SPEED-NET Arkadiusz Broniecki, 43-300 Bielsko-Biała,
ul. Jana Matejki 3
Telefon +48 33 475 25 25, 33 475 20 00
www.speed-net.com.pl, email: biuro@speed-net.com.pl

Jakie są zagrożenia w Internecie? 10 niebezpieczeństw

Poniżej przedstawiamy powszechnie występujące zagrożenia w sieci. Na większość z nich jest narażony każdy użytkownik internetu, bez względu na miejsce zamieszkania, wiek czy biegłość w obsłudze komputera.

1. Złośliwe oprogramowanie

Hakerzy są w stanie wyrządzić sporo szkód, jeżeli posłużą się malware, czyli złośliwym oprogramowaniem. Należą do niego różnego rodzaju wirusy, m.in.

- robaki komputerowe – programy, które posiadają zdolność do replikowania się i rozprzestrzeniania w samoistny sposób. W efekcie powodują szybkie wyczerpywanie zasobów zainfekowanego komputera,

- adware – złośliwy wirus, który wyświetla w przeglądarce i na pulpicie niechciane komunikaty reklamowe, np. w postaci bannerów, okien pop-up czy pasków narzędzi. Po kliknięciu w nie użytkownik jest przekierowywany na reklamowaną stronę internetową. Takie programy zwykle nie są szkodliwe, jednak mocno utrudniają korzystanie z komputera,

- spyware – oprogramowanie szpiegujące, które monitoruje aktywność użytkownika – np. przeglądane strony czy uruchamiane programy. Rodzajem spyware jest keylogger, czyli program rejestrujący naciśnięcia klawiszy na klawiaturze czy wykonujący zrzuty ekranu,

- ransomware – rodzaj malware posiadający zdolność blokowania dostępu do komputera. Aby zdjąć blokadę, ofiara jest nakłaniana do wpłacenia okupu na podany numer konta bankowego.

Cyberprzestępcy w celu zainstalowania szkodliwego oprogramowania zwykle wykorzystują luki w systemie operacyjnym komputera. Można również nieświadomie doprowadzić do infekcji, np. pobierając z internetu zarażony plik czy wchodząc na zainfekowaną stronę.
Malware często udaje legalne i przydatne programy, które okazują się trojanem. Wykrycie złośliwego programu staje się wyjątkowo trudne, jeżeli jest on instalowany razem z rootkitem, czyli szkodliwym kodem, ukrywającym niebezpieczne procesy w systemie. Hakerzy są również w stanie całkowicie przejąć kontrolę nad komputerem, na co pozwala im exploit – program umożliwiający przejęcie uprawnień administratora, np. w celu kradzieży lub usunięcia plików.

2. SPAM

Kolejny rodzaj zagrożenia w sieci to niechciane wiadomości, zwykle o charakterze reklamowym. Są wysyłane w sposób masowy do wielu użytkowników. Reklamy zachęcają do kliknięcia w link, pobrania pliku czy podjęcia określonej aktywności – np. zakupu czy skorzystania z usługi. Do rozsyłania SPAM-u najczęściej służy poczta elektroniczna oraz komunikatory internetowe.

3. Phishing

Poważnym typem zagrożenia w internecie jest phishing, czyli stosowane przez cyberprzestępców techniki wprowadzające użytkownika w błąd z zamiarem odniesienia określonych korzyści. Cyberprzestępcy podszywają się pod znane firmy i instytucje, np. pocztę, kuriera, policję, sąd, kancelarię prawniczą, bank, urząd skarbowy, ZUS, dostawcę energii elektrycznej czy operatora telefonicznego. Próbują wpłynąć na emocje swoich ofiar,

zwykle wywołując u nich lęk czy wywierając poczucie presji czasu. Celem akcji phishingowych jest najczęściej przejęcie dostępu do konta bankowego lub wyłudzenie prywatnych danych.

4. Łamanie zbyt prostych haseł

Hakerzy są w stanie w łatwy sposób przejąć dostęp do konta w banku, poczty elektronicznej, sklepu internetowego czy innych serwisów internetowych. Najszybciej będą w stanie złamać proste i powszechnie używane hasła, np. składające się wyłącznie z imion czy następujących po sobie liczb.

