Fałszywe domeny – jak nie dać się oszukać?

Kategoria: Styl życia
Opublikowano: piątek, 12, styczeń 2024 11:07
Katarzyna Sekuła
Odsłony: 627

Podejrzanie niska cena, brak kontaktu do biura obsługi klienta, skrajne opinie o sklepie wystawione przez innych użytkowników – wszystkie te rzeczy powinny zwrócić uwagę przeglądającego i skłonić do sprawdzenia, czy nie trafiono na fałszywą domenę, która podszywa się np. pod znany sklep internetowy.

Celem oszustów jest wyłudzenie naszych danych, a w konsekwencji – kradzież pieniędzy z naszych kont bankowych. Jeśli klikamy w reklamę np. jakiegoś sklepu lub w przechodzimy do stron, które wyskoczyły nam w wynikach wyszukiwania, zwracajmy szczególną uwagę, dokąd ten link nas przekieruje. To popularna metoda oszustów działających w sieci.

Jak się przed tym chronić?

Warto mieć świadomość tego, że płatne reklamy może wykupić w sieci każdy, również złodziej. Dlatego zanim zdecydujemy się na zakupy online, warto wyszukać o nim maksymalnie dużo informacji. Zwracać uwagę na adres strony „na pasku" – szukać literówek czy innych błędów. Uważać też na pliki, które pobieramy z internetu – mogą one zawierać szkodliwe oprogramowanie. Lepiej korzystać z oficjalnych i autoryzowanych sklepów (np. Sklep Googla, AppStore), a na komputerach – ze stron producenta albo dostawcy oprogramowania.

Ministerstwo Cyfryzacji przypomina, aby przed zakupami sprawdzić, jakie opinie sklep ma w sieci. Liczba opinii i czas, w jakim zostały dodane, to cenne wskazówki – jeśli intuicyjnie wyczujemy, że są one np. pisane „na zamówienie" – zrezygnujmy z zakupów. Każdy sklep internetowy powinien mieć też udostępniony na stronie telefon kontaktowy oraz adres siedziby. Naszą uwagę powinien zwrócić fakt, czy na stronie dostępne są popularne metody płatności – jeśli nie ma tych opcji i możliwości płatności przy odbiorze to znak, że mogliśmy trafić na fałszywy panel sprzedażowy.

„Jeśli trafimy na fałszywą domenę, namawiam do zgłoszenia jej na incydent.cert.pl. Specjaliści z CERT przygotowali listę domen, które wprowadzają użytkowników w błąd i wyłudzają od nich dane i jest ona na bieżąco aktualizowana" – wyjaśnia minister cyfryzacji Krzysztof Gawkowski i dodaje, że lista ostrzeżeń jest wykorzystywana przez operatorów telekomunikacyjnych, firmy, organizacje i samych użytkowników do automatycznego blokowania dostępu do złośliwych stron. To ogranicza skutki ataków phishingowych i innych kampanii wymierzonych w użytkowników.

Lista ostrzeżeń przed niebezpiecznymi stronami dostępna pod linkiem: cert.pl/lista-ostrzezen/

Źródło: MC

Phoca PDF