Bezpieczeństwo w Internecie

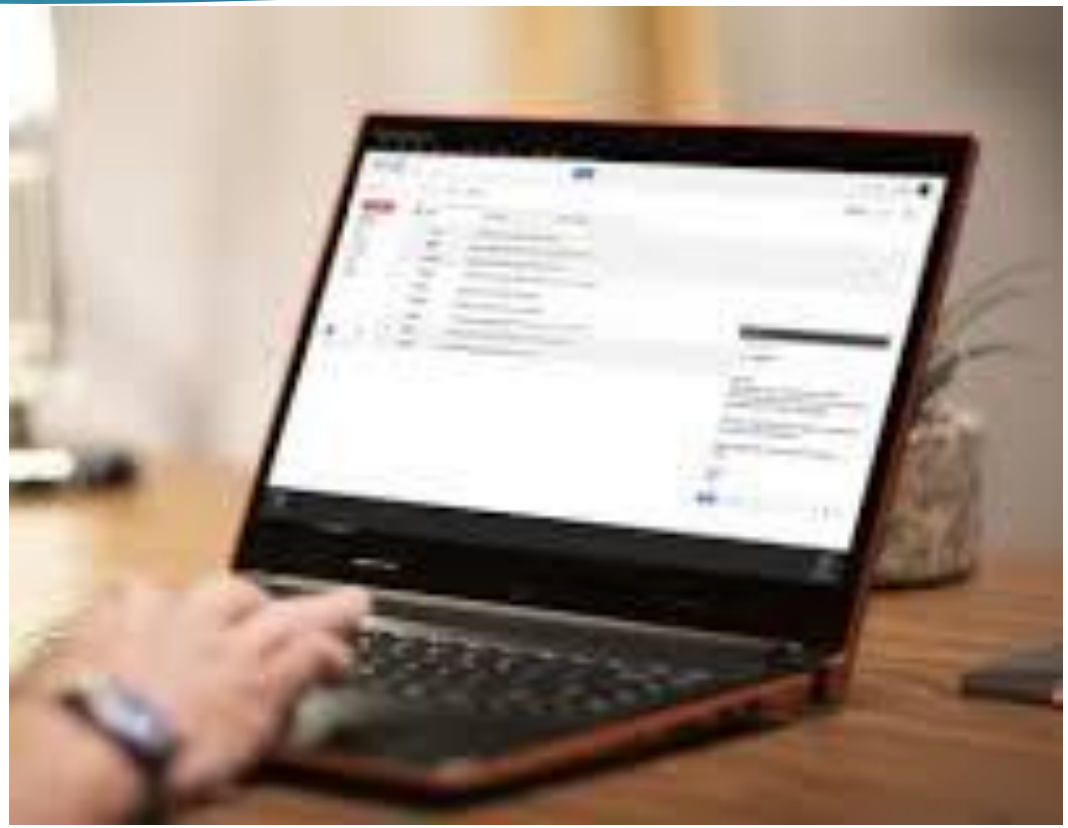
Sebastian Hanejko

Hasło to podstawa

- Hasła to Twoje podstawowe i w zasadzie najważniejsze zabezpieczenie. Twoje podstawowe i w zasadzie najważniejsze zabezpieczenie. Nie idź pod tym względem na łatwiznę i na przykład nie dodawaj wszędzie takiego samego hasła, np. daty urodzenia albo imienia swojego czworonoga. Silne hasło to zdecydowanie najlepsze zabezpieczenie.

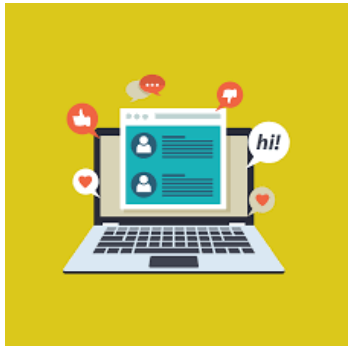
Zachowaj ostrożność wchodząc w nieznane linki

- Bardzo częstym sposobem atakowania prywatności i wyciągania danych są rozsyłane na skrzynki pocztowe wiadomości e-mail, zawierające dziwne załączniki lub proszące o kliknięcie w jakieś linki. To tak zwany **phishing.** Nie istnieje jeden i do tego 100-procentowo pewny sposób na obronę. Najlepiej po prostu uważać i nigdy ich nie otwierać. Znacznie bezpieczniejsze jest samodzielne wchodzenie na interesującą Cię stronę.