5. Nieodpowiednie treści dla nieletnich

Szczególnie narażone na zagrożenia w internecie są dzieci, które mogą trafić na nieodpowiednie dla nich treści, np. pornografię, materiały promujące przemoc czy nielegalne i przestępcze działania.

6. Przyjmowanie fałszywej tożsamości

W sieci działa wiele przestępców, którzy przyjmują fałszywą tożsamość, np. oszuści matrymonialni. Najczęściej można się na nich natknąć w serwisach społecznościowych oraz na czatach internetowych.

7. Internetowy hejt i fake newsy

Poczucie anonimowości skłania wielu użytkowników do zamieszczania w internecie opinii, których nie byliby w stanie wypowiedzieć w realnym świecie. W sieci można więc znaleźć wiele wypowiedzi określanych jako mowa nienawiści. Są to komunikaty pełne agresji, wulgaryzmów, ostrej krytyki i obraźliwych uwag. Hejt może mieć związek z dyskryminacją, np. ze względu na płeć, rasę, religię, światopogląd czy orientację seksualną.
W sieci nie zawsze są publikowane prawdziwe i wiarygodne treści. Często można trafić na newsy zamieszczane dla żartu czy z zamiarem celowego wprowadzenia użytkowników w błąd. Na podstawie fake newsów spora część z nich podejmuje szkodliwe dla siebie działania.

8. Siecioholizm

Spore zagrożenie wiąże się również z ryzykiem popadnięcia w siecioholizm. Zjawisko to polega na korzystaniu z internetu w dysfunkcyjny sposób. Osoba dotknięta tym problemem odczuwa wewnętrzny przymus bycia online i nie kontroluje czasu spędzanego w sieci. Często zaniedbuje inne aspekty życia, np. obowiązki zawodowe, szkolne czy domowe, a także znacząco ogranicza kontakty z innymi ludźmi w realnym świecie.

9. Upublicznianie prywatnych zdjęć, nagrań i wiadomości

Korzystając w nierozważny sposób z internetu, można również narazić się na utratę dobrego wizerunku. Istnieje niebezpieczeństwo, że zamieszczane w sieci prywatne fotografie czy nagrania wideo zostaną upublicznione bez zgody ich właściciela.

10. Fałszywe sklepy internetowe

Spora część użytkowników internetu dokonuje zakupów w sklepach online oraz serwisach aukcyjnych. Jest to rozwiązanie wygodne i pozwalające zaoszczędzić czas. W sieci działa jednak wielu oszustów, którzy zakładają fałszywe sklepy oraz zamieszczają oferty wprowadzające w błąd. Klient będący ich ofiarą po wniesieniu zapłaty nie otrzymuje zamówionego towaru.

SPEED-NET Arkadiusz Broniecki, 43-300 Bielsko-Biała,
ul. Jana Matejki 3
Telefon +48 33 475 25 25, 33 475 20 00
www.speed-net.com.pl, email: biuro@speed-net.com.pl

Sposoby zapobiegania niebezpieczeństwu w sieci:

1) zachować czujność – podczas korzystania z sieci nie klikać w linki od nieznanych nadawców i wyskakujące reklamy ani nie pobierać załączników z przesyłanych przez nich wiadomości,

2) chronić komputer za pomocą programu antywirusowego – koniecznie z funkcją ochrony sieciowej w czasie rzeczywistym.

3) pamiętać o regularnych aktualizacjach – zarówno systemu operacyjnego, antywirusa, przeglądarki, jak i innych aplikacji,

4) tworzyć trudne do rozszyfrowania hasła – składające się z wielu liter, cyfr oraz znaków specjalnych,

5) pobierać pliki z wiarygodnych źródeł – legalnie działających serwisów i cieszących się dobrą opinią wielu użytkowników.

6) bezpieczny protokół HTTPS - starć się wchodzić wyłącznie na strony, które są odpowiednio zabezpieczone przed atakami z zewnątrz. Jeżeli strona nie ma protokołu https zapisanego przed swoim adresem, można wykorzystać wtyczkę HTTPS Everywhere, która wymusza połączenie tego typu. Dotyczy to zwłaszcza tych stron, na których planujesz podać swoje dane.

7) VPN to rozwiązanie pozwalające na bezpieczne przesyłanie danych bez pokazywania lokalizacji.