KOMENDA STOŁECZNA POLICJI

https://ksp.policja.gov.pl/pl/dzialania/aktualnosci/58175,Oszustwo-internetowe-czytaj-nie-klikaj.html
2022-08-20, 08:28

OSZUSTWO INTERNETOWE - CZYTAJ, NIE KLIKAJ

Data publikacji 03.12.2021

Okres przedświąteczny właśnie się rozpoczął. Pochłonięci gorączką świątecznych zakupów i przygotowań często zapominamy o własnym bezpieczeństwie. Przez pośpiech i roztargnienie tracimy czujność, a to w rezultacie może doprowadzić do wielu przykrych zdarzeń. Biorąc pod uwagę fakt, że okres przedświąteczny to także czas wytężonej pracy oszustów - stołeczni policjanci apelują o ostrożność przy internetowych transakcjach i „klikaniu" bez weryfikacji wiadomości.

Dostałeś sms, w którym zakład energetyczny lub firma kurierska prosi Cię o dopłacenie niewielkiej kwoty, a dalej przesyła link do wykonania przelewu? Uważaj, to oszustwo!

Oszuści nieustannie doskonalą swoje metody działania i korzystają z każdej nadarzającej się okazji, aby wprowadzić nas w błąd, wykorzystać nasze zaufanie i okraść z pieniędzy. Okres przedświąteczny to czas wzmożonych zakupów, także tych internetowych, to też doskonała okazja dla oszustów próbujących wykraść nasze hasła, dane i pieniądze.

W tej opcji oszuści podszywają się pod firmy kurierskie i za pomocą SMS-a informują o konieczności dopłaty do przesyłki. Zazwyczaj kwota, jaką należy wpłacić, jest bardzo niska i nie wzbudza naszego podejrzenia. W wiadomości podany jest także link, który przekierowuje potencjalną ofiarę na stronę łudząco podobną do strony banku, gdzie osoba wprowadza wrażliwe dane dotyczące konta, takie jak login czy hasło i umożliwia tym samym przechwycenie tych danych i przejęcie kontroli przez oszustów nad konkretnym kontem bankowym.

Innym wariantem, z którego chętnie korzystają oszuści jest SMS z prośbą o dopłatę do rachunku za prąd. Przestępcy podszywają się pod zakład energetyczny i poprzez wiadomość SMS, informują, że trzeba będzie dopłacić niewielką kwotę, by uregulować zaległości, co wstrzyma wydaną dyspozycję odcięcia dopływu energii elektrycznej do twojego domu. W SMS-ie zamieszczają link przekierowujący do bankowości elektronicznej. W momencie, kiedy w niego klikniemy pozwalamy dysponować swoim kontem.

Wystawiłeś przedmiot na sprzedaż? Uważaj, możesz paść ofiarą oszustwa.

Przestępcy wyszukują oferty sprzedaży, a potem kontaktują się ze sprzedawcą przez SMS lub jeden z komunikatorów jakie użytkujemy i od razu deklarują, że są zainteresowani zakupem. Sprzedawca otrzymuje wiadomość od osoby potencjalnie zainteresowanej kupnem, która proponuje zapłatę poprzez specjalny link wysłany do sprzedawcy. Żeby sfinalizować transakcję wymaga podania danych z karty płatniczej tj. numeru, daty ważności, kodu CVV/CVC, często też hasła jednorazowego, który przychodzi SMS-em na telefon zaraz po podaniu danych karty. Gdy ofiara wpisze takie dane, zamiast otrzymać zapłatę za towar, z jej konta znikną wszystkie oszczędności.

Stołeczni policjanci ostrzegają! Aby uniknąć problemów należy dokładnie i uważnie czytać otrzymywane wiadomości, a przede wszystkim nie „klikać" w podejrzane linki, szczególnie jeśli prowadzą do systemów elektronicznych płatności. Poświęcenie kilku sekund na zweryfikowanie, jaką transakcję mamy zaakceptować, może uratować nas przed utratą

pieniędzy, danych osobowych, a także zawartego na nasze konto kredytu.

Tekst: podkom. Marta Gierlicka

Film: sierż. szt. Rafał Markiewicz, mł. asp. Rafał Rutkowski

Film Czytaj, nie klikaj

Opis filmu: Czytaj, nie klikaj

Aby obejrzeć film włącz obsługę JavaScript w swojej przelądarce.

Pobierz plik Czytaj, nie klikaj (format mp4 - rozmiar 11.75 MB)

Film paczka.mp4

Aby obejrzeć film włącz obsługę JavaScript w swojej przelądarce.

Pobierz plik paczka.mp4 (format mp4 - rozmiar 32.41 MB)

Film Czytaj_nie_klikaj_sms.mp4

Aby obejrzeć film włącz obsługę JavaScript w swojej przelądarce.

Pobierz plik Czytaj_nie_klikaj_sms.mp4 (format mp4 - rozmiar 8.92 MB)