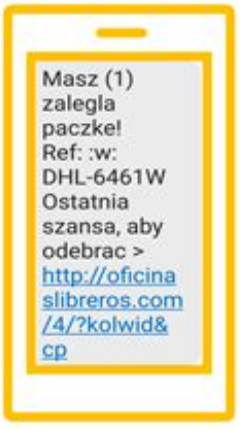
Okres pandemii związanej z koronawirusem COVID-19 oraz przedświąteczny szał zakupowy spowodowały, że nasza aktywność przeniosła się do e-commerce i platform aukcyjnych i ogłoszeniowych w Internecie. Jest to także okres bardzo dużej aktywności oszustów, którzy stosując socjotechnikę i licząc na naszą nieuwagę podsyłają do nas między innymi wiadomości SMS rzekomo zawierające informację o przesyłce kurierskiej.

FinCERT.pl – Bankowe Centrum Cyberbezpieczeństwa Związku Banków Polskich obserwuje w ostatnim okresie zwiększoną ilość przestępczych kampanii SMS, w których oszuści podszywają się np. pod legalnie działające FIRMY KURIERSKIE. W treści przesłanych SMS przestępcy zamieszczają AKTYWNY LINK oraz informują np. o statusie przesyłki: **przesyłka zostanie dostarczona dzisiaj, podjęliśmy próbę dostarczenia Twojej paczki, Twoja paczka znajduje się w punkcie odbioru, czy ostatnia szansa, aby odebrać przesyłkę.**

Przykładowe komunikaty oszukańczych SMS – źródło własne: FinCERT.pl – BCC ZBP:







Kliknięcie w aktywny link w takiej wiadomości może skutkować między innymi:

- ujawnieniem danych poufnych służących do logowania do bankowości internetowej lub mobilnej lub wykonaniem płatności oszukańczej;
- uruchomieniem szkodliwego oprogramowania, które np. pozwoli przejąć kontrolę nad urządzeniem lub zbierze i przekaże przestępcom nasze dane wrażliwe;
- zaszyfrowaniem urządzenia.

W związku z tego typu zagrożeniem FinCERT.pl - Bankowe Centrum Cyberbezpieczeństwa ZBP oraz Komenda Główna Policji rekomendują:

- nieklikanie w podejrzane linki;
- przeanalizowanie adresu zawartego w linku pod kątem firmy kurierskiej, która nas obsługuje;
- śledzenie zamówionego towaru tylko przy użyciu oficjalnej strony internetowej firmy kurierskiej lub jej aplikacji mobilnej pobranej ze strony internetowej tego dostawcy;
- zgłoszenie podejrzanej wiadomości zawierającej aktywne linki do CSIRT NASK pod numer 799-448-084, wystarczy użyć w telefonie funkcję „przekaż" albo „udostępnij" i wiadomość odesłać pod ww. numer;
- usunięcie takiej wiadomości (aby w przyszłości uniknąć przypadkowego kliknięcia na niebezpieczny link).

Więcej można przeczytać na stronie internetowej NASK - państwowego instytutu badawczego nadzorowanego przez Kancelarię Prezesa Rady Ministrów: Teraz jeszcze łatwiej zgłosić incydent bezpieczeństwa - przez SMS

(Komenda Główna Policji, FinCERT.pl - Bankowe Centrum Cyberbezpieczeństwa ZBP - Centrum Wymiany i Analiz Informacji Sektora Finansowego / mw)