Nie zapisuję w komputerze haseł i kodów. Dlaczego?

Jeśli ktoś uzyska dostęp do mojego komputera, będzie miał dostęp do wszystkich moich kont lub profili użytkownika. Może to skutkować na przykład kradzieżą mojego konta w portalu społecznościowym lub kradzieżą pieniędzy z konta bankowego.

Bezpieczne hasła i kody do logowania w Internecie. Jak je ustawić?

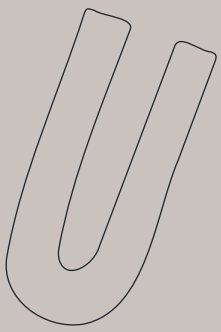
1. Bezpieczne hasło powinno być trudne do złamania, długie i składać się z losowych kombinacji liter, cyfr i znaków specjalnych (znak specjalny to symbol, który nie jest ani literą, ani cyfrą, na przykład „!”, „%”). Bezpieczne hasło zawiera co najmniej 12 znaków i nie powinno składać się z samych liter lub cyfr (na przykład „abcdefgh”, „123654”), imion, nazwisk lub nazw znanych postaci lub popularnych słów (na przykład „kasia1”, „batman2”), sekwencji odczytywanych z klawiatury (na przykład „123456”, „qwerty”).
2. Warto korzystać z różnych haseł dla różnych kont internetowych. Warto regularnie zmieniać hasła. Warto też zdecydować się na aktywację logowania dwuetapowego. Oznacza to, że po wpisaniu hasła należy się uwierzytelnić jeszcze w inny sposób: na przykład w aplikacji mobilnej lub podając kod SMS.

Nie ufam wszystkim informacjom w sieci. Dlaczego?

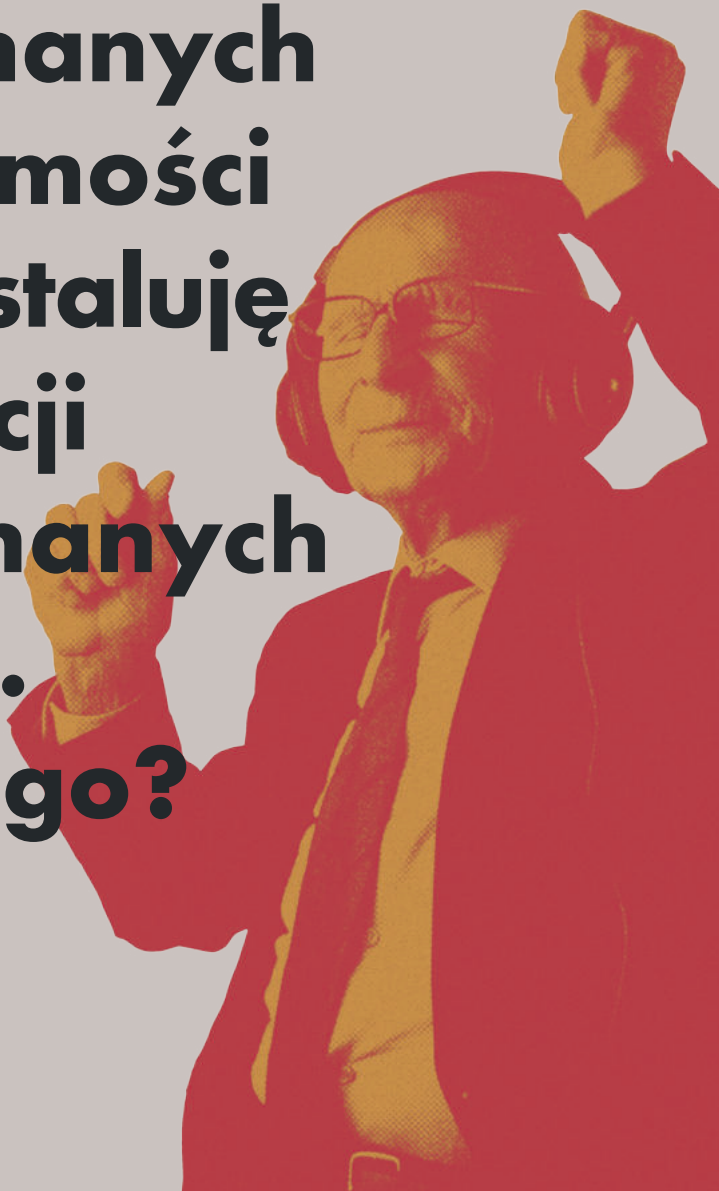
Niektóre z informacji w Internecie mogą być fałszywe lub nieaktualne. W Internecie każdy może publikować informacje, a nie zawsze są one prawdziwe lub rzetelne. Dlatego sprawdzam źródło informacji i korzystam z wiarygodnych stron internetowych.

