

Wiadomości

2022-05-25

Najpopularniejsze oszustwa internetowe w sieci



Czy otrzymałeś kiedyś mail o rzekomym spadku, który czeka na Ciebie gdzieś za granicą? A może jakiś bogaty więzień polityczny obiecał Ci majątek? W obu przypadkach wystarczy tylko, żebyś uścił drobną – w porównaniu do oczekiwanego zysku – kwotę na cele operacyjne, opłatę administracyjną itp. Są to przykłady tzw. „nigeryjskiego przekrętu”, oszustwa znanego od stuleci, wcześniej stosowanego listownie, obecnie za pośrednictwem internetu. Przymiotnik „nigeryjski” odnosi się do innej znanej nazwy tego procederu, czyli oszustwa 419, gdzie 419 to numer paragrafu z nigeryjskiego kodeksu karnego opisującego oszustwo.

Jak wygląda takie oszustwo?

Zaczyna się od kontaktu email, czasem również w komunikatorze internetowym. Nieznajoma osoba obiecuje znaczny zysk i wynagrodzenie, w zamian za niewielki wkład finansowy. Często wykorzystywany jest również motyw spadku czy darowizny, które rzekomo otrzymaliśmy od dalekiej rodziny lub całkiem obcej nam osoby, ale żeby je fizycznie uzyskać, należy dokonać kilku wpłat.

Wiadomość przeważnie jest pisana po angielsku lub w łamanej, niepoprawnej polszczyźnie (przetłumaczone w translatorze), ale może zawierać uwiarygadniające załączniki – skany dokumentu tożsamości, postanowienia sądu, zagraniczne certyfikaty, których autentyczności nie jesteś w stanie potwierdzić. W bardziej wyrafinowanej formie, cyberprzestępcy wykorzystują już jakąś wiedzę na temat ofiary – podobne nazwisko czy powołanie się na wspólnych znajomych lub członków rodziny.

Autor wiadomości oczekuje wpłaty zadatku w obcej walucie (przeważnie dolary lub funty brytyjskie). Jeżeli ofiara złapie haczyk i podejmie korespondencję z oszustem, dosyłane są dodatkowe informacje. Pewną odmianą tego przestępstwa są tzw. oszustwa „na zaliczkę” na różnych portalach aukcyjnych czy sprzedażowych, gdzie oszuści wyszukują wystawione wartościowe przedmioty, proszę sprzedawcę o

szybką wysyłkę i proponują dokończenie transakcji poza portalem zakupowym. Następnie przesyłają fałszywe potwierdzenie dokonania wpłaty, sprzedawca wysyła towar, a środki nigdy nie trafiają na jego konto.

Takie oszustwa mają często charakter międzynarodowy, a przestępcy je wykorzystujący stosują techniki utrudniające ich identyfikację. Wykrywalność sprawców jest wobec tego niska. Jeżeli prześlesz pieniądze, i nie otrzymasz obiecanej nagrody – raczej nigdy nie odzyskasz swojego „wkładu”.

Jak ochronić się przed takim oszustwem?

Przede wszystkim, należy zachować zdrowy rozsądek. Prawdopodobieństwo takiego uśmiechu losu jest bardzo niewielkie. Nie pozwól na to, aby emocje i chęć łatwego zysku przesłoniły logiczne myślenie. Zachowaj spokój i podejdz do opisywanych historii z dystansem, kierując się zasadą ograniczonego zaufania.

Pamiętaj!

- Nie odpisuj na podejrzone wiadomości i zaznaczaj je jako spam.
- Nie przysyłaj danych osobowych, numerów kont bankowych, informacji dotyczących polis ubezpieczeniowych itp.
- Podchodź z dystansem do historii opisywanych w mediach społecznościowych, portalach internetowych.

Źródło: Cyfryzacja KPRM

Źródło: <https://paliwa.pl/strona-startowa/archiwum/najpopularniejsze-oszustwa-internetowe-w-sieci>