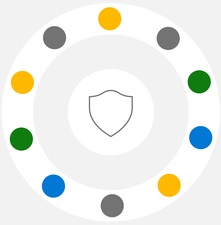
Microsoft

10 prostych zasad cyberhigieny



Cel:

Aby nie musieć odtwarzać swojej cyfrowej tożsamości, wymieniać dokumentów, kart kredytowych i nie stracić efektów pracy na skutek działań cyfrowych przestępców.

Oto 10 prostych zasad, dzięki którym twoja poczta, konta i urządzenia będą bezpieczniejsze, a ty unikniesz kradzieży tożsamości cyfrowej.

1 Jeśli udostępniasz dane osobowe, rób to wyłącznie w czasie rzeczywistym – osobiście lub przez telefon. Zachowaj ostrożność w mediach społecznościowych

Udostępniaj dane osobowe tylko osobiście lub podczas zweryfikowanej rozmowy telefonicznej. Jeśli absolutnie musisz wysyłać takie dane pocztą, włącz szyfrowanie. Chroń swoją prywatność i wrażliwe informacje przed cyberprzestępcami w mediach społecznościowych. Zanim opublikujesz informacje w mediach społecznościowych, zastanów się, jakie dodatkowe dane mogą zostać z pozyskane.

2 Bądź podejrzliwy wobec wiadomości zawierających odsyłacze do stron internetowych – szczególnie takich, które proszą o podanie danych osobowych

Odszukaj numer telefonu na oficjalnej stronie nadawcy i zadzwoń, aby upewnić się, że wiadomość jest prawdziwa.

3 Uważaj na wiadomości zawierające załączniki

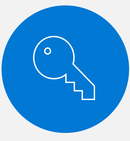
Nigdy nie otwieraj nieoczekiwanych załączników, nawet jeśli pochodzą od osób lub organizacji, którym ufasz. Jeśli masz jakiekolwiek podejrzenia, zadzwoń do nadawcy i zweryfikuj.

4 Pozbądź się hasła i używaj aplikacji uwierzytelniających dla podwyższenia poziomu bezpieczeństwa

Nie można ukraść hasła, jeśli go nie używasz. Wiele urządzeń i serwisów umożliwia logowanie przy użyciu metody bez hasła. Po usunięciu hasła z konta możesz zalogować się na przykład dzięki aplikacji Microsoft Authenticator, fizycznych kluczy zabezpieczeń, kodów SMS lub danych biometrycznych.

5 Jeśli musisz używać hasła, upewnij się, że jest silne

Silne hasło to przynajmniej 14 znaków zawierających wielkie i małe litery, cyfry oraz znaki specjalne. Używaj unikalnych haseł dla różnych usług.



6 Aktywuj blokowanie swoich urządzeń mobilnych

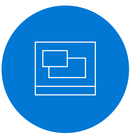
Wymagaj PINu, włącz rozpoznawania twarzy albo odblokowanie odciskiem palca na wszystkich swoich urządzeniach mobilnych.

7 Nie odkładaj na później aktualizacji oprogramowania

Wiele aktualizacji aplikacji i systemów operacyjnych dotyczy poprawy bezpieczeństwa w reakcji na nowe zagrożenia. Instaluj aktualizacje, gdy tylko są dostępne.

8 Upewnij się, że wszystkie twoje aplikacje są legalne i bezpieczne

Instaluj wyłącznie aplikacje pochodzące z oficjalnych sklepów właściwych dla twojego urządzenia.



9 Miej na komputerze zainstalowany system operacyjny wspierany przez producenta

Zawsze używaj najnowszej wersji systemu operacyjnego.
Uważaj na wszelkie wyświetlane informacje dotyczące zmian w ustawieniach związanych z bezpieczeństwem i prywatnością.

10 Aktualizuj na bieżąco swoją przeglądarkę. Korzystaj z trybu incognito lub prywatnego. Włącz blokowanie wyskakujących okienek

Nie zwlekaj z aktualizacją swojej przeglądarki. Tylko w ten sposób zapewnisz wypełnienie bieżących standardów bezpieczeństwa.

Uzyskaj więcej informacji na temat bezpieczeństwa twoich danych i urządzeń:
https://support.microsoft.com/security

Więcej informacji na temat bezpieczeństwa od Microsoft:
https://www.microsoft.com/en-us/securitynow

Udostępnij ten dokument:

Microsoft