JAK BEZPIECZNIE KORZYSTAĆ Z INTERNETU?

Internet to współcześnie podstawowy środek do komunikacji, biznesu, rozrywki. Korzysta z niego prawie każdy, jednak nie wszyscy wiedzą w jaki sposób poruszać się po nim bezpiecznie. Nawet użytkownicy, którzy myślą, że są świadomi, często popełniają błędy i stają się ofiarami różnorodnych ataków. Dlatego ten tekst powinien przeczytać każdy. Sprawdź swoją wiedzę na temat bezpiecznego korzystania z internetu i zobacz, czy w artykule znajdują się jakieś informacje, o jakich nie miałeś pojęcia.

Jak bezpiecznie korzystać z internetu? Podstawowe zasady!

Przede wszystkim zadbaj o sprawdzony system antywirusowy. To gwarancja tego, że Twoje dane będą chronione, a niebezpieczne oprogramowanie nie dostanie się do zasobów Twojego komputera. Ataki pochodzą z różnych źródeł: mail, serwisy społecznościowe, strony internetowe. Odpowiednie zabezpieczenie sprawi, że nie będziesz narażony na działania hakerów, którzy chcą wykraść Twoje dane.

1. Nie podawaj danych osobowych

Podstawą bezpieczeństwa w sieci jest ochrona swoich danych. Dlatego nie podawaj nikomu numeru PESEL, danych do logowania oraz informacji osobistych. Nawet, jeśli ufasz danej osobie, to nie przekazuj takich danych przez internet. Zarówno poczta, jak i konta społecznościowe mogą zostać przejęte przez oszustów. Jeśli uważasz, że odpowiednio chronisz się podczas korzystania z internetu, to nigdy nie masz pewności jak robią to inne osoby.

2. Zadbaj o hasła

Wciąż wiele osób w zły sposób przechowuje swoje hasła. Nigdy nie zapisuj ich na swoim dysku, mailu, a nawet w chmurze (chyba, że jest chroniona przez antywirus). Możesz mieć je zapisane w notesie lub wykorzystać do ich przechowywania specjalistyczne programy. Niezwykle istotne jest także to, aby hasła się nie powtarzały. Jeśli na przykład robisz zakupy w jakimś sklepie internetowym, a hasło do niego jest takie samo, jak do maila, banku i innych kont, to jesteś bardzo narażony na przechwycenie tych danych. Wystarczy, że sklep online będzie miał wyciek danych – hakerzy wykorzystają je do tego, aby Cię okraść. Ponadto konstruuj niezwykle trudne hasła, których złamanie jest bardzo ciężkie. Nie powinny one

składać się ze słów słownikowych, muszą mieć różne znaki, a także cyfry oraz duże i małe litery. Każde hasło powinno być długie – im dłuższe, tym trudniej je rozszyfrować.

3. Włącz dwuskładnikową autoryzację

Aby dodatkowo chronić swoją sieć, warto zastosować wieloskładnikową autoryzację wszędzie tam, gdzie jest to możliwe. Jest to dodatkowa warstwa zabezpieczeń, która wymaga od użytkownika np. podania dodatkowego kodu, czy potwierdzenia swojej tożsamości poprzez dane biometryczne. Takie rozwiązanie ogranicza ryzyko włamania się na konto danej osoby, nawet jeśli jej hasło zostało rozszyfrowane.

4. Zwracaj uwagę na strony, jakie odwiedzasz

Zawsze weryfikuj czy dana witryna posiada zieloną kłódkę. Ponadto sprawdzaj czy adres URL jest poprawny. Oszuści często tworzą strony niezwykle podobne do oryginalnych, których adres delikatnie się różni. Oszuści cyfrowi często tworzą witryny, które wyglądają identycznie, jak strony banków i wyłudzają dane osób, które zrobią literówkę w adresie. To jednak nie jest jedyny sposób, aby przez pomyłkę przekazać dane do hakerów. Możesz kliknąć w link do płatności na stronie internetowej z ogłoszeniami, przejść do fałszywej witryny przez wiadomość e-mail albo SMS. Dlatego zawsze wpisuj adres banku ręcznie.

