INTERPOL OSTRZEGA PRZED OSZUSTWAMI

Data publikacji 18.03.2020

Od czasu identyfikacji choroby zakaźnej COVID-19, wywoływanej przez koronawirusa i jego rozprzestrzenianiem się na inne kraje, w ostatnim czasie pojawiły się różne typy oszustw. Interpol ostrzega przed przestępcami, którzy wykorzystują strach związany z pandemią.

Oszustwa dokonywane przez przestępców od momentu pierwszych przypadków zakażeń koronawirusem można podzielić na trzy sposoby:

- podrobione strony internetowe, platformy handlu elektronicznego, konta w mediach społecznościowych, fałszywe wiadomości e-mail oferujące maski ochronne na twarz i maski chirurgiczne;
- oszustwo telefoniczne;
- schematy phishingowe.

Poprzez fikcyjne strony internetowe, platformy e-commerce itp. oszuści wykorzystują strach przed koronawirusem. Oszuści tworzą i zakładają fałszywe strony internetowe, platformy handlu elektronicznego, konta społecznościowe i e-maile, oferujące do sprzedaży i dystrybucji maski ochronne na twarz i maski chirurgiczne. W pewnym stopniu oszuści używają nazw znanych firm, które zajmują się produkcją i dostawą masek, szczególnie tych z siedzibą w Europie. Ofiary tych przestępstw proszone są o dokonanie płatności z góry za pomocą przelewów bankowych, zazwyczaj na konta bankowe w krajach europejskich, takich jak Niemcy, Holandia, Hiszpania i Portugalia.

Jak się okazuje, maski nie są w ogóle dostarczane, podczas gdy oszuści pozostają poza zasięgiem, a witryny, platformy są nagle usuwane. Zdarzały się również przypadki, w których ofiary są proszone o odbiór płatnych masek na twarz z różnych klinik, tylko po to, aby ofiary zostały ostatecznie poinformowane, że nie podjęto takich uzgodnień.

Sprawa z Singapuru. (Siły Policyjne Singapuru):

„Cztery osoby aresztowane za oszustwa w handlu elektronicznym obejmujące sprzedaż masek na twarz”

Link: https://www.police.gov.sg/media-room/news/20200222_arrest_four_arrested_for_ecommerce_scams_involving_sale_of_face_masks_cad

Podczas gdy oszustwa telekomunikacyjne i oszustwa telefoniczne pod różnymi pretekstami nie są nowym zjawiskiem, w ostatnim czasie pojawiły się doniesienia o nowszych odmianach oszustw telefonicznych związanych z sytuacją COVID-19.

Sprawcy kontaktują się z osobami starszymi przez telefon, udając krewnego (np. wnuka), który obecnie przebywa w szpitalu z powodu zakażenia COVID-19. W niektórych przypadkach ofiary otrzymały drugie wezwanie od rzekomego lekarza, dyrektora szpitala w celu potwierdzenia leczenia. Następnie ofiary są informowane o konieczności niezwłocznego pokrycia kosztów leczenia poprzez zdeponowanie pieniędzy lub przekazanie gotówki, lub innych kosztowności „przedstawicielom szpitala", którzy pojawią się pod adresem ofiary.

Zdarza się też, że ofiary otrzymują telefony od rzekomych urzędników służby zdrowia z prośbą o podanie danych osobowych w celu przeprowadzenia „śledzenia kontaktów", co jest procesem identyfikacji i monitorowania osób, które miały bliski kontakt z zarażonymi osobami po wybuchu jakiejkolwiek choroby. W przeciwieństwie do prawdziwych urzędników ds. zdrowia, oszuści zwykle proszą ofiary o dane bankowe i dotyczące płatności w celu rzekomej weryfikacji.

W ostatnich tygodniach odnotowano kilka przypadków phishingowych listów i wiadomości e-mail związanych z COVID-19. Przestępcy rozpowszechniają złośliwe linki i dokumenty, które zawierają informacje o tym, jak chronić się przed rozprzestrzenianiem COVID-19 oraz zalecenia dotyczące działania przeciwko pandemii. Niektóre z tych e-maili zachęcają odbiorców do otwarcia linku lub strony, która rzekomo zawiera dodatkowe ważne informacje.

Aby otworzyć taką stronę, odbiorcy proszeni są o zalogowanie się przy użyciu swojego adresu e-mail i hasła. W ten sposób przestępcy mogą instalować złośliwe oprogramowanie na urządzeniu odbiorcy i kraść pieniądze lub poufne informacje. Takie listy i wiadomości e-mail sugerują, że zostały wysłane przez znane organizacje, takie jak Światowa Organizacja Zdrowia (WHO).

Strzeż się przestępców udających WHO!

Link: https://www.who.int/about/communications/cyber-security

KGP