

Jak bezpiecznie korzystać z Internetu?

Internet daje nam wiele możliwości – od kontaktu z bliskimi, przez rozrywkę, zakupy, aż po rozwój biznesu. Niestety, wiąże się też z zagrożeniami, takimi jak cyberataki, kradzież danych osobowych czy próby wyłudzeń. Aby zwiększyć Twoje bezpieczeństwo w sieci, przygotowaliśmy dla Ciebie krótką listę zasad:

1. Zachowaj ograniczone zaufanie

Otrzymałeś wiadomość e-mail od nieznanego nadawcy? Znajomy na Facebooku lub WhatsApp wysłał Ci dziwny link albo prosi o pożyczkę? Kurier żąda opłaty za przesyłkę?

Jeśli coś budzi Twoje wątpliwości – **nie klikaj w linki, nie przysyłaj pieniędzy, nie pobieraj plików z nieznanymi źródłami**. Najpierw upewnij się, że wszystko jest w porządku.

Możesz to zrobić, np.:

- kontaktując się z firmą przez oficjalną infolinię,
- pisząc do znajomego innym kanałem,
- sprawdzając w wyszukiwarce adres e-mail, numer telefonu lub stronę – często znajdziesz ostrzeżenia o oszustwach.

Pamiętaj także, aby każdą podejrzaną wiadomość, link czy prośbę o płatność zgłaszać do wsparcia technicznego lub administratora IT usługi, z której korzystasz. Pozwoli Ci to zweryfikować, czy sytuacja jest bezpieczna, a jednocześnie pomożesz chronić innych użytkowników przed podobnymi oszustwami.

2. Korzystaj tylko ze stron z certyfikatem bezpieczeństwa

Bezpieczne strony mają certyfikat SSL. Sprawdzenie tego zajmie Ci mniej niż 3 sekundy! Upewnij się, że adres zaczyna się od **https://** (z literą „s” na końcu – jak „security”). Jeśli widzisz http://, strona nie jest w pełni zabezpieczona.

Tip: Jeśli nie widzisz całego adresu, kliknij w niego dwa razy – pojawi się pełna wersja.

3. Używaj silnych haseł i włącz dwuskładnikową autoryzację

Silne hasło to takie, które trudno odgadnąć. Unikaj prostych słów, sekwencji cyfr czy dat urodzenia. Twoje hasło powinno mieć:

- minimum 8 znaków,
- duże i małe litery,
- cyfry i znaki specjalne.

Nie używaj tego samego hasła w wielu miejscach!

Dwuskładnikowa autoryzacja (2FA) to dodatkowa warstwa ochrony – oprócz hasła musisz potwierdzić logowanie np. kodem SMS lub w aplikacji. Dzięki temu nawet jeśli ktoś pozna Twoje hasło, nie zaloguje się bez drugiego kroku.

4. Aktualizuj system i korzystaj z dodatkowej ochrony

Regularnie aktualizuj system, przeglądarkę i programy zabezpieczające. Aktualizacje naprawiają wykryte luki w zabezpieczeniach.

Warto też zainstalować antywirusa lub zaporę sieciową – to dodatkowa tarcza chroniąca Twój komputer i telefon przed zagrożeniami.