Bezpieczeństwo w sieci.

Internet to z pewnością jeden z najważniejszych wynalazków współczesnego świata. Świadczy o tym choćby ilość użytkowników, która liczona jest w miliardach czy fakt, że bez internetu nie funkcjonowałoby wiele dziedzin życia. Jednocześnie jednak warto pamiętać, że internet niesie ze sobą wiele zagrożeń – sieć nie jest w pełni kontrolowana, dlatego nie ma tu miejsca na jakiekolwiek zaniedbania ze strony użytkowników. Niejednokrotnie w mediach pojawiają się informacje o kradzieżach danych, przemocy wirtualnej i innych negatywnych zjawiskach, na które mogą być narażone osoby korzystające z internetu. Wiele osób wychodzi z założenia, że zagrożenia ich nie dotyczą, ponieważ w wolnej chwili przeglądają jedynie witryny internetowe lub kontaktują się ze znajomymi – takie podejście nie jest właściwe, ponieważ każdy z nas jest potencjalną ofiarą wirtualnych zagrożeń.

Wśród głównych niebezpieczeństw, które mogą czyhać na użytkowników sieci, wymienić można zagrożenie złośliwych oprogramowaniem i wirusami komputerowymi. Mogą one zablokować możliwość korzystania z urządzenia, a nawet pobrać poufne dane, takie jak dane osobowe czy namiary konta bankowego. W niektórych przypadkach złośliwe oprogramowanie mogą uzyskać dostęp do kamery urządzenia, przez co będzie śledziło konkretnego użytkownika lub ruch danej osoby w sieci. Choć programy chroniące przed wirusami komputerowymi są nieustannie unowocześniane, warto o nich pamiętać i dbać o jak najwyższy poziom zabezpieczeń.

Kolejne poważne zagrożenie w sieci to wyłudzanie i kradzież danych osobowych. Wystarczy raz udostępnić swoje poufne dane, aby stały się upublicznione w sieci – w ten sposób stają się również dostępne dla osób, które mogą wykorzystać je w różny sposób. Wiele osób lub grup wyłudza i wykorzystuje dane osobowe, tworząc i sprzedając specjalne bazy lub biorąc kredyty, do których wystarczy znajomość podstawowych danych. Warto pamiętać, aby w żaden sposób nie przesyłać swoich danych osobowych ani nie umieszczać ich w sieci, również podczas prywatnych rozmów.

Innym zagrożeniem, czyhającym przede wszystkim na młodszych użytkowników internetu, jest pornografia i wirtualna przemoc. Wszelkiego rodzaju wirtualne znajomości, korzystanie z serwisów matrymonialnych, dostępność serwisów z treściami pornograficznymi czy usługami dla dorosłych oraz wiele innych elementów stanowią ogromne zagrożenie dla dzieci. Z tego powodu rodzice powinni monitorować aktywność swoich dzieci w sieci oraz uświadamiać je o potencjalnych zagrożeniach. Jednym z najnowszych problemów w wirtualnym świecie jest tzw. hejt – jego ofiarą padają nie tylko dzieci, ale też dorośli, dlatego bardzo ważne jest jak najszybsze reagowanie na niewłaściwe zachowanie innych użytkowników internetu.

Internet niesie ze sobą o wiele więcej zagrożeń, jednak istnieje zestaw zasad, których przestrzeganie może ochronić użytkowników przed negatywnymi konsekwencjami korzystania z sieci.

