



Gabriela Kurowska
specjalista ds. informacji | wirtualna asystentka

#bezpieczeństwosieci

czyli na co uważać w Internecie

- dane osobowe
- hasła
- wylogowanie
- śledzenie użytkownika
- wyszukiwarki
- wysyłanie wiadomości
- wifi
- publiczny komputer
- https
- aplikacje
- używaj blokady
- nie pożyczaj smartfona



#bezpieczeństwosieci

Dane osobowe. Jeśli nie musisz ich podawać — nie rób tego. Im mniej informacji jest o Tobie w sieci, tym trudniej się pod Ciebie podszyć. Do różnych usług i serwisów warto się logować, podając nick, czyli pseudonim. Nie należy podawać też miejsca zamieszkania, a w szczególności numeru PESEL w zestawieniu z np. numerem dowodu osobistego.

Hasła. Używaj haseł trudnych do zapamiętania przez osoby postronne. Dobre hasło NIE jest ani numerem telefonu, numerem PESEL czy krótkim wyrażeniem np. misiek1234. Silne, dobre hasło jest zbudowane z małych i wielkich liter, cyfr 0-9, oraz znaków specjalnych np. % czy # i zawiera co najmniej 10-12 znaków (im więcej tym lepiej).

Hasła i danych do logowania nie należy **nigdzie zapisywać ani nikomu podawać**. Warto też używać różnych haseł do różnych serwisów. Szczególnie ważne jest osobne hasło do bankowości online. Hasła należy też regularnie zmieniać!



#bezpieczeństwosieci

Sporym ułatwieniem i zabezpieczeniem jest korzystanie z aplikacji przechowującej hasła. Na przykład Microsoft Authenticator posiada opcję tworzenia skomplikowanych haseł. Oprócz tego ma też funkcję, z której warto korzystać - uwierzytelnianie dwuskładnikowe. Co to? Sprawdź dokładnie na infoblogerka.pl, ale w skrócie to podwójne logowanie. Po wpisaniu loginu i hasła do danego serwisu trzeba je potwierdzić/autoryzować w osobnej aplikacji lub z pomocą kodu wysłanego SMSem.

Po zakończonej pracy z danym serwisem (np. bankowym) pamiętaj o tym, żeby się **wylogować**, w szczególności, jeśli pracujesz na komputerze, z którego korzysta więcej osób lub komputer jest do dyspozycji ludzi w miejscu publicznym.

Zainstaluj wtyczki, które **zapobiegają śledzeniu Twojej aktywności** w sieci oraz zablokują wyświetlające się reklamy. np. AdBlocker czy Privacy Badger.



#bezpieczeństwowsieci

Szyfruj wysyłane wiadomości — korzystaj np. z Mozilli ThunderBird z wtyczką Enigmail. Jeśli korzystasz z mediów społecznościowych, możesz użyć opcji "tajna konwersacja" na Facebooku lub korzystać z szyfrowanego czatu WhatsApp.

W miejscach publicznych **nie** używaj niezabezpieczonego hasłem WiFi. Nie rób przez takie połączenie żadnych operacji na koncie bankowym, transakcji, przelewów. Twoje dane, w tym te do logowania mogą zostać wykradzione, a wraz z nimi środki zgromadzone na koncie bankowym.

Jeśli korzystasz z publicznego komputera np. w bibliotece, **nie korzystaj z opcji "zapamiętaj hasło"** w przeglądarce. Korzystaj z trybu "okna incognito" albo tzw. "trybu prywatnego". Dzięki temu, po zamknięciu okna przeglądarki usunięte zostaną tzw. ciasteczka oraz cała historia wyszukiwania i odwiedzonych stron.

Korzystaj z **HTTPS** - (Hypertext Transfer Protocol Secure) – szyfrowana wersja protokołu HTTP). Można do tego użyć wtyczki do Firefoxa lub Chrome HTTPS Everywhere.