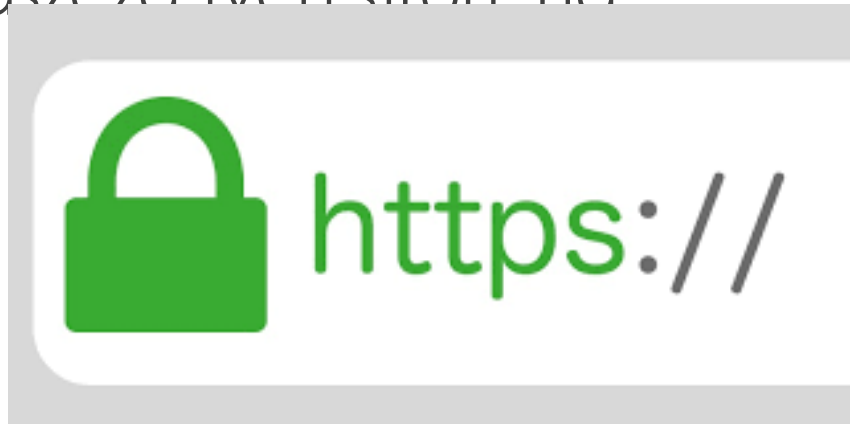
Bądź ostrożny przy nawiązywaniu nowych kontaktów przez Internet

- Należy być ostrożnym przy nawiązywaniu nowych kontaktów podczas "rozmów na żywo" prowadzonych przez Internet. Szczególnie dotyczy to umawiania się na spotkania z takimi osobami. Zdarza się, że mają one złe zamiary. Nie należy podawać swoich danych i do końca ufać otrzymywanym informacjom, gdyż mogą być nieprawdziwe(zwłaszcza wiek rozmówcy i intencje). Zachowując ostrożność, możemy uniknąć wielu zagrożeń i niebezpieczeństw, związanych z internetowymi znajomościami.



Bezpieczny protokół HTTPS

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

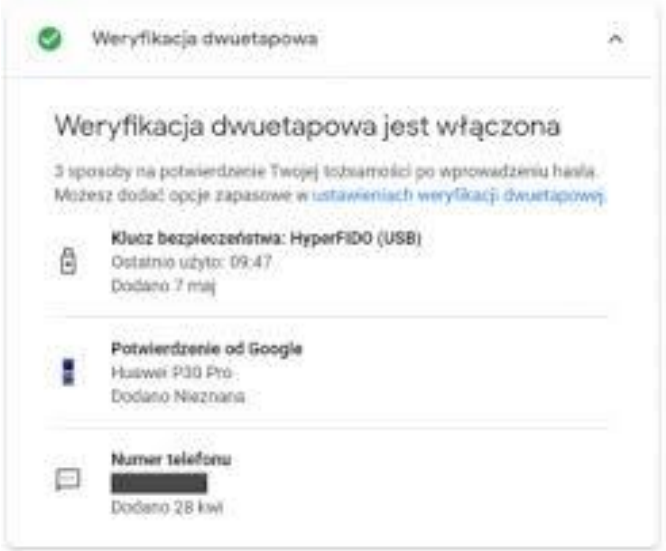


Tryb incognito

- Wykorzystanie trybu incognito nie rozwiązuje wszystkich problemów związanych z widocznością w sieci. Aktywności widzi na przykład dostawca Internetu. Wybranie tego trybu wpływa jedynie na brak zapisywania historii przeglądarki i nie pokazuje lokalizacji.

Weryfikacja dwuetapowa

Tam, gdzie konieczna jest weryfikacja, na przykład przy płatnościach internetowych, konieczna jest jej dwuetapowość. Czyli oprócz zalogowania się na danej stronie, ustaw sobie dodatkowo na przykład kod otrzymywany w wiadomości SMS. Potencjalnemu złodziejowi z dużym prawdopodobieństwem nie uda się wówczas dokonać zakupów bez Twojej woli.



Komunikatory szyfrujące w trakcie rozmów tekstowych

- Lubisz dużo pisać i to poprzez Internet najczęściej kontaktujesz się ze znajomymi? W takim razie wykorzystaj komunikator, który szyfruje przesyłane teksty. Przykładem takiego rozwiązania jest Signal. Możesz mieć wówczas pewność, że treści nie wpadną w niepowołane ręce.