5. Uważaj na publiczne sieci

Publiczne sieci wifi są wygodne. Będąc w centrum handlowym wiele osób chętnie sprawdzi pocztę, czy popracuje przebywając w kawiarni. Jednak otwarte sieci internetowe są łatwym sposobem na atak hakerski. Zabezpieczenia takich połączeń można złamać niezwykle szybko. Dlatego, jeżeli korzystasz z internetu w miejscu publicznym, to zawsze korzystaj przy tym z VPN.

6. Uważaj na spam i phishing

Wiadomości mailowe to źródło wielu ataków. Niekiedy przypominają maile od operatora komórkowego, banku, firmy energetycznej. Zawierają faktury albo linki. Zawsze sprawdzaj takie wiadomości przed kliknięciem. Pierwszym krokiem powinno być przeskanowanie maila systemem antywirusowym (niekiedy dzieje się to automatycznie). Potem sprawdź adres mailowy, z którego otrzymałeś wiadomość. Następnie przeczytaj tekst i zobacz, czy nie ma on rażących błędów, na przykład gramatycznych. Nigdy nie wchodź w podejrzane linki i nie pobieraj załączników. Zawsze możesz skontaktować się z nadawcą telefonicznie, aby upewnić się, że wiadomość pochodzi od niego.

7. Dokonuj aktualizacji programów

Mnóstwo hakerów tworzy oprogramowanie, które dostaje się na Twój komputer poprzez luki w różnych aplikacjach oraz programach. Dlatego tak ważne jest to, aby na bieżąco aktualizować wszystkie programy i posiadać ich najnowsze wersje. W ten sposób uchronisz się przed oprogramowaniem, które wykorzystuje luki.

8. Bądź ostrożny podczas zawierania znajomości

Coraz powszechniejsze jest korzystanie z internetu w celu nawiązywania nowych znajomości. Fora internetowe, grupy dyskusyjne, społeczności na Facebooku, aplikacje randkowe. To wszystko narzędzia, dzięki którym można zyskać przyjaciół. Jednak są to miejsca, w których jest mnóstwo oszustów, jacy chcą wyłudzić od Ciebie dane. Mogą przesłać link lub plik ze szkodliwym oprogramowaniem lub podchwytliwie nakłonić Cię do tego, abyś sam wysłał te dane w wiadomości. Dlatego bądź uważny i zawsze zwracaj uwagę na próby wyłudzenia danych oraz nie klikaj w podejrzane linki.

9. Ostrożnie korzystaj z mediów społecznościowych

Media społecznościowe to platformy, na których publikujemy wiele informacji na swój temat. Przy tych działaniach także warto zachować ostrożność. Przede wszystkim dobrze jest tak skonfigurować swoje ustawienia prywatności, aby wgląd w nasze profile miały tylko osoby zaufane. Warto również bardzo ostrożnie dzielić się faktami ze swojego życia oraz fotografiami. Należy mieć na uwadze to, że raz udostępniona w sieci informacja pozostaje w niej na zawsze.

10. Edukuj swoją rodzinę

Jeśli jesteś odpowiedzialny i stosujesz wszystkie zasady bezpieczeństwa, nie oznacza to, że Twoi domownicy robią dokładnie to samo. Dlatego rozmawiaj z nimi o bezpieczeństwie w internecie.

Bezpieczne korzystanie z internetu wymaga uważności i weryfikacji wielu kwestii. Właśnie dlatego należy zadbać o oprogramowanie antywirusowe, które będzie chroniło Cię przed atakami, których nie możesz być świadomy. Pamiętaj, aby zawsze tworzyć kopię zapasową – jeśli stracisz dane w wyniku ataku hakerskiego, to zawsze będziesz mógł je odzyskać. Jeśli korzystasz z internetu głównie na telefonie to co jakiś czas sprawdzaj zainstalowane aplikacje, skanuj go także programem antywirusowym na telefon.