Cyberdefence 24

18.01.2021

KPRM OSTRZEGA PRZED "CYBERWIRUSEM"

Cyberprzestępcy nie mają litości. Aby okraść swoje ofiary wykorzystają ich lęk, niepokój o bliskich i chęć zadbania o zdrowie. KPRM rekomenduje jak się przed nimi ochronić.

Ostatnie miesiące, tygodnie i dni to czas wyjątkowej aktywności cyberprzestępców. Od początku stycznia na listę ostrzeżeń przed fałszywymi stronami trafiło 600 witryn. Od marca 2020 r. – 8151.

Bezwzględni

„Czy myślisz, że masz koronawirusa? Ustal to z 99,9% prawdopodobieństwem. Po prostu nagraj swój kaszel w aplikacji i uzyskaj wyniki" – na takie wiadomości jeszcze kilka dni temu można było natknąć się w internecie. Ich autorzy podszywali się pod aplikację STOP COVID – ProteGO Safe, wykorzystując przy tym fałszywą domenę. Ich celem było zainstalowanie na telefonach potencjalnych ofiar złośliwego oprogramowania w celu wyłudzenia danych osobowych, danych uwierzytelniających do kont bankowych lub serwisów społecznościowych.

"Domena trafiła już na listę fałszywych stron i ataki z tego adresu zostały powstrzymane. Nie oznacza to, że niebawem cyberprzestępcy podejmą kolejną próbę. Dlatego ważne, aby być czujnym" – ostrzega minister Marek Zagórski, pełnomocnik rządu ds. cyberbezpieczeństwa.

KPRM przedstawia kilka prostych sposób, które pozwolą nie paść ofiarą cyberprzestępców:

- Dokładnie sprawdzać wygląd i adres strony (na pierwszy rzut oka może nie różnic się od tego oficjalnego, ale wystarczy się przyjrzeć, by znaleźć np. drobną literówkę), na której podawane są dane logowania, dane osobowe czy karty płatniczej.
- Nie działać pod presją czasu, uważać na maile, SMS-y, strony internetowe, aplikacje i telefony, które skłaniają do natychmiastowego działania.
- Uważać na sensacyjne wiadomości, strony wymagające dodatkowego logowania, również te udostępniane z kont znajomych w mediach społecznościowych.
- Weryfikować źródła informacji zanim podejmie się działania na ich podstawie lub zaczniemy je powielać.
- Pamiętać, że szczepienia przeciwko koronawirusowi są bezpłatne i dobrowolne. Nie jest wymagane dokonywanie żadnych opłat, ani wypisywanie się z rejestracji. Oficjalne informacje o szczepieniach można znaleźć na stronie https://www.gov.pl/szczepimysie, a inne oficjalne i prawdziwe informacje o sytuacji epidemicznej (w tym o dostępnych aplikacjach) na https://www.gov.pl/koronawirus
- Jeśli nie ma pewności, że dana informacja jest prawdziwa - należy skontaktować się z rzekomym nadawcą innym znanym kanałem i/lub poszukajcie potwierdzenia informacji w innych źródłach.
- Zgłaszać do CSIRT NASK każdą podejrzaną stronę, a także wiadomości e-mail i SMSy, które mogą wyłudzać dane. Formularz można znaleźć na stronie https://incydent.cert.pl

Wzmożona aktywność

Aby ostrzegać użytkowników przed nadużyciami, w tym przed fałszywymi stronami internetowymi, za pośrednictwem których wyłudzane są dane osobowe lub pieniądze uruchomiono razem z NASK i UKE oraz we współpracy z operatorami telekomunikacyjnymi listę ostrzeżeń przed fałszywymi stronami.

"Jest dostępna publicznie i tylko od marca trafiło na nią ponad 8151 domen, z tego tylko w tym miesiącu – 600" – mówi minister Marek Zagórski, pełnomocnik rządu ds. cyberbezpieczeństwa. Zgłoszenie może wysłać każdy, kto trafi w sieci na podejrzaną stronę. Każde zgłoszenie jest dokładnie weryfikowane, a jeśli strona okazuje się fałszywa - jest blokowana przez operatorów – dodaje.

Z informacji o przestępczych stronach bezpłatnie korzystać mogą wszyscy administratorzy, którzy chcą chronić swoich użytkowników przed atakami przeprowadzanymi poprzez strony podszywające się pod znane podmioty i usługi.

Oszustwo na szczepionkę

Policja w Wielkiej Brytanii ostrzega przed cyberprzestępcami, którzy oferują szczepionki na COVID-19. Potencjalne ofiary, które skuszą się na "super ofertę" mogą stracić dane albo pieniądze. W Polsce właśnie rozpoczął się program szczepień skierowanych do seniorów 80+, a potem zostaną do niego przyłączone pozostały grupy osób. Dlatego też można spodziewać się podobnych fałszerstw, a szczególnie podatne mogą być właśnie osoby starsze. Policja w Polsce w odpowiedzi na pytania CyberDefence24.pl poinformowała, że nie posiada informacji o podobnych procederze w Polsce.

Od początku pandemii koronawirusa Komenda Główna Policji oraz FinCERT.pl – Bankowe Centrum Cyberbezpieczeństwa Związku Banków Polskich nieustannie ostrzegają przed oszukańczymi ogłoszeniami związanymi np. potrzebą zapłaty za szczepionkę przeciwko koronawirusowi COVID-19. Funkcjonariusze na terenie całej Polski apelują o zachowanie ostrożności i rozsądku oraz przestrzegają przed oszustami.

AK/Informacja prasowa