10 ZASAD CYBERBEZPIECZEŃSTWA

Zapoznaj się z dziesięcioma zasadami cyberbezpieczeństwa i poczuj się bezpiecznie w sieci.
Twoje bezpieczeństwo w sieci zaczyna się od małych decyzji każdego dnia.

1.

Chroń swoje dane osobowe

Ludzie pokazują zbyt wiele w Internecie, chwaląc się np. zdanym prawem jazdy lub nowym dowodem. Czy wiesz, że takie działania mogą mieć bardzo poważne konsekwencje? W ten sposób złodzieje bardzo szybko identyfikują swoją ofiarę, ponieważ mogą poznać numer PESEL, adres zamieszkania i inne dane, które następnie wykorzystują do działań przestępczych. Nie publikuj swoich danych w sieci i nie pomagaj cyberprzestępcom.

2.

Aktualizuj swój program antywirusowy

W każdej chwili możesz stać się ofiarą cyberataku. Zabezpiecz swoje urządzenia elektroniczne (komputer, tablet, smartfon) programem antywirusowym i regularnie go aktualizuj. Bądź o krok przed oszustami i nie daj się zaskoczyć.

3.

Zawsze ustawiaj silne hasła

Według najnowszych badań mniej niż połowa (48%) użytkowników Internetu stosuje silne hasła. Aby hasło było silne, musi być odpowiednio i długie i zawierać cyfry i znaki specjalne. Pomocne mogą okazać się gotowe generatory oraz tzw. menedżerowie haseł.
Nawet najsilniejsze hasło warto zmieniać co trzy miesiące. Tam, gdzie to możliwe – włącz m.in. opcję logowania dwuetapowego. Pamiętaj, że jest to pierwsza bariera, z jaką musi spotkać się cyberoszust, w trakcie próby włamania na Twoje konto. Spraw, by była twierdzą nie do zdobycia.

4.

Nie zapominaj o wylogowaniu się

Silne hasła mają sens tylko wtedy, gdy pamiętasz o wylogowaniu się! Ta czynność po zakończeniu pracy z danym systemem, aplikacją lub usługą powinna być Twoim naturalnym odruchem. Jeśli pozostajesz zalogowany/a dłużej niż potrzebujesz i zostawiasz przy tym sprzęt bez nadzoru, zapraszasz do nadużycia, włamania czy przejęcia konta.

5.

Zachowaj ostrożność używając bankowości elektronicznej

Przestrzegaj zasad bezpieczeństwa, jakich wymaga od Ciebie bank, gdy korzystasz z bankowości elektronicznej.
Kupując w sklepach internetowych, sprawdzaj, czy mają one szyfrowane połączenie – oznaczone kłódką i odpowiednim certyfikatem. Płać tylko z własnego komputera lub telefonu. Nie wchodź też na stronę banku z linku w wyszukiwarce, lecz wpisuj adres ręcznie. Tak samo postępuj z numerem konta odbiorcy przelewu. Jeśli osoba podszywająca się pod „bank" pyta Cię o hasła, czy też inne poufne dane, np. kod PIN do karty płatniczej, nie odpowiadaj! Na pewno nie jest to bank, który nigdy nie pyta o Twoje poufne dane i hasła! Zachowuj ostrożność, nie spiesz się i nie rozpraszaj.

6.

Nigdy nie odwiedzaj podejrzanych stron

Zanim wejdziesz na nieznaną Ci stronę internetową, upewnij się, że jest ona bezpieczna. Możesz w tym celu użyć wbudowanych narzędzi bezpieczeństwa przeglądarek internetowych, jednak najlepiej zastosuj dodatkowo zewnętrzne narzędzie do sprawdzania witryn. Warto również zweryfikować czy strona posiada certyfikat https. Chodzi o twoje bezpieczeństwo, dlatego pamiętaj – podejrzane strony i linki to także źródło wirusów.

7.

Uważaj na wiadomości i linki nieznanego pochodzenia

Nigdy nie otwieraj wiadomości i dołączonych do nich załączników z nieznanych źródeł. Zawsze weryfikuj linki, które chcesz otworzyć i upewnij się, że wiesz, dokąd one zaprowadzą. Najedź myszką na dowolny link, żeby zweryfikować adres URL, z którym link jest naprawdę powiązany. Trzeba mieć świadomość, że najczęściej to właśnie w załącznikach mogą być ukryte złośliwe oprogramowania, wirusy i wiele innych.

8.

Zawsze twórz kopię zapasową

Tworzenie kopii zapasowej danych, czyli tzw. „backup", to nic innego jak dodatkowe zabezpieczenie Twoich plików. Służy ono do odtworzenia oryginalnych danych w przypadku ich utraty bądź uszkodzenia.

9.

Uważaj na fake newsy

Cokolwiek czytasz – daj sobie czas na sprawdzenie źródła, autorów, datę publikacji, dokładną analizę tekstu i porównanie go z opiniami ekspertów. Cyberprzestępcy będą grać na Twoich emocjach oraz będą Tobą manipulować, produkując „fake newsy", którym łatwo uwierzyć.

10.

Pamiętaj – nigdy nie jest za późno na edukację

Zwracaj m.in. uwagę na komunikaty, jakie otrzymujesz od swojego banku na temat bezpieczeństwa. Chwila, którą poświęcisz na ich przeczytanie, może uchronić Cię w przyszłości przed utratą danych i pieniędzy.


CYBERLIGA
Korzystaj z aktualnego oprogramowania
Używaj uwierzytelniania dwuskładnikowego
Kapitan Antywir
Jak być bezpiecznym online?
Włączaj automatyczne aktualizacje
Zainstaluj oprogramowanie antywirusowe
Zadbaj o silne hasła: różne hasła do różnych kont, oparte na frazach
Sprawdzaj aplikacje przed pobraniem: oceny, twórcy, żądane dostępy
Zgłaszaj incydenty na www.incydent.cert.pl
EUROPEJSKI MIESIĄC CYBERBEZPIECZEŃSTWA
NASK
www.bezpiecznymiesiac.pl


PAŹDZIERNIK
#ECSM
#PomyślZanimKlikniesz
CHAT
PLAY