Fałszywe strony internetowe – jak się chronić przed utratą danych lub pieniędzy

Fałszywe strony internetowe to jedne z najczęściej stosowanych sposobów, by w nieuczciwy sposób pozyskać nasze dane lub wyłudzić od nas pieniądze. Jak nie dać się nabrać?

Przestępcy w różnych kampaniach phishingowych lub przy wykorzystaniu fałszywych reklam lub innych nieuczciwych sposobów przesyłają wiadomości i zamieszczają w nich linki, które po kliknięciu, przenoszą nas na fałszywe witryny internetowe. Mimo licznych kampanii i akcji informacyjnych skierowanych do użytkowników internetu, liczba ofiar różnych przestępstw internetowych jest nadal wysoka. Istnieje kilka sposobów, które mogą pomóc w weryfikowaniu, czy dana strona jest prawdziwa czy też nie.

Błędy w adresie czy zawartości strony

Fałszywe strony internetowe przygotowywane przez oszustów wyglądają bardzo podobnie lub niemalże identycznie, jak te prawdzie. Ich układ, szata graficzna, czcionka, układ obrazków czy logotypów firmy, niczym się nie różnią od tej właściwej. Jak je zatem rozróżnić? Przede wszystkim należy zwrócić uwagę na adres strony, na którą wchodzimy. Z pozoru adres może wydawać się identyczny, jednak po przeanalizowaniu możemy znaleźć literówkę, zamienioną kolejną wyrazów lub inne błędy, np. www.pkobq.pl, www.face-book.pl.

Strony internetowe tworzone przez cyberprzestępców często zawierają błędy na stronie – np. są pisane niepoprawną polszczyzną, brakuje polskich znaków czy używane logo firmy jest stare, nieaktualne. Gdy próbujemy „przeklikać się" na inne podstrony, zostajemy odesłani w zupełnie inne miejsce niż chcieliśmy. W przypadku fałszywych sklepów internetowych ciężko odnaleźć regulamin sklepu lub zakładkę kontakt, pod którym moglibyśmy otrzymać więcej informacji, np. numer telefonu.

Na jakie elementy zwrócić uwagę, by zweryfikować stronę?

Jeszcze do niedawna fałszywe strony internetowe można było rozpoznać po braku certyfikatu bezpieczeństwa i braku tzw. kłódki. Obecnie oszuści coraz rzetelniej przygotowują swoje strony, i należy uznać, że certyfikat bezpieczeństwa nie świadczy o tym, że dana strona jest bezpieczna.

Pamiętaj, jeśli połączysz się z witryną i otrzymasz komunikat, że może to być niebezpieczne dla Twojego sprzętu, nie bagatelizuj go.

Zasady, które mogą nas uchronić przed utratą danych lub pieniędzy:

- Pamiętajmy, że najważniejsza jest zasada ograniczonego zaufania. Jeśli mamy jakiekolwiek wątpliwości, by wejść w dany link lub by podjąć jakieś działania, wycofajmy się z tego;
- Starajmy się również nie działać w pośpiechu, czy pod wpływem emocji. Zanim zdecydujemy się kliknąć w dany link, dajmy sobie chwilę czasu, złapmy oddech i zweryfikujmy wiadomość, która przekierowuje nas na podejrzaną witrynę;
- Korzystając z bankowości elektronicznej, adres zawsze wpisujmy ręcznie lub dodajmy witrynę do ulubionych. Nie klikajmy w linki w nieoczekiwanych wiadomościach „z banku". Dzięki temu unikniemy wejścia na witrynę, która może być fałszywa;
- Aktualizujmy swój sprzęt i oprogramowanie, z którego korzystamy. Jeśli to możliwe, włączmy automatyczne aktualizacje;
- Nie bagatelizujmy komunikatów wyświetlanych na stronach internetowych, które przestrzegają przed zagrożeniem i stosujmy się do zaleceń, które otrzymujemy;
- Zawsze pamiętajmy, by korzystać z programów antywirusowych i jeśli to możliwe, zapory firewall.

Jeśli natrafisz w sieci na fałszywe strony internetowe lub inne zagrożenia, zgłoś je do zespołu CSIRT NASK:

- na stronie: https://incydent.cert.pl
- e-mailem: cert@cert.pl
- sms-em: 799 448 084