TYSIĄCE NIEBEZPIECZNYCH STRON. JAK NIE STAĆ SIĘ OFIARĄ CYBERPRZESTĘPCÓW?

Ponad 10 tysięcy adresów znajduje się obecnie na liście ostrzeżeń przed niebezpiecznymi stronami. „Na listę trafiają strony wyłudzające dane lub pieniądze. Każde zgłoszenie jest weryfikowane w CSIRT NASK" - wskazuje Marek Zagórski, pełnomocnik rządu ds. cyberbezpieczeństwa. Jak nie stać się ofiarą cyberprzestępców?

Dzięki współpracy Cyfryzacji KPRM z NASK PIB, UKE oraz operatorami telekomunikacyjnymi, w ubiegłym roku uruchomiono listę ostrzeżeń przed fałszywymi stronami. Z założenia inicjatywa ma alarmować użytkowników przed nadużyciami, w tym przed fałszywymi stronami internetowymi, za pośrednictwem których wyłudzane są dane osobowe lub pieniądze. „Do dziś znalazło się na niej już ponad 10 tysięcy adresów" - czytamy w oficjalnym komunikacie Cyfryzacji KPRM.

„Na listę trafiają strony wyłudzające dane lub pieniądze. Każde zgłoszenie jest weryfikowane w CSIRT NASK. Kiedy podejrzenia okazują się prawdziwe – strona trafia na listę ostrzeżeń, użytkownicy są ostrzegani przed wejściem na taką stronę, a operatorzy mogą ograniczać obsługę takiej strony. W niektórych wypadkach powiadamiane są też organy ścigania - prokuratura i policja" - tłumaczy minister Marek Zagórski, pełnomocnik rządu ds. cyberbezpieczeństwa.

Jak wskazano w komunikacie, podejrzaną stronę może zgłosić każdy. Wystarczy jedynie wypełnić specjalny internetowy formularz. Z kolei sama lista ostrzeżeń jest dostępna publicznie.

„Cyberprzestępcy nie mają litości. Ostatnie miesiące i tygodnie to czas ich wyjątkowej aktywności" - wskazuje Cyfryzacja KPRM. Aby okraść użytkowników, wykorzystają m.in. lęk, niepokój o bliskich oraz chęć zadbania o zdrowie. W tym kontekście najważniejsza jest czujność - to niezmiennie fundament cyberbezpieczeństwa.

Jak zadbać o cyberbezpieczeństwo?

A co konkretnie należy zrobić, aby nie stać się ofiarą cyberprzestępców? Cyfryzacja KPRM zaprezentowała kilka prostych sposobów, które pozwolą podnieść bezpieczeństwo użytkowników:

- Należy 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 użytkownik zamierza podać dane logowania, dane osobowe czy karty płatniczej;
- Nie wolno działać pod presją czasu, a także uważać na maile, SMS-y, strony internetowe, aplikacje i telefony, które skłaniają do natychmiastowego działania;
- Konieczne jest podchodzenie z ograniczonym zaufaniem do sensacyjnych wiadomości, stron wymagających dodatkowego logowania, również tych udostępnianych z kont znajomych w mediach społecznościowych;

- Warto weryfikować źródła informacji przed podjęciem działania na ich podstawie lub powielenia;
- Należy pamiętać, że szczepienia przeciwko koronawirusowi są bezpłatne i dobrowolne. Nie jest wymagane dokonywanie żadnych opłat, ani wypisywanie się z rejestracji. Oficjalne informacje o szczepieniach znajdują się 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;
- W przypadku, gdy użytkownik nie jest pewny, że dana informacja jest prawdziwa - powinien skontaktować się z rzekomym nadawcą innym znanym kanałem i/lub poszukać potwierdzenia informacji w innych źródłach;
- Należy także zgłaszać do CSIRT NASK każdą podejrzaną stronę, a także wiadomości e-mail i SMSy, które mogą wyłudzać dane. Odpowiedni formularz znajduje się na stronie https://incydent.cert.pl.

Warto zgłosić

Cyberprzestępcy najczęściej podczas wrogich działań wykorzystują metodę tzw. phishingu. „Ta nazwa nie przez przypadek budzi dźwiękowe skojarzenia z fishingiem, czyli - po angielsku - łowieniem ryb. Przestępcy, podobnie jak wędkarze, stosują bowiem odpowiednio przygotowaną >przynętę<" - wyjaśnia Cyfryzacja KPRM.

