POLICJA MAŁOPOLSKA

https://malopolska.policja.gov.pl/krk/aktualnosci/8232,Jak-chronic-sie-przed-cyberprzestepcami-w-czasie-pandemii.html
2021-05-16, 22:49

JAK CHRONIĆ SIĘ PRZED CYBERPRZESTĘPCAMI W CZASIE PANDEMII?

Fałszywe sklepy internetowe, oszustwa telefoniczne, ransomware - cyberprzestępcy nie próżnują i szukają wciąż nowych sposobów na uzyskanie korzyści finansowych kosztem użytkowników Internetu. Na co zwracać uwagę i jak wyjść ze starcia z przestępcami obronną ręką informuje kampania Interpolu, Biura do Walki z Cyberprzestępczością Komendy Głównej Policji i Państwowego Instytutu Badawczego NASK.

W czasie pandemii zmuszeni jesteśmy spędzać w internecie coraz więcej czasu, nie tylko ucząc się i pracując zdalnie, załatwiając sprawy urzędowe, ale również robiąc zakupy czy utrzymując relacje towarzyskie.

Warto zadbać o swoje bezpieczeństwo w sieci. Najważniejsza jest zasada ograniczonego zaufania. Tylko ostrożność i dokładne weryfikowanie informacji i kontaktów w internecie pozwoli ograniczyć cyberprzestępcom zdobycie dostępu do zawartości naszych urządzeń – smartfonów i komputerów – za ich pośrednictwem do naszych kont bankowych, kont w portalach społecznościowych, skrzynek poczty elektronicznej – zarówno prywatnych jak i służbowych.

- Cały świat jest aktualnie skupiony na przeciwdziałaniu pandemii COVID-19, nie znaczy to jednak, że cyberprzestępcy zaniechali swoich działań. Jest wręcz odwrotnie – wykorzystując fakt, że nasza uwaga skierowana jest na coś innego, nadal atakują sieci komputerowe światowych organizacji, przedsiębiorstw i korzystają z nieuwagi osób prywatnych dla własnego zysku – podkreśla Przemysław Jaroszewski Kierownik CERT Polska.

Maseczka z dostawą – czy aby na pewno?

W związku z pandemią na celowniku cyberprzestępców znalazły się m.in. artykuły medyczne. Intensywnie poszukiwane maseczki czy środki ochrony osobistej, często niedostępne w sklepach stacjonarnych, pojawiały się w sprzedaży na fałszywych stronach internetowych czy kontach w mediach społecznościowych. Niepodejrzewające niczego ofiary nie otrzymywały zakupionych przedmiotów, a ich pieniądze przepadały w rękach oszustów.

Dotyczy to jednak nie tylko środków medycznych. Podobny mechanizm – kiedy przestępcy obiecują ofiarom poszukiwane towary, przyjmują płatność i znikają – można powiązać z dowolnym produktem, m.in. odzieżą, artykułami biurowymi, elektroniką czy usługą.

Dla uchronienia się przed oszustwem wystarczy stosowanie kilku podstawowych zasad:

1. Przed zakupami w Internecie (artykułów medycznych, elektroniki, odzieży itp.) zweryfikuj firmę lub osobę oferującą produkty i sprawdź opinie w Internecie.
2. Uważaj na fałszywe strony internetowe - przestępcy często używają adresu internetowego, który wygląda prawie identycznie jak prawdziwy, np. „abc.org” zamiast „abc.com”.
3. Zachowaj ostrożność, jeśli zostaniesz poproszony o dokonanie płatności na konto bankowe zlokalizowane w innym kraju niż siedziba firmy.

4. Nie klikaj linków ani nie otwieraj załączników, których się nie spodziewasz lub które pochodzą od nieznanego nadawcy.
5. Uważaj na niechciane e-maile oferujące sprzęt medyczny lub proszące o podanie danych osobowych w celu przeprowadzenia badań lekarskich - legalne instytucje ochrony zdrowia zwykle nie kontaktują się w ten sposób.
6. Jeśli uważasz, że padłeś ofiarą oszustwa, natychmiast powiadom swój bank lub dostawcę usług płatniczych, aby można było wstrzymać płatność i złóż zawiadomienie w najbliższej jednostce Policji.

Pandemia koronawirusa spowodowała znaczący wzrost liczby wyłudzeń danych w związku z treściami dotyczącymi koronawirusa. CERT Polska wspólnie z operatorami telekomunikacyjnymi prowadzi listę ostrzeżeń przed stronami wyłudzającymi dane osobowe, dane uwierzytelniające do kont bankowych i serwisów społecznościowych. Lista jest dostępna publicznie każdy może się z nią zapoznać, a także zgłosić podejrzaną stronę, wypełniając krótki formularz pod adresem: incydent.cert.pl/phishing.

Oszustwa telefoniczne „na koronawirusa”

W wielu przypadkach oszuści podszywają się pod legalne firmy, używając podobnych nazw, stron internetowych i adresów e-mail, próbując oszukać nieświadome osoby. Dzwonią do ofiary i podają się za pracowników szpitala lub przychodni. Przekonują rozmówcę, że jego krewny zakaził się koronawirusem i trzeba opłacić jego leczenie.

