20 wskazówek jak bezpiecznie korzystać z internetu

w jaki sposób zachować bezpieczeństwo w sieci, unikając pułapek zastawionych przez cyberprzestępców. Przede wszystkim należy przestrzegać kilkunastu podstawowych zasad.

Zagrożenia internetowe na początku stanowiły niewielką grupę wirusów stworzonych przez osoby szukające sławy i rozgłosu. Obecnie jest to kwitnący, złożony podziemny rynek zorganizowany przez przestępców, których jedynym celem jest osiągnięcie jak największych zysków. Ich działalność przynosi firmom i osobom indywidualnym miliardy dolarów strat każdego roku.

Poniżej przedstawiamy 20 wskazówek, których stosowanie pozwoli ochronić się przed zagrożeniami internetowymi i coraz częstszym problemem wycieku danych oraz umożliwi bezpieczniejsze korzystanie z komputera.

ZALECENIA OGÓLNE DOTYCZĄCE BEZPIECZEŃSTWA

- Oprogramowanie zabezpieczające powinno być zawsze uruchomione i aktualne, zwłaszcza gdy używa się laptopa w niechronionej sieci bezprzewodowej na lotniskach, w kawiarniach i w innych miejscach publicznych.
- Należy zainstalować oprogramowanie, które zapewni ochronę podczas poruszania się w internecie lub pobierania plików bezpośrednio do komputera.
- Oprogramowanie zabezpieczające przed zagrożeniami z sieci powinno zapewniać ochronę poczty elektronicznej, sieci równorzędnych (P2P) i wszystkich aplikacji dla użytkowników indywidualnych oraz generować w czasie rzeczywistym ostrzeżenia dotyczące ruchu przychodzącego i wychodzącego.
- Należy stosować najnowsze technologie, które sprawdzają wiarygodność i bezpieczeństwo serwisów internetowych przed ich otwarciem w przeglądarce.
- Należy używać najnowszej wersji przeglądarki internetowej oraz zainstalować wszystkie dostępne poprawki zabezpieczeń.
- Należy używać przeglądarki z wtyczką blokującą skrypty.
- Należy sprawdzić, jakie zabezpieczenia są oferowane przez sieć operatora internetu.
- Jeżeli wykorzystywany jest system operacyjny Microsoft Windows, należy włączyć funkcję automatycznych aktualizacji i instalować wszelkie aktualizacje zaraz po ich udostępnieniu przez firmę Microsoft.
- Należy zainstalować zapory i oprogramowanie wykrywające włamania oraz zabezpieczające przed szkodliwym oprogramowaniem i programami szpiegującymi. Programy te powinny być zawsze uruchomione i regularnie aktualizowane.
- Należy upewnić się, że oprogramowanie zabezpieczające jest aktualne.

POCZTA ELEKTRONICZNA

- Należy używać oprogramowania zabezpieczającego przed spamem dla każdego posiadanego adresu e-mail.
- Należy wystrzegać się nieoczekiwanych lub podejrzanych wiadomości e-mail, bez względu na to, kto jest nadawcą. W przypadku takich wiadomości nie należy nigdy otwierać załączników ani klikać znajdujących się w nich łączy.
- Podejrzane wiadomości należy zgłaszać odpowiednim władzom.

- Jeżeli ufamy nadawcy, należy przeskanować załączniki odpowiednim programem przed ich otwarciem. Jeżeli taka wiadomość zawiera adres URL i jest on niezbyt długi, należy wpisać go ręcznie w odpowiednie pole przeglądarki.
- Należy uważać na wiadomości z prośbą o podanie szczegółów konta (banki i inne instytucje finansowe bardzo rzadko proszą o podanie takich szczegółów drogą elektroniczną).
- Nie należy przesyłać pocztą elektroniczną informacji dotyczących danych finansowych.

PRZEGLĄDANIE STRON INTERNETOWYCH I POBIERANIE PROGRAMÓW Z INTERNETU

- Należy korzystać z usług oceniających reputację stron, aby mieć pewność, że odwiedzany serwis internetowy nie stwarza żadnych zagrożeń.
- Należy uważać na strony internetowe, które wymagają instalacji oprogramowania. Należy skanować wszystkie programy pobierane z internetu za pomocą aktualnego oprogramowania zabezpieczającego.
- Należy zawsze czytać umowy licencyjne i przerywać proces instalacji, jeżeli razem z daną aplikacją mają być zainstalowane inne „programy".
- Nie należy podawać danych osobowych w przypadku nieprzewidzianego żądania informacji. Dane osobowe można podawać tylko w takich serwisach, w przypadku których przeglądarka wyświetla ikonę kłódki

Gdzie przeglądarki internetowa przechowuąe hasła do witryn?

FireFox ……
……
……

Google Chrome ……
……
……

Napisz przykład hasła:

…… ……

słabe hasło mocne hasło

Jak należy postępować gdy jest się obrażanym lub zastraszanym przez internet np.: na facebooku?

……
……
……
……
……
……
……
……