Nie podaję swoich danych osobowych w Internecie. Dlaczego?

1. Podawanie swoich danych osobowych w Internecie jest niebezpieczne. W ten sposób „pomagam” oszustom i ułatwiam im dostęp do wszystkich moich danych. Jeżeli podam swoje dane osobowe w Internecie, to tak jakbym zapraszał oszusta nie tylko do swojego domu, ale i do swojego życia.
2. Dane osobowe to informacje, które pozwalają zidentyfikować użytkownika. Nigdy, pod żadnym pozorem czy naciskiem nie podaję swoich danych osobowych w Internecie. Wyjątkiem mogą być strony rządowe oraz zakupy online.



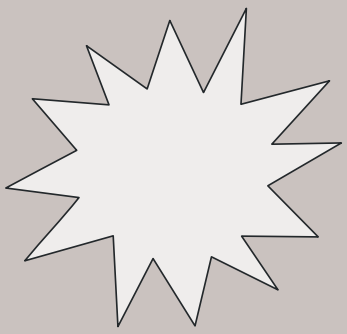
Nie otwieram załączników z nieznanych wiadomości i nie instaluję aplikacji z nieznanych źródeł. Dlaczego?



Załączniki i aplikacje mogą zawierać wirusy lub inne szkodliwe oprogramowanie, które mogą uszkodzić mój komputer, telefon lub ukraść moje dane.

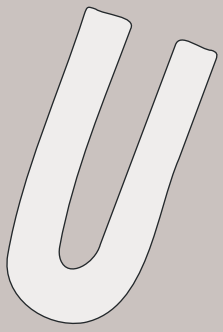
Dostaję SMS, że zalegam z płatnością. Co robię?

1. Powinienem skontaktować się z firmą, której rzekomo zalegam z płatnością. Mogę również skontaktować się z bankiem lub firmą, która obsługuje moją kartę, aby upewnić się, że wszystko jest w porządku.
2. Jeśli nie jestem pewien, czy SMS jest prawdziwy, nie klikam w linki ani nie podaję swoich danych osobowych.
3. Jeśli podejrzewam oszustwo, dzwonię na policję pod numer 997 lub 112.



Nie umieszczam swoich zdjęć i zdjęć moich dzieci oraz wnuków w Internecie. Dlaczego?

1. Umieszczanie zdjęć w Internecie może narazić mnie i moją rodzinę na niebezpieczeństwo kradzieży tożsamości lub inne formy oszustwa.
2. Chronię prywatność swoją i mojej rodziny. Umieszczanie zdjęć na przykład moich wnuków w Internecie może narazić je na niebezpieczeństwo. Ktoś może wykorzystać zdjęcia w sposób, który może być szkodliwy.



Nie ufam osobom poznanym w Internecie. Dlaczego?