Bezpieczeństwo w sieci – podstawowe zasady

- pamiętaj o tym, aby zawsze korzystać z aktualnego programu antywirusowego – wybieraj oprogramowania, które są sprawdzone. Warto również na bieżąco i regularnie skanować komputer pod kątem wirusów i złośliwego oprogramowania,
- twórz bezpieczne, skomplikowane hasła – nie wybieraj tych, które są łatwe do odgadnięcia. Zadbaj o to, aby mieć inne hasło do każdego portalu i profilu – dzięki temu nawet w sytuacji, kiedy Twoje hasło do jednego miejsca zostanie wykradzione, inne hasła pozostaną bezpieczne. Warto również korzystać ze specjalnych generatorów haseł, które pozwalają na stworzenie długich, bardzo skomplikowanych haseł zabezpieczających;
- zwracaj uwagę, czy witryna, z którą chcesz się połączyć, posiada certyfikat SSL – dzięki temu zyskasz pewność, serwer, z którym się łączysz, jest tym właściwym, a IP nie zostało podmienione. Dzięki certyfikatom SSL internetowe transakcje są o wiele bardziej bezpieczne – na przykład w sklepach internetowych;
- nie podawaj w internecie żadnych prywatnych danych – unikaj wszelkich ogłoszeń o pracę lub serwisów, wymagających podania numeru PESEL, numeru dowodu osobistego, adresu, nazwiska czy numeru telefonu;
- unikaj pobierania plików z niepewnych źródeł, na przykładu plików typu torrent;
- rozważ szyfrowanie dysku twardego – warto zrobić to zawczasu, aby w razie awarii komputera nie ryzykować, że ktoś niepożądany (na przykład w serwisie) uzyska dostęp do prywatnych danych;
- nie otwieraj podejrzanych wiadomości e-mail, nie pobieraj załączonych w nich plików oraz nie wchodź na strony z linków w takich wiadomościach – mogą one zawierać złośliwe oprogramowanie;
- unikaj nawiązywania relacji z osobami, których nie znasz – jeśli ktoś obcy zaprasza Cię do znajomych na portalu społecznościowym, bezpieczniej będzie odrzucić takie zaproszenie;
- uważaj na skrócone adresy URL – często mogą stanowić niebezpieczną pułapkę. Jeśli chcesz skorzystać ze skróconego linku, upewnij się, że został udostępniony przez osobę, którą znasz lub pochodzi z bezpiecznego źródła;
- dwukrotnie przemyśl, zanim pozwolisz aplikacji na uzyskanie dostępu do Twojej lokalizacji czy treści w telefonie. Ta sama zasada dotyczy korzystania ze stron internetowych – nie klikaj "Akceptuję" czy "Potwierdzam" za każdym razem, kiedy chcesz jak najszybciej dostać się na witrynę internetową. W ten sposób udzielasz zezwoleń na dostęp do wielu informacji – warto najpierw zapoznać się z regulaminem i dokładnie sprawdzić, co akceptujesz.

Biorąc pod uwagę, jak ważnym miejscem naszej aktywności stał się internet, warto stosować się również do zasad savoir vivre. Warto odnosić się do innych w taki sam sposób, w jaki robimy to na co dzień – z kulturą i szacunkiem. Co prawda internetowe kontakty często postrzegane są jako mniej istotne, przez co dochodzi do wielu negatywnych zjawisk, a nawet do cyberprzemocy. Odnoś się do innych grzecznie i reaguj, kiedy spotkasz się z hejtem. Jeśli dojdzie do kontaktu z osobą, która odnosi się do Ciebie niegrzecznie, nie kontynuuj rozmowy – dzięki temu zapewnisz sobie komfort psychiczny.

Bezpieczeństwo dzieci w internecie

Dzieci są szczególnie narażone na zagrożenia ze strony internetu. Bardzo ważne jest pilnowanie aktywności dziecka w sieci oraz reagowanie, kiedy zdarzy się coś niepokojącego. Wyjaśnij dziecku, co jest akceptowalne, a czego nie można tolerować. Obecnie coraz młodsze dzieci korzystają z internetu. Warto wykorzystać możliwości, jakie dają wszelkiego typu blokady rodzicielskie, na przykład przed stronami dla dorosłych. Jakiś czas temu Google zaprezentował YouTube Kids w Polsce – wersja popularnego serwisu stworzona została z myślą o dzieciach – ma ona ustrzec maluchów przed kontaktem z nieodpowiednimi treściami.

Regularnie przypominaj dziecku, aby informowało Cię za każdym razem, kiedy coś w sieci je zaniepokoi – dzięki temu zyskasz możliwość szybkiego zareagowania. Nie pozwól dziecku na nawiązywanie wirtualnych znajomości – jest to ogromne zagrożenie, w szczególności dla najmłodszych dzieci. Jednocześnie pamiętaj, że obecność dziecka w sieci jest nieunikniona – internet wykorzystywany jest między innymi w szkole, dlatego uświadamianie dziecka na temat potencjalnych zagrożeń jest najlepszym rozwiązaniem.

Solecka Dagmara