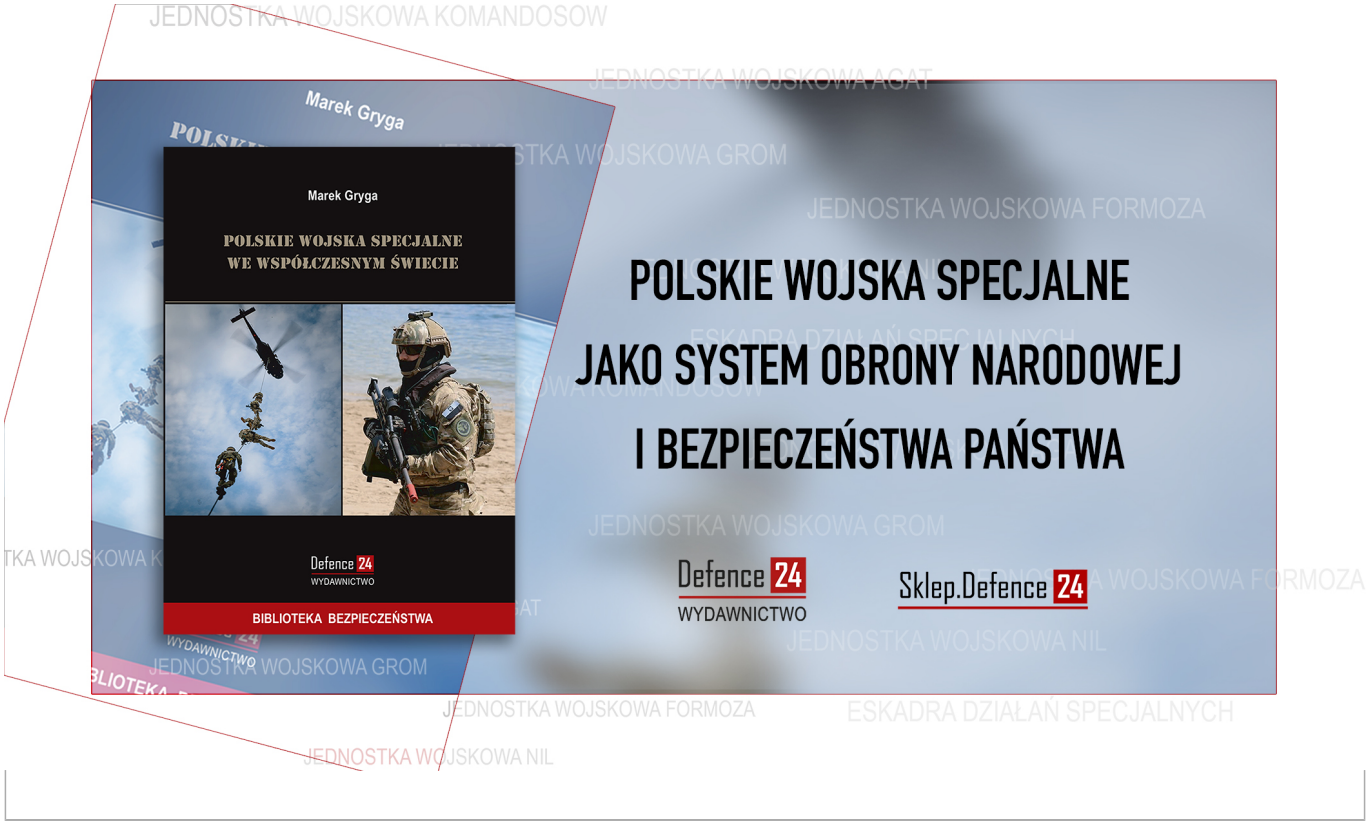
W oficjalnym komunikacie podkreślono, że phishing to jeden z najpopularniejszych typów ataków opartych o wiadomości e-mail lub SMS. Stosujący go cyberprzestępcy wykorzystują znaną technikę, która ma spowodować że podejmiemy działania zgodne z ich zamierzeniami. „To dlatego kuszą nas sensacyjnymi tytułami, rzekomymi niepowtarzalnymi ofertami, czy promocjami, które nigdy więcej się nie powtórzą. Są przy tym bezwzględni" - wskazuje Cyfryzacja KPRM. Jak podkreślono, cyberprzestępcy podszywają się np. pod firmy kurierskie, urzędy, operatorów telekomunikacyjnych, czy nawet naszych znajomych. Podczas działań wykorzystują w coraz większym stopniukomunikatory i portale społecznościowe.

„Cyberprzestępcy nie ustają w wysiłkach, by stale tworzyć nowe metody oszukiwania nas, czy wyłudzenia naszych pieniędzy lub danych. Dlatego my także nieustannie musimy być czujni. Weryfikujmy informacje, nie działajmy w emocjach, a jeśli mamy pewność, że jesteśmy świadkami przestępstwa, zgłaszajmy to" - radzi minister cyfryzacji Marek Zagórski.

Incydenty można zgłosić wchodząc na stronę https://incydent.cert.pl i wypełnić dostępny tam formularz.

SZP/Cyfryzacja KPRM

Czytaj też: Jak stworzyć mocne hasło? KPRM przygotowało poradnik


Marek Gryga
POLSKIE WOJSKA SPECJALNE
WE WSPÓŁCZESNYM ŚWIECIE
Defence 24
WYDAWNICTWO
BIBLIOTEKA BEZPIECZEŃSTWA
POLSKIE WOJSKA SPECJALNE
JAKO SYSTEM OBRONY NARODOWEJ
I BEZPIECZEŃSTWA PAŃSTWA
Defence 24
WYDAWNICTWO
Sklep.Defence 24