

**DZIEŃ BEZPIECZNEGO
KOMPUTERA 2026:
TWÓJ CYFROWY PANCERZ!**

Silne hasła to podstawa

- **Zasada długości:** Dobre hasło ma minimum 12-14 znaków.
- **Miks znaków:** Używaj wielkich i małych liter, cyfr oraz znaków specjalnych (np. @, !, *).
- **Unikalność:** Nigdy nie używaj tego samego hasła do różnych kont (bank, e-mail, gry, social media).
- **Menedżer haseł:** Zamiast zapisywać hasła na kartkach przyklejonych do monitora, używaj bezpiecznych programów do ich przechowywania.
- **Weryfikacja dwuetapowa (2FA):** Włącz ją wszędzie, gdzie to możliwe. Nawet jeśli ktoś pozna Twoje hasło, nie zaloguje się bez kodu z SMS-a lub aplikacji.

Ochrona sprzętu i danych

- **Kopie zapasowe (Backup):** Rób regularne kopie najważniejszych plików na dysku zewnętrznym lub w bezpiecznej chmurze. W razie awarii komputera lub ataku ransomware nie stracisz danych.
- **Aktualizacje systemowe:** Regularnie aktualizuj system operacyjny oraz wszystkie programy i aplikacje. Aktualizacje łatają luki, przez które mogą się włamać hakerzy.
- **Program antywirusowy:** Zainstaluj sprawdzony program antywirusowy i dbaj o to, aby jego baza wirusów była zawsze aktualna.
- **Blokada ekranu:** Odchodząc od komputera (nawet na chwilę w szkole czy pracy), zawsze blokuj ekran skrótem Windows + L (lub odpowiednikiem na macOS).

Uważaj na cyfrowe pułapki

- **Phishing:** Nie klikaj w podejrzane linki w wiadomościach SMS, e-mailach czy na komunikatorach. Cyberprzestępcy często podszywają się pod kurierów, banki lub znajomych proszących o kod BLIK.
- **Zasada ograniczonego zaufania:** Nie pobieraj plików ani programów z nieznanych i niesprawdzonych stron internetowych.
- **Publiczne sieci Wi-Fi:** Nie loguj się do banku ani nie wpisuj haseł, będąc połączonym z otwartym, darmowym Wi-Fi w parku czy galerii handlowej (chyba że używasz VPN).
- **Świadome klikanie:** Zanim klikniesz „akceptuję” na wyskakującym okienku, przeczytaj, na co się zgadzasz.

Cyfrowy dekalog (Krótkie hasła do zapamiętania)

- *Myśl, zanim klikniesz!*
- *Twój komputer jest tak bezpieczny, jak Twoje najsłabsze hasło.*
- *Kopia zapasowa to Twój najlepszy przyjaciel na czarną godzinę.*
- *W sieci nikt nie jest całkowicie anonimowy – dbaj o swoją prywatność.*

MINI-QUIZ WIEDZY Z CYBERBEZPIECZEŃSTWA

1.

Które z poniższych haseł jest najbezpieczniejsze i najtrudniejsze do złamania przez cyberprzestępców?

A.

12345678

B.

Kot123

C.

Trudne!Haslo#2026!Bezpieczne

D.

data_urodzenia

2.

Otrzymujesz SMS-a z nieznanego numeru z informacją, że Twoja paczka została zatrzymana z powodu niedopłaty 1,50 zł i linkiem do strony przypominającej portal kurierski. Co to za zagrożenie?

A.

Atak typu DDoS

B.

Zainfekowanie pamięci RAM

C.

Awaria techniczna operatora

D.

Phishing

3.

Czym dokładnie jest uwierzytelnianie dwuskładnikowe (2FA) i dlaczego warto je włączać?

A.

Dodatkowa warstwa ochrony, która oprócz hasła wymaga podania drugiego elementu (np. kodu z SMS-a lub aplikacji), co utrudnia włamanie na konto nawet w przypadku wycieku hasła.

B.

Sposób na dwukrotne wpisanie tego samego hasła podczas rejestracji, aby uniknąć literówek.

C.

Automatyczne zmienianie hasła co dwa tygodnie przez system komputera.

D.

Korzystanie z dwóch różnych przeglądarek internetowych jednocześnie.

Pokaż wskazówkę

4.

Dlaczego regularne tworzenie kopii zapasowych (backupu) najważniejszych plików jest kluczowym elementem cyberbezpieczeństwa?

A.

Ponieważ przyspiesza to działanie komputera i zwalnia miejsce na dysku systemowym.

B.

Umożliwia legalne pobieranie płatnych gier za darmo.

C.

Pozwala na odzyskanie cennych danych i dokumentów w razie awarii sprzętu, usunięcia plików lub ataku złośliwego oprogramowania (np. ransomware).

D.

Zabezpiecza komputer przed fizycznym zalaniem wodą.

5.

Jaka zasada jest najważniejsza podczas korzystania z darmowej, otwartej sieci Wi-Fi w kawiarni lub na dworcu?

A.

Można bezpiecznie logować się do bankowości elektronicznej, ponieważ darmowe sieci są zawsze monitorowane przez administratorów.

B.

Unikaj logowania się do poufnych kont lub używaj sprawdzonej sieci VPN, ponieważ otwarte Wi-Fi może być podsłuchiwane przez hakerów.

C.

Należy od razu wyłączyć antywirusa, aby nie spowalniał przeglądania stron na publicznym łączu.

D.

Publiczne Wi-Fi automatycznie szyfruje wszystkie przesyłane hasła za pomocą najwyższych norm wojskowych.

ODPOWIEDZI MINI-QUIZ WIEDZY Z CYBERBEZPIECZEŃSTWA

Pytanie 1: Które hasło jest najbezpieczniejsze?

Odp: 'Trudne!Hasło#2026!Bezpieczne' – ponieważ jest długie, wielowyrazowe i zawiera miks różnych znaków.

Pytanie 2: Otrzymujesz SMS z informacją o niedopłacie do paczki i linkiem. Co robisz?

Odp: Ignorujesz wiadomość i nie klikasz w link. To próba wyłudzenia danych (phishing).

Pytanie 3: Co daje włączenie dwuskładnikowego uwierzytelniania (2FA)?

Odp: Zapewnia dodatkową ochronę. Nawet jeśli ktoś pozna Twoje hasło, nie wejdzie na konto bez kodu z telefonu.

Pytanie 4: Jak najszybciej zabezpieczyć komputer przed dostępem osób trzecich, gdy odchodzisz od biurka?

Odp: Zablokować ekran za pomocą skrótu klawiszowego Windows + L (lub odpowiednika dla macOS).

Pytanie 5. Jaka zasada jest najważniejsza podczas korzystania z darmowej, otwartej sieci Wi-Fi w kawiarni lub na dworcu?

Odp: Unikaj logowania się do poufnych kont lub używaj sprawdzonej sieci VPN, ponieważ otwarte Wi-Fi może być podsłuchiwane przez hakerów.