#bezpieństwowsieci

Jeśli korzystasz z aplikacji na smartfonie, przeczytaj przed instalacją, **do jakich danych żądają dostępu**. Prosta aplikacja latarki nie powinna żądać dostępu do Twojej lokalizacji.

Ustaw hasło blokady do telefonu i komputera. Zasady tworzenia haseł patrz pkt. 2. Hasło cyfrowe do telefonu nie powinno być datą urodzenia, a w przypadku zapomnienia hasła należy ustawić drugą metodę awaryjną.

Nie **użyczaj** nikomu obcemu swojego smartfona bez nadzoru, szczególnie jeśli masz na nim aplikację bankową lub mObywatel.

Jeśli zadzwoni do Ciebie (nawet z numeru telefonu banku) osoba podająca się za jego pracownika i poprosi o zainstalowanie jakiegoś oprogramowania, w celu rozwiązania problemu (często fikcyjnego), **nie rób tego**. Programy typu AnyDesk pozwalają na **zdalne przejęcie kontroli** nad komputerem. W takiej sytuacji rozłącz się i sam zadzwoń do swojego banku, aby upewnić się, czy ta osoba naprawdę tam pracuje.



#bezpieczeństwowsieci

Korzystaj z firewalla, czyli zapory ogniowej. Jest to oprogramowanie, które bada, filtruje dane przychodzące i wychodzące z danego komputera, aby chronić go przed atakiem hakerów.

Zainstaluj na swoim komputerze program antywirusowy i regularnie aktualizuj bazę danych o zagrożeniach. Pamiętaj, nie instaluj więcej niż jednego programu antywirusowego, żeby nie sabotowały swoich działań i nie zwalczały się nawzajem, zamiast szukać zagrożenia z zewnątrz.

Korzystaj z wyszukiwarek, które nie zbierają o Tobie informacji np. DuckDuckGo. Śledzenie służy do personalizowania wyników wyszukiwania oraz wyświetlanych reklam.

Nie klikaj w linki, które przychodzą mailem lub SMSem z nieznanych Ci adresów mailowych czy numerów telefonów. Uważaj na wiadomości informujące o konieczności dopłaty za dostawę zamówionej paczki lub zaległości w opłatach za gaz czy prąd. Jeśli przypadkiem klikniesz taki link, nie podawaj tam żadnych informacji.



#bezpieczeństwowsieci

Jeśli dany serwis umożliwia taką opcję korzystać z uwierzytelniania dwuskładnikowego, czyli włącz konieczność potwierdzenia logowania do danego serwisu drugą metodą - np. kodem z Smsa czy z pomocą dodatkowej aplikacji.

Korzystaj z **legalnych** kopii programów. Nie korzystaj z torrentów i niezgodnych z prawem źródeł oprogramowania. To, że coś jest np. za darmo, może być pierwszą i ostatnią zaletą. Taka nielegalna kopia programu może być zawirusowana, a to prosta droga do utraty kontroli nad swoją prywatnością, danymi, zdjęciami, pieniędzmi i wszystkim, do czego ma dostęp Twój komputer.



infobloggerka.pl

Dziękuję Ci za poświęcony czas na przeczytanie tego ebooka.

Jeśli na przykład jesteś nauczycielem, możesz go wydrukować i powiesić w ważnym miejscu w klasie lub rozdać uczniom.

Jestem zwolenniczką **oszczędzania** drzew, papieru i innych materiałów, dlatego nie użyłam w nim wielkich zdjęć w tle. A Ciebie proszę, wydrukuj go w formie 2 strony na jednej lub dwustronnie i bez tej strony. Jeśli nie wiesz jak to zrobić — napisz do mnie, postaram się pomóc. Większość drukarek powinna mieć tę opcję. Możesz go także pobrać i wysłać mailem.

Zajrzyj na www.infobloggerka.pl i zobacz jakich innych zadań się podejmuję oraz po więcej treści jak ta.