Poniżej kilka sposobów umożliwiających rozpoznanie i ochronę przed oszustwami telefonicznymi:

1. Sprawdź tożsamość dzwoniącego.
2. Nie sprawdzaj dzwoniącego za pomocą numeru telefonu, który ci podał – to może być fałszywy numer.
3. Wyszukaj w Internecie numer telefonu instytucji/organizacji/firmy i zadzwoń bezpośrednio.
4. Nie działaj pod presją czasu. Uważaj na wszystkie wiadomości, które skłaniają do natychmiastowego działania.
5. Nie podawaj żadnych poufnych danych przez telefon (haseł, loginów, danych karty kredytowej, itp.).
6. Nie ufaj komuś, kto podaje się za urzędnika państwowego lub funkcjonariusza organów ścigania i żąda zapłaty lub poufnych informacji. Od razu skontaktuj się z lokalną Policją, aby to sprawdzić.

Złośliwe oprogramowanie, złośliwe domeny i ransomware – to problemy bardzo aktualne

Pandemia zaowocowała powstaniem ogromnej liczby zarejestrowanych w internecie stron, których domeny zawierają słowa: „koronawirus”, „korona-wirus”, „covid19” i „covid-19”. Niektóre z nich to legalne strony, ale cyberprzestępcy tworzą każdego dnia tysiące nowych, aby prowadzić kampanie spamowe, phishingowe lub rozpowszechniać złośliwe oprogramowanie. Odwiedzając takie strony, np. z interaktywnymi mapami rozprzestrzeniania się koronawirusa, można zainfekować urządzenie złośliwym oprogramowaniem, oprogramowaniem szpiegującym i trojanami.

Przestrzeganie poniższych zasad pozwoli uniknąć ryzyka zainfekowania urządzenia:

1. Przeglądając Internet, nie klikaj w podejrzane linki, wyskakujące okienka (pop-up), okna dialogowe ani podejrzane reklamy.
2. Nie otwieraj załączników i nie klikaj linków w nieoczekiwanych lub podejrzanych mailach czy smsach.
3. Aktualizuj oprogramowanie i system operacyjny. Nie wyłączaj automatycznych aktualizacji.
4. Pobieraj tylko oficjalne wersje oprogramowania z zaufanych witryn.
5. Korzystaj z oprogramowania antywirusowego i zapory sieciowej i na bieżąco je aktualizuj.
6. Pamiętaj o poprawnym wylogowywaniu się z kont w poczcie e-mail, mediach społecznościowych, sklepach internetowych itp.
7. Regularnie wykonuj kopię zapasową danych przechowywanych na komputerze. Kopię przechowuj w chmurze lub na zewnętrznych dyskach.

Fałszywe inwestycje, pranie pieniędzy i sextortion

Przestępcy dostosowują swoje działania do panujących okoliczności, ale sięgają też po wypróbowane sposoby oszukiwania potencjalnych ofiar. Wśród nich warto wymienić oszustwa inwestycyjne, kiedy namierzone osoby są namawiane, aby zainwestować w fałszywe lub bezwartościowe akcje. Jeśli otrzymujemy niespodziewaną wiadomość o możliwościach inwestycyjnych, należy być sceptycznym i zweryfikować autentyczność produktów inwestycyjnych np. kontaktując się z niezależnym doradcą – przekonuje Przemysław Jaroszewski z CERT Polska.

Zdarzają się też coraz częściej przypadki prania pieniędzy, kiedy ofiara (muł finansowy, słup) zostaje poproszona o umożliwienie korzystania z jej konta bankowego, na którym może później dochodzić do obracania dużymi kwotami. Działaność „muła finansowego" jest nielegalna i umożliwia zorganizowanym grupom przestępczym łatwe pranie pieniędzy i przenoszenie funduszy na całym świecie oraz wspomaga takie przestępstwa jak handel narkotykami, handel ludźmi czy oszustwa internetowe. Przestępcy często nawiązują relacje ze swoimi ofiarami, zanim nakłonią je do operowania pieniędzmi. Wykorzystywany jest do tego proceder tzw. romance scams. Przestępcy rekrutują muły na portalach randkowych. Uwodząc ofiary, z czasem przekonują je do otworzenia rachunków bankowych pod pozorem wysyłania lub otrzymywania środków finansowych.

Jak się chronić?

1. Nigdy nie otwieraj konta bankowego na prośbę kogoś, kogo właśnie poznałeś.
2. Nie podawaj nikomu numeru swojego konta bankowego ani żadnych innych danych osobowych.
3. Uważaj na niechciane e-maile lub oferty składane w mediach społecznościowych lub osobiście, obiecujące łatwe pieniądze.
4. Zignoruj wszelkie oferty pracy obejmujące przelewy pieniężne za pośrednictwem konta bankowego, niezależnie od tego, jak autentyczne mogą się wydawać. Jeśli okazja brzmi zbyt dobrze, aby była prawdziwa, prawdopodobnie tak jest.

Cyberataki i wszelkie naruszenia w sieci należy zgłaszać do CERT Polska w Państwowym Instytucie Badawczym NASK pod adresem: https://incydent.cert.pl

Niniejsze działania realizowane są w ramach obowiązków CSIRT NASK (Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego) wynikających z przepisów ustawy o Krajowym Systemie Cyberbezpieczeństwa (ustawa z dnia 5 lipca 2018r. (Dz.U. 2018 poz. 1560 z późn.zm.).

Bieżąca działalność CSIRT NASK dofinansowana jest ze środków budżetu państwa - dotacja podmiotowa z Ministerstwa Cyfryzacji / Kancelarii Prezesa Rady Ministrów.

(Biuro d/w z Cyberprzestępczością KGP)