1. Nie znam osobiście osób poznanych w Internecie. Nie mam więc pewności, czy mówią prawdę o sobie. W Internecie łatwo jest udawać kogoś innego lub ukrywać swoją tożsamość.
2. Pamiętam, że w Internecie mogę spotkać różne osoby – zarówno te dobre, jak i złe. Dlatego zachowuję ostrożność i nie ufam osobom, których nie znam osobiście.
3. Nigdy nie mam pewności, że ta osoba jest tym, za kogo się podaje. Mogła przesłać zdjęcie kogoś innego i podszyć się pod inną osobę. Być może chce wyłudzić ode mnie pieniądze.

Wyznaczam sobie konkretny czas na korzystanie z Internetu. Dlaczego? Do czego może prowadzić zbyt długie *siedzenie* w Internecie?

Chcę utrzymać równowagę w życiu i nie chcę uzależnić sie od Internetu. Zbyt długie ***siedzenie*** w Internecie może powodować:

1. Problemy z koncentracją.
2. Problemy ze snem.
3. Problemy w relacjach z innymi.
4. Problemy ze wzrokiem.
5. Otyłość, ze względu na ograniczony ruch.
6. Doświadczenie przemocy w Internecie.

Pamiętam o regularnych aktualizacjach w komputerze i telefonie. Dlaczego?

1. Aktualizacje wyposażają system i zainstalowane na nim oprogramowanie w nowe funkcje, których starsze wersje są pozbawione. Poprawiają zarówno bezpieczeństwo, jak i komfort użytkownika.
2. Aktualizacje są ważne dla bezpieczeństwa urządzenia. Aktualizacje zawierają poprawki bezpieczeństwa, które pomagają chronić urządzenie przed wirusami i innymi zagrożeniami.

Pamiętam o wylogowywaniu się z internetowych serwisów. Dlaczego?

1. Zwiększam w ten sposób swoje bezpieczeństwo w sieci.
2. Uniemożliwiam cyberprzestępcom przejęcie moich danych.

Tworzę kopie zapasowe dokumentów. Dlaczego?

1. Kopie zapasowe pozwalają mi odzyskać dane, jeśli dysk twardy w moim komputerze miał awarię albo skradziono mój komputer lub nośnik danych (na przykład pendrive).
2. Kopie zapasowe są przydatne w przypadku pomyłkowego wykasowania danych lub skasowania danych przez inne osoby.
3. Kopie zapasowe chronią dane przed utratą wskutek działania wirusów komputerowych lub innych zdarzeń losowych.