Wylogowywanie się i używanie pseudonimów

- Zawsze po skończonej pracy powinno się wylogowywać z danej strony oraz z komputera. Dotyczy to zwłaszcza korzystania z komputera w miejscu publicznym, gdzie dostęp do niego mogłyby mieć niepowołane osoby. Inaczej stać się można ofiarą żartu albo w dużo poważniejszej sytuacji, utracić swoje dane. Dotyczy to również korzystania z pseudonimów, które nie pozwalają na łatwą identyfikację swojej osoby oraz podawania w Internecie jak najmniejszej ilości informacji na swój temat. Lepiej pozostawić je dla osób znanych w realnym świecie.

Korzystaj z ochrony przed wirusami

- Bezpieczeństwo w sieci w dużym stopniu zależy od stanu urządzenia, z którego korzysta internauta. Dlatego na każdym komputerze, laptopie czy smartfonie należy zainstalować oprogramowanie przeciwdziałające wirusom i programom szpiegującym, które pozwala obniżyć ryzyko zainfekowania sprzętu. Dobrze, jeśli oferuje ono ochronę w czasie rzeczywistym, czyli na bieżąco monitoruje bezpieczeństwo urządzenia i sygnalizuje ewentualne próby ataku.

Używaj oryginalnego systemu operacyjnego oraz legalnych wersji programów

- Tylko legalnie działające oprogramowanie jest bieżąco udoskonalane przez producentów i możliwe jest jego uaktualnianie do nowszych wersji. Dzięki temu mogą być usuwane luki w bezpieczeństwie, które umożliwiają hakerom przeprowadzanie niebezpiecznych ataków.

Systematycznie aktualizuj oprogramowanie

- Aby program antywirusowy mógł skutecznie wywiązywać się ze swoich zadań, trzeba go systematycznie aktualizować – podobnie zresztą jak system operacyjny. Tylko w ten sposób użytkownik może na bieżąco eliminować luki w oprogramowaniu, czyli „furtki”, przez które hakerzy mogą dostać się do jego urządzenia.

Nie wykorzystuj hot- spotu do wykonywania ważnych zadań

- Publiczna sieć Wi-Fi, a więc ta dostępna w sieciach handlowych, pojazdach komunikacji miejskiej, kawiarniach itp., nie jest bezpieczna i wiąże się z dużym ryzykiem „podejrzenia" przesyłanych danych przez cyberzłodzieja. Z konta bankowego, e-maila czy innych serwisów wymagających zalogowania, należy korzystać wyłącznie w ramach sieci „prywatnych", czyli tych zabezpieczonych hasłem.

Pobieraj pliki i programy jedynie z zaufanych źródeł

- Jednym z najczęstszych powodów infekcji komputera szkodliwym oprogramowaniem jest pobieranie plików z nielegalnie działających stron. Jeżeli zastanawiasz się, jak być bezpiecznym w Internecie, to w żadnym wypadku nie korzystaj z serwisów typu torrent do pobierania filmów. Ściągaj pliki jedynie z zaufanych i legalnych źródeł, których wiarygodności jesteś pewien.

Twórz kopie zapasowe i zapisuj je w różnych miejscach

- W wyniku działań cyberprzestępców możesz bezpowrotnie utracić wszystkie cenne dane zapisywane na dysku komputera. Dlatego warto pamiętać o systematycznym wykonywaniu kopii zapasowych. Plików backup nie należy przechowywać na komputerze, lecz na zewnętrznych nośnikach danych (np. pendrive) oraz w wirtualnej chmurze.

Co jeszcze warto wiedzieć?

- Jak widać, aby zapewnić sobie możliwie najwyższy poziom bezpieczeństwa w sieci, nie trzeba posiadać zaawansowanej wiedzy czy narzędzi informatycznych. Wystarczy zachować czujność i zdrowy rozsądek, a przy tym stosować się do elementarnych zasad bezpieczeństwa i korzystać z odpowiedniego oprogramowania ochronnego.

Dziękuję za uwagę

ŹRÓDŁA

- Dziennikprawny.pl
- Benchmark.pl
- Pl.ccm.net
- Arte24.pl
- Ixion.pl
- Wirtualnemedia.pl
- Evelsoft.pl
- Netia.pl
- Benchmark.pl
- p.wikipedia.org
- Blitrix24.scan-it.pl