

Jak bezpiecznie korzystać z Internetu i nie stać się ofiarą cyberprzestępcy

Internet – jako ogólnosiwiatowy system połączeń między komputerami – niesie za sobą wiele zagrożeń, z których nie zawsze jako korzystający zdajemy sobie sprawę. Tak jak przy wykonywaniu każdej czynności, tak samo korzystając z Internetu należy zachować ostrożność, by skutecznie ograniczać ryzyko stania się ofiarą cyberprzestępcy. Bezpieczeństwa w sieci internetowej nie można zdecydowanie ograniczyć jedynie do ochrony technologicznej.

Cyberprzestępcy podejmują się najróżniejszych sposobów w tym zwykłej socjotechniki w celu nakłonienia użytkownika Internetu do wykonania czynności, które ujawnią informacje o hasłach i stosowanych przez niego zabezpieczeniach, wykorzystując zainfekowane załączniki, fałszywe strony www i wiadomości e-mail, łudząco podobne do prawdziwych.

Aby zminimalizować ryzyko stania się ofiarą cyberprzestępcy należy w szczególności:

- 1) korzystać z e-usług lub portali internetowych tworząc długie i skomplikowane hasła dostępu – co najmniej ośmioznakowe zawierające małe, wielkie litery, znaki specjalne lub cyfry. Dobrym rozwiązaniem jest korzystanie z tzw. haseł frazowych poprzez np zestawienie pięciu wyrazów niepowiązanych ze sobą i nieoddzielonych spacją
- 2) dokonywać cyklicznych zmian haseł (średnio co 60 dni) oraz niezwłocznie w przypadku podejrzenia, że hasło mogło zostać ujawnione osobie nieuprawnionej,
- 3) pliki zawierające Twoje dane osobowe przysyłać innym użytkownikom sieci za pośrednictwem poczty email w formie zabezpieczonej hasłem, natomiast samo hasło przekazywać innym środkiem przekazu np. wiadomością sms, bądź podczas rozmowy telefonicznej po uprzednim zweryfikowaniu tożsamości adresata,
- 4) logując się na nieznane strony internetowe zwracać uwagę na poziom bezpieczeństwa danej strony – symbolami znaczącymi o bezpieczeństwie są m.in. „zielona kłódka” informująca, że strona jest wyposażona w sprawdzony i ważny certyfikat lub element „https”, oznaczający, że strona jest szyfrowana. Dla pewności należy „kliknąć” na ikonkę kłódki i sprawdzić, czy właścicielem certyfikatu jest wiarygodny właściciel,
- 5) w przypadku spostrzeżenia w adresie strony internetowej czerwonej kłódki ze znakiem krzyżyka,

zachować szczególną ostrożność i powstrzymać się od wprowadzania danych, gdyż istnieje możliwość, iż ktoś podszywa się pod daną witrynę, aby przechwycić cenne informacje,

6) unikać umieszczania w tzw. publicznej chmurze plików i informacji zawierających wrażliwe dane na Twój temat;

7) unikać logowania się na swoje konta internetowe przy pomocy publicznego wifi lub na publicznych komputerach,

8) uważać na strony internetowe, które wymagają instalacji oprogramowania - w takim przypadku najlepiej uprzednio przeskanować wszystkie programy pobierane z internetu za pomocą aktualnego oprogramowania antywirusowego,

9) unikać otwierania nieznanymi linków i załączników w wiadomościach e-mail;

10) unikać korzystania ze stron internetowych, w szczególności o charakterze przestępczym, hackerskim, pornograficznym lub innym zakazanym przez prawo (na większości stron tego typu może być zaimplementowany złośliwy kod, który może automatycznie zainfekować system operacyjny komputera w sposób niewidoczny dla użytkownika) oraz zwracać uwagę na reklamy wyświetlane na innych stronach internetowych które są przeglądane.

11) zwracać uwagę i upewnić się czy osoba, z którą nawiązywany jest kontakt jest tym, za kogo się podaje;

12) zwracać uwagę na wiadomości z prośbą o podanie szczegółów konta, gdyż instytucje finansowe oraz urzędy unikają takich sytuacji ze względów bezpieczeństwa;

13) zainstalować oprogramowanie antywirusowe i na bieżąco je aktualizować;

14) korzystać z najnowszych i zaktualizowanych wersji przeglądarek internetowych;

15) zapewnić, by system operacyjny posiadał włączoną funkcję automatycznych aktualizacji i instalować wszelkie aktualizacje zaraz po ich udostępnieniu przez producenta.

Bieżące informacje na temat złośliwych kampanii lub zagrożeń bezpieczeństwa można znaleźć na

stronie NASK-u na Facebooku https://plpl.facebook.com/NASKpl/?hc_location=ufi

Zachęcamy również do śledzenia informacji publikowanych na poniższych stronach:

- <https://www.cert.pl/publikacje/>
- <https://www.cert.pl/ouch/>

Dodatkowe informacje można uzyskać pod adresem mailowym :

informatyk@wohyn.home.pl