Bezpieczeństwo w sieci Internet *

Zagrożenia związane z użytkowaniem sieci Internet

Poniżej przedstawiono najczęstsze zjawiska i działania w sieci, które mogą zagrażać jej bezpieczeństwu lub interesowi innych użytkowników albo stanowić naruszenie prawa:

- działania mogące powodować zakłócenia pracy urządzeń podłączonych do sieci;
- kierowanie do sieci, bez zgody operatora, ruchu pochodzącego z innych sieci telekomunikacyjnych;
- uzyskanie nielegalnego dostępu lub wykorzystanie usług telekomunikacyjnych niezgodnie z przeznaczeniem;
- generowanie ruchu sieciowego nie służącego bezpośredniej wymianie informacji pomiędzy użytkownikami, a mającego na celu przeciążenia elementów infrastruktury telekomunikacyjnej;
- wykorzystywanie hasła dostępu do systemów informatycznych bez zgody uprawnionego użytkownika;
- instalowanie w urządzeniu końcowym użytkownika, bez jego zgody, aplikacji niewiadomego pochodzenia, która może spowodować utratę kontroli użytkownika nad urządzeniem lub doprowadzić do utraty poufności danych osobowych;
- podmienianie danych identyfikacyjnych nadawcy poprzez fałszowanie lub podmianę danych identyfikacyjnych nadawcy w celu zmylenia odbiorcy i w konsekwencji wyłudzenia danych (np. numeru karty kredytowej, numeru PIN, hasła, itp.);
- kradzież danych z urządzenia końcowego użytkownika (np. poprzez wykorzystanie Bluetooth, Wi-Fi);
- wysyłanie niezamówionych informacji handlowych (t.zw. SPAM-u), do innych użytkowników końcowych bez ich zgody;
- wysyłanie wirusów do innych użytkowników końcowych;
- zwalczanie programów antywirusowych;
- prowadzenie takich działań niezgodnych z prawem i/lub dobrymi obyczajami, jak promowanie lub rozpowszechnianie nielegalnych i szkodliwych treści dotyczących rasizmu, faszyzmu, komunizmu, ksenofobii, szerzenia nienawiści lub nakłaniania do przemocy wobec odmiennej rasy, pochodzenia etnicznego, wyznania, płci, wieku, orientacji seksualnej itp.;
- rozpowszechnianie lub propagowanie pornografii, w tym pornografii dziecięcej;
- uzyskiwanie dostępu do systemów informatycznych lub do informacji nieprzeznaczonych dla sprawcy takich działań poprzez omijanie lub przełamywanie zabezpieczeń tych systemów;
- prowadzenie działań mających na celu dokuczanie i nękanie innych osób lub instytucji;
- działania naruszające prawa autorskie lub pokrewne, z których często pojawiającymi się przykładami wykorzystującymi usługi dostępu do Internetu są:
  - nielegalne ściąganie programów z sieci bez wymaganej zgody podmiotu dysponującego prawami autorskimi;
  - obchodzenie zabezpieczeń programów w celu uzyskania możliwości korzystania z nich;
  - kopiowanie, udostępnianie lub rozpowszechnianie zdjęć, filmów, muzyki, gier, programów, artykułów, ilustracji z gazet poza zakresem dozwolonego użytku, bez wymaganej zgody na korzystanie z utworów;
  - publikowanie cudzego tekstu jako swojego lub bez podania autora i źródła utworu;
  - usuwanie lub zmiana elektronicznych informacji na temat zarządzania prawami autorskimi lub świadome rozpowszechnianie utworów z bezprawnie usuniętymi takimi informacjami.

Zalecane sposoby ochrony bezpieczeństwa, prywatności i danych osobowych podczas korzystania z usług dostępu do Internetu

Poniżej przedstawiono podstawowe zalecane sposoby ochrony bezpieczeństwa, prywatności i danych osobowych podczas korzystania z usług dostępu do Internetu:

- zainstalowanie w swoim komputerze i uruchomienie programów zabezpieczających, w szczególności programu antywirusowego oraz częsta aktualizacja sygnatur oprogramowania antywirusowego;
- systematyczna aktualizacja wersji systemu operacyjnego i przeglądarki internetowej;
- weryfikacja adresu wpisanego do przeglądarki internetowej;
- korzystanie z połączeń szyfrowanych z wykorzystaniem protokołu HTTPS, w szczególności w trakcie wykonywania zakupów w sklepach internetowych lub dostępu do usług bankowości elektronicznej;
- nieotwieranie wiadomości pocztowych pochodzących od nieznanych nadawców;
- nieodpowiadanie na wiadomości poczty elektronicznej, w których użytkownik jest proszony o podanie lub zweryfikowanie poufnych danych, w szczególności danych osobowych, identyfikatorów, haseł lub kodów dostępu, numerów kont lub kart kredytowych itp.;
- ignorowanie linków przesłanych w wiadomościach poczty elektronicznej lub zamieszczonych na stronach www, które pochodzą z podejrzanych źródeł, w szczególności zachęcają do zmiany hasła do serwisu internetowego;
- nieotwieranie, nieuruchamianie i nieinstalowanie żadnych plików lub aplikacji nieznanego pochodzenia, pobranych z niezaufanych stron www lub otrzymanych pocztą elektroniczną;
- nierejestrowanie się i nieujawnianie bez wyraźnej potrzeby na portalach społecznościowych, forach dyskusyjnych czy blogach swoich danych osobowych ze względu na ryzyko wykorzystania tych informacji przez osoby nieupoważnione;
- niewyłączanie w trakcie korzystania z sieci Internet programów zabezpieczających, w szczególności programów ochrony antywirusowej;
- systematyczne usuwanie plików tymczasowych przeglądarki internetowej;
- wyłączenie w przeglądarce internetowej funkcji zapamiętywania haseł w formularzach;
- nieprzechowywanie haseł do kont w serwisach internetowych w łatwo dostępnych miejscach;
- używanie bezpiecznych (silnych) haseł, nieużywanie tego samego hasła do logowania w różnych serwisach internetowych;
- nieudostępnianie osobom trzecim identyfikatora i hasła do serwisów internetowych;
- korzystanie z bezpiecznych mechanizmów umożliwiających potwierdzanie wykonywanych operacji w serwisach internetowych (takich jak: tokeny, kody SMS lub hasła jednorazowe);
- zachowanie szczególnej czujności przy wchodzeniu na strony internetowe zachęcające do obejrzenia bardzo atrakcyjnych treści lub ofert;
- zachowanie szczególnej ostrożności w przypadku korzystania z sieci Internet w miejscach publicznych lub za pomocą niezabezpieczonych sieci Wi-Fi. W takim przypadku należy ograniczyć do niezbędnego minimum wykonywanie zakupów w sklepach internetowych lub korzystanie z usług bankowości elektronicznej;
- unikanie takich internetowych sprzedawców towarów i usług, którzy jako jedyną formę płatności akceptują tylko nieznane firmy obsługujące płatności internetowe.

---

* przygotowano na podstawie opracowania dostępnego na stronie internetowej UKE nt. zagrożeń występujących podczas korzystania z publicznie dostępnych usług telekomunikacyjnych i sposobów ochrony przed tymi zagrożeniami