Warto wiedzieć...

Bezpieczeństwo w sieci czyli jak zadbać o siebie?

Po(d)ręcznik internauty

Nowe technologie mają wpływ na nasze życie. Należy jednak poznać współczesne zagrożenia, aby świadomie i bezpiecznie korzystać z sieci. Podpowiadamy, jak zadbać o siebie i zwiększyć swoje bezpieczeństwo oraz zyskać większą kontrolę nad danymi osobowymi w Internecie, aby nie stały się łatwym łupem przestępców.

1. ZADBAJ O ZRÓŻNICOWANE I SILNE HASŁA LOGOWANIA

Nie zaleca się zapamiętywania haseł w pamięci przeglądarki lub w aplikacji na urządzeniu.
Jeśli dowiesz się o wycieku danych z portalu, natychmiast zmień hasło dostępu;

2. DWUSKŁADNIKOWE ZABEZPIECZENIE KONTA

Samo hasło to często zbyt mało, aby ochronić dostęp do naszego konta np. w serwisie społecznościowym, banku, w sklepie internetowym czy w państwowej usłudze zdrowotnej. Warto do logowania dodać drugi składnik (np. kod przekazany przez email, sms), który dodatkowo chroni nasze konto przed dostępem osób niepowołanych. W ten sposób znacznie podniesiemy poziom bezpieczeństwa tego konta;

3. DOPASUJ USTAWIENIA PRYWATNOŚCI KONTA

Sprawdź domyślne ustawienia prywatności konta w mediach społecznościowych. Ustaw je tak, aby dostęp do prywatnych informacji, danych osobowych, zdjęć, miały wyłącznie zaufane osoby. Rozważ także, czy Twój profil powinien być widoczny dla zewnętrznych wyszukiwarek;

4. UWAŻAJ, JAKIMI INFORMACJAMI, ALE TEŻ ZDJĘCIAMI LUB FILMAMI, DZIELISZ SIĘ Z INNYMI

Pamiętaj, że osoba której zdjęcia zamieszczasz, powinna wyrazić na to zgodę. Nie publikuj zdjęć intymnych, ośmieszających czy zdradzających zbyt wielu informacji o Tobie i osobach bliskich. Chroń dane, które podlegają szczególnej ochronie m.in. dane o zdrowiu, nałogach, poglądach politycznych czy orientacji seksualnej;

5. NIE UJAWNIAJ ZBYT WIELU INFORMACJI O SOBIE

Minimalizuj liczbę informacji o sobie i swoich danych osobowych udostępnianych w Internecie. Uważaj na zamieszczenie zdjęć/nagrań wraz danymi o lokalizacji. Nie zamieszczaj zdjęć dokumentów np. legitymacji szkolnej, dowodu tożsamości, karty płatniczej, świadectwa szkolnego czy prawa jazdy;

6. UWAŻAJ NA ZAPROSZENIA OD NIEZNANYCH UŻYTKOWNIKÓW

Zachowaj ostrożność przy zawieraniu nowych znajomości w sieci. Pamiętaj też, że ktoś obcy może się podszyć za osobę Ci znaną, po przejęciu jego konta np. w mediach społecznościowych;

7. UWAŻAJ NA TZW. PHISHING i SZKODLIWE OPROGRAMOWANIE

Oszuści wyłudzają dane osobowe z pomocą socjotechniki. Próbują nakłonić nas do podania naszego loginu i hasła na fałszywej stronie internetowej, która do złudzenia przypomina np. stronę logowania do portalu społecznościowego, maila czy konta w banku. Oszuści wykorzystują również ankiety w mediach społecznościowych, oferty pieniędzy za reklamę czy wykonane szczepienia. Mogą w ten sposób przejąć kontrolę nad kontem użytkownika;

8. WERYFIKUJ, KTO JEST PRAWDZIWYM NADAWCĄ WIADOMOŚCI E-MAIL

Zwracaj uwagę na adres mailowy, z którego została wysłana wiadomość, czy na pewno pochodzi od zaufanego nadawcy. Często w fałszywych mailach występują błędy np. w nazwie domeny. Oryginalna strona instytucji może mieć domenę z końcówką „.pl", a nadawca fałszywego maila korzysta z domeny np. „.com";

9. UWAŻAJ NA PUBLICZNE LUB NIEZABEZPIECZONE POŁĄCZENIA INTERNETOWE

Nie loguj się do serwisów społecznościowych oraz kont podczas korzystania z otwartych sieci tj. takich do których dostęp nie jest zabezpieczony hasłem, albo do których dostęp posiada większa lub niedająca się określić liczba użytkowników.

Dbajmy o siebie i swoje bezpieczeństwo. Dobre praktyki, powinny stać się nawykiem każdego internauty. O tym warto pamiętać nie tylko od święta.

URZĄD OCHRONY DANYCH OSOBOWYCH