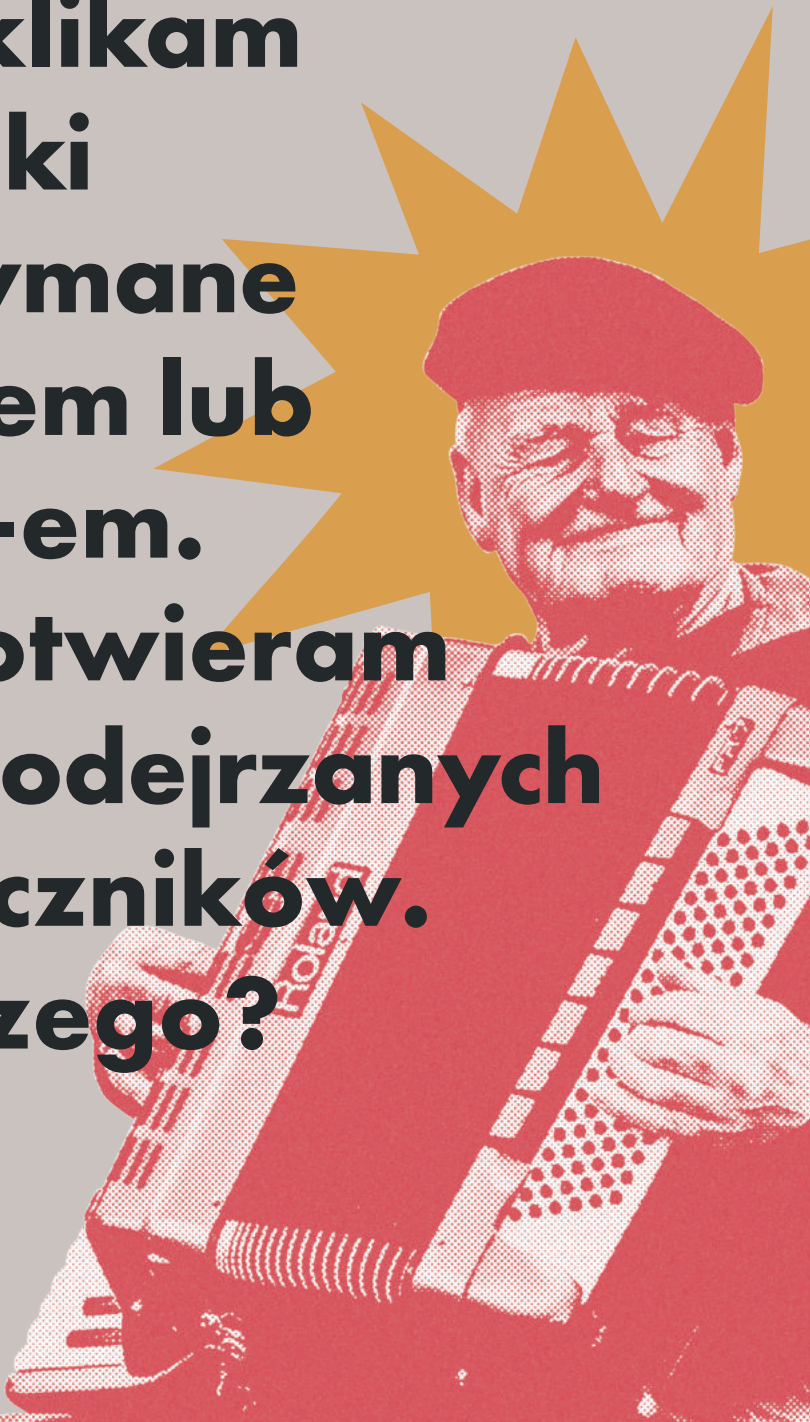
Unikam korzystania z publicznych sieci Wi-Fi. Dlaczego?

1. Korzystanie z publicznych sieci Wi-Fi może być niebezpieczne, ponieważ osoby trzecie mogą przechwytywać przesyłane przeze mnie informacje.
2. Unikam logowania się do banków lub portfeli walutowych oraz prowadzenia prywatnej korespondencji, która zawiera wrażliwe dane, jeśli korzystam z publicznych sieci Wi-Fi.
3. Jeśli muszę korzystać z publicznej sieci Wi-Fi, to pamiętam, że warto zainstalować oprogramowanie antywirusowe.
4. Unikam korzystania z nieznanych sieci Wi-Fi.

Otrzymuję informację, że wygrałem nagrodę, w konkursie, w którym nie brałem udziału. Co robię?

1. Zachowuję ostrożność. Może to być próba oszustwa.
2. Nie odpowiadam na takie informacje i nie podaję swoich danych osobowych i finansowych.

Nie klikam w linki otrzymane mailem lub SMS-em. Nie otwieram też podejrzanych załączników. Dlaczego?



1. Może to prowadzić do różnych problemów związanych z bezpieczeństwem. Może to spowodować infekcję mojego komputera wirusem i mogę wtedy stracić dane. Może również zainstalować się na moim komputerze oprogramowanie szpiegujące, które może przesłać moje dane do cyberprzestępców.
2. Pamiętam, że warto sprawdzać adres URL strony internetowej przed kliknięciem w link. Jeśli link wygląda podejrzanie lub nie znam tej strony internetowej, nie klikam w link.

Co to jest *phishing* i jak mogę się przed nim chronić?

