Warto wiedzieć...

Uważni w cyberprzestrzeni

Jak bezpiecznie przeglądać strony w Internecie?

Zachowaj ostrożność w przypadku udostępniania swoich danych osobowych w cyberprzestrzeni. Aby uniknąć różnych metod oszustwa lub nieuczciwego wykorzystania informacji o Tobie, istotne jest wyrobienie w sobie nawyku sprawdzania przekazywanych informacji lub konsultowania się z zaufanymi osobami przed podjęciem działań w sieci, które mogłyby potencjalnie Tobie zaszkodzić. Uważaj, aby nie udostępniać danych osobowych na fałszywych stronach. Jak więc bezpiecznie przeglądać strony w Internecie i rozpoznać oznaki cyberataków, aby uniknąć zainfekowania złośliwym oprogramowaniem urządzeń oraz utraty danych osobowych? Oto kilka podpowiedzi, na co zwracać uwagę.

WSKAZÓWKI DOTYCZĄCE BEZPIECZNEGO PRZEGLĄDANIA W INTERNECIE

⊗ Nie wprowadzaj żadnych danych na stronach, które nie stosują szyfrowania danych, tj. nie posiadają na początku adresu skrótu https oraz ikony zamkniętej kłódki w pasku adresu przeglądarki;

⊗ Zawsze upewnij się, że na przeglądanej stronie internetowej znajduje się polityka prywatności, która zawiera informacje o administratorze (dane kontaktowe) i zasady ochrony danych osobowych;

⊗ Zainstaluj oprogramowanie zabezpieczające do blokowania nietypowej aktywności w przeglądarce, tj. wyskakujących okienek z ofertami/plikami/programami do pobrania;

⊗ W przypadku znalezienia się na stronie internetowej, która wzbudza Twoje podejrzenia, nie podawaj danych osobowych np. danych logowania w serwisie społecznościowym czy danych do poczty e-mail itp.;

⊗ Nie ufaj informacjom o możliwych wygranych czy nagrodach. Nie podawaj danych osobowych w celu odebrania wygranej, a także nie pobieraj dodatkowych aplikacji w celu odebrania wygranej.

CECHY CHARAKTERYSTYCZNE DLA NIEBEZPIECZNYCH STRON INTERNETOWYCH

1. ZNIEKSZTAŁCENIE TREŚCI

Atak ten jest łatwy do zidentyfikowania. Oszuści zmieniają zawartość witryny za pomocą własnej nazwy, logo czy obrazów zawierających treści przyciągające uwagę np. prowokacyjnych reklam.

2. OKIENKA ZAWIERAJĄCE ODNOŚNIKI

Występowanie „wyskakujących" okienek, które zawierają informacje niezwiązane z zawartością przeglądanej strony. Kliknięcie okienka może spowodować pobranie złośliwego oprogramowania.

3. MALVERTISING

Złośliwe reklamy, które łatwo dostrzec promują „cudowne" uzdrowienia lub skandale z celebrytami. Zwykle wyglądają nieprofesjonalnie i zawierają błędy ortograficzne czy gramatyczne. Takie reklamy, ale także te które pasują do Twojej historii przeglądania, mogą również zawierać złośliwe oprogramowanie.

4. ZESTAWY DO PHISHINGU

To są strony naśladujące najczęściej odwiedzane strony w sieci np. strony banków, portali społecznościowych, aby nakłonić użytkowników do podania danych osobowych nieuprawnionym osobom. Zwracaj uwagę, czy nazwa strony widoczna w przeglądarce (adres URL) nie zawiera błędów gramatycznych, czy też np. innego rozszerzenia.

5. ZŁOŚLIWE PRZEKIEROWANIE

Jeśli podczas wpisywania adresu URL następuje przekierowanie na inną stronę, która wygląda podejrzanie, nie przeglądaj takiej strony i uruchom ponownie przeglądarkę.

6. SPAM W WYSZUKIWARKACH

Pojawienie się nietypowych linków na stronie, często w sekcji komentarzy, jest prawdziwą oznaką spamu wyszukiwawczego.

7. ALERTY WYSZUKIWAREK I PROGRAMÓW ANTYWIRUSOWYCH

Popularne wyszukiwarki skanują witryny w poszukiwaniu złośliwego oprogramowania i ostrzegają o tym. Wbudowany moduł do sprawdzania witryn posiadają również niektóre programy antywirusowe. Ostrzeżenia te jednoznacznie wskazują, że strona jest zainfekowana złośliwym oprogramowaniem.

Źródło: https://vdai.lrv.lt/lt/naujienos/patarimai-kaip-apsaugoti-savo-asmens-duomenis-ir-finansus-karo-ukrainoje-metu-padaugejus-sukciavimo-atveju-internete

URZĄD OCHRONY DANYCH OSOBOWYCH