Phishing to metoda oszustwa, w której przestępca podszywa się pod inną osobę lub instytucję, żeby wyłudzić poufne informacje (na przykład dane logowania, dane osobowe, dane karty kredytowej), zainfekować komputer szkodliwym oprogramowaniem albo nakłonić osobę, którą chce oszukać, do określonych działań. Przestępcy internetowi często wykorzystują phishing do kradzieży haseł i loginów do kont bankowych lub serwisów społecznościowych. Atak phishingowy może przybierać różne formy – mogą to być na przykład fałszywe strony internetowe, fałszywe e-maile lub wiadomości SMS.
Jak się bronię przed phishingiem?

1. Nie otwieram podejrzanych wiadomości e-mail, nie klikam w podejrzane linki.

2. Nie podaję poufnych informacji osobowych ani danych logowania do kont bankowych lub serwisów społecznościowych.

3. Instaluję oprogramowanie antywirusowe i zawsze aktualizuję przeglądarkę internetową.

4. Korzystam z narzędzi oferowanych przez banki i serwisy społecznościowe, na przykład z uwierzytelniania dwuskładnikowego.

Chcę sprawdzić wiarygodność sklepu internetowego. Co mogę zrobić?

1. Sprawdzam dane przedsiębiorcy – nazwę firmy, adres siedziby, dane kontaktowe, numer KRS. Kontroluję, czy dane ze strony zgadzają się z danymi w Centralnej Ewidencji i Informacji Gospodarczej na stronie Ceidg.gov.pl.
2. Sprawdzam opinie na temat danego sklepu internetowego na forach internetowych, w mediach społecznościowych.
3. Zapoznaję się z metodami płatności w danym sklepie. Unikam przelewania pieniędzy na prywatne konto sprzedającego. Bezpieczniejsze jest korzystanie z systemów płatności internetowej.

Bezpieczne zakupy w Internecie. Co robię?

1. Kupuję tylko w sprawdzonych sklepach.
2. Podaję tylko niezbędne dane. Żaden sprzedawca nie potrzebuje mojego numeru PESEL, daty urodzenia czy nazwiska panieńskiego matki. Jeśli jakiś sklep prosi mnie o takie dane, nie robię w nim zakupów.
3. Używam silnych haseł, logując się do sklepów. Do każdego sklepu używam innego hasła.
4. Przeglądam elektroniczne rachunki z wyciągu bankowego. Jeśli coś mnie zaniepokoi, dzwonię do banku z pytaniami.
5. Nie robię zakupów, kiedy używam publicznego Wi-Fi – hakerzy mogą łatwo przejąć moje dane.
6. Korzystam z uwiarygodniania dwuetapowego, jeśli sklep daje taką możliwość.

Co to jest *cyberprzemoc* i jak się przed nią bronię?

Cyberprzemoc to wszelkie formy agresji przy użyciu Internetu i urządzeń elektronicznych. Najpopularniejsze formy takiej agresji to:

- publikowanie poniżających filmów lub zdjęć,
- publikowanie ośmieszających, wulgarnych, komentarzy i postów,
- włamania na konta serwisów społecznościowych,
- ***flood***, czyli zasypywanie wiadomościami w komunikatorze, telefonami, SMS-ami podszywanie się pod inne osoby,
- wykluczanie z internetowych społeczności.

Jak się bronię przed cyberprzemocą?

1. Nigdy nie wysyłam swoich zdjęć nieznajomym.
2. Jestem ostrożny w udostępnianiu swoich danych w Internecie.
3. Ustawiam bezpieczne hasła do swoich mediów społecznościowych, poczty elektronicznej.

Doświadczyłem *cyberprzemocy*. Co robię?

1. Kopiuję dowody cyberprzemocy – robię zrzuty ekranu (screen), nie kasuję wiadomości e-mail, SMS-ów.
2. Zgłaszam problem serwisom internetowym, na których doświadczyłem cyberprzemocy – wysyłam zrzut ekranu wiadomości.
3. Jeśli cyberprzemoc ma znamiona przestępstwa, dzwonię na policję pod numer 997 lub 112.