TAURON

BezpieczeństWWWo w sieci

Poznaj najważniejsze zasady bezpiecznego korzystania z internetu

tauron.pl

Spis treści

Wstęp:

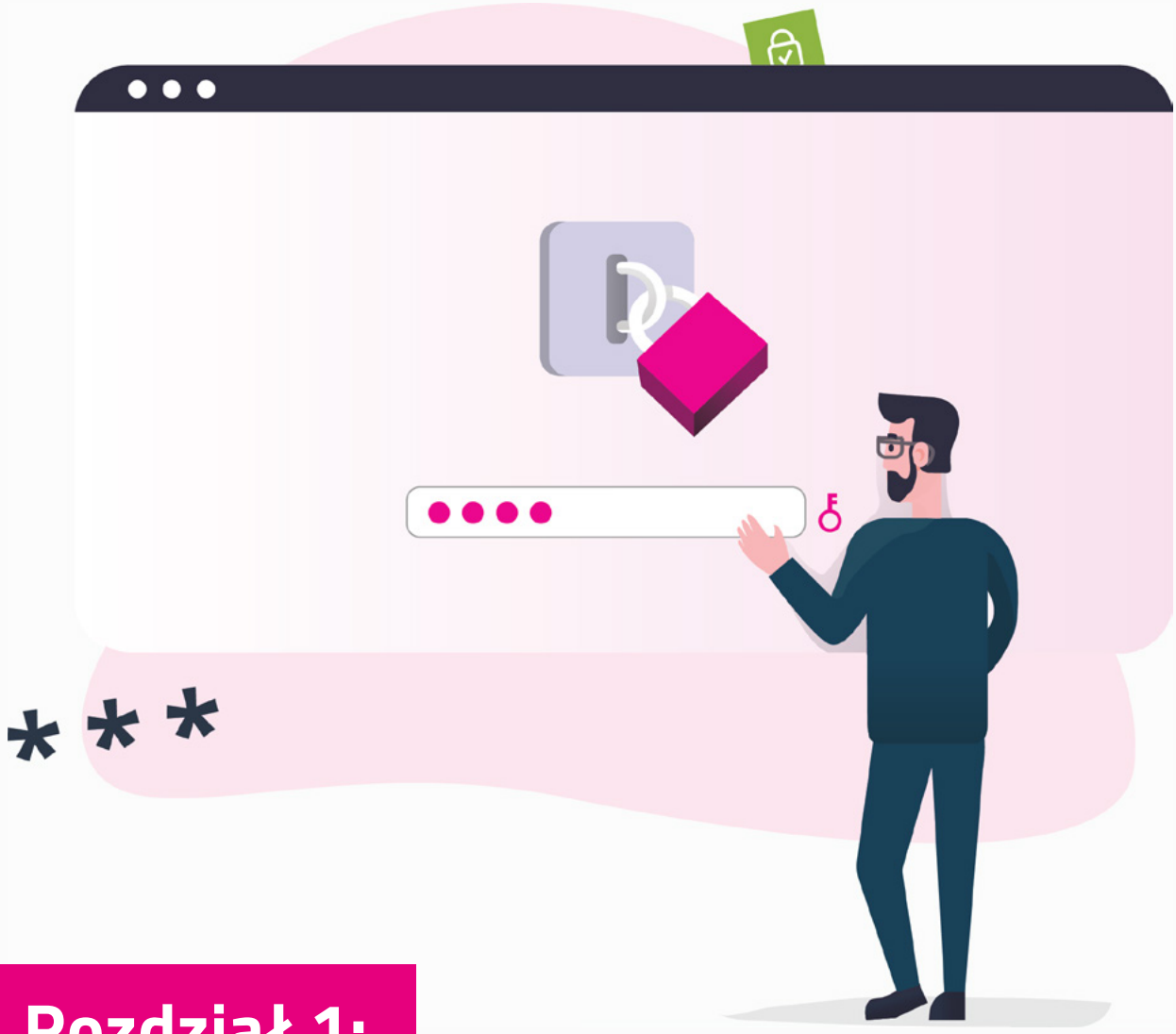
Jak być bezpiecznym w sieci?

Internet daje nam mnóstwo możliwości – to właśnie za jego pomocą komunikujemy się z rodziną i znajomymi, kupujemy, pracujemy, uczymy się i relaksujemy. Jednak sieć ma też swoje **ciemne strony:** grozi nam coraz częściej możliwość utraty danych czy wyłudzenie pieniędzy za pomocą złośliwego oprogramowania. Czasami nie zdajemy sobie sprawy, jak duże niebezpieczeństwo może stanowić niepozornie wyglądający e-mail czy aplikacja mobilna pobrana z niezaufanej strony.

Postanowiliśmy więc oddać w Twoje ręce poradnik „**BezpieczeństWWWo w sieci**". Umieściliśmy w nim konkretne wskazówki i porady, w jaki sposób ustrzec się przed cyberatakami w internecie.
Podstawą bezpiecznego korzystania z sieci jest zawsze po prostu zdrowy rozsądek i ograniczone zaufanie.

Mamy nadzieję, że z naszym e-bookiem korzystanie z internetu będzie jeszcze **przyjemniejsze** i **bezpieczniejsze**!

Zespół bezpieczeństwa TAURON



Rozdział 1:

Silne hasło to podstawa!

Hasło - ciąg znaków, niezbędny podczas logowania do urządzeń, serwisów lub programów. Serwis lub program może wskazać minimalną liczbę i typ znaków potrzebnych do ustalenia hasła.

Hasło to najważniejsze zabezpieczenie

Hasło to najważniejsze zabezpieczenie zarówno zawartości Twojego sprzętu, jak i systemów, z których na co dzień korzystasz, takich jak np. bankowość elektroniczna. W systemach znajdują się Twoje **dane osobowe**, **finanse** oraz **informacje o Tobie**, takie jak **nazwisko**, **adres zamieszkania** czy **data urodzenia**. Nie pozwól, aby ktoś poza Tobą miał do nich dostęp!

Silne hasło powinno:

01

Zawierać co najmniej 10 znaków oraz składać się z kombinacji dużych i małych liter, cyfr lub znaków specjalnych.

02

Być trudne do odgadnięcia – nie powinno nim być Twoje imię, nazwisko, data urodzenia czy następujące po sobie znaki, np.123, abc, qwerty itp.

03

Być natychmiast zmienione, jeżeli masz obawy, że padło ofiarą wycieku danych lub jeśli używasz tego samego hasła do wielu systemów.

Dodatkowe wskazówki

- **Nie przekazuj** nikomu swoich haseł i **nie zapisuj** ich na kartkach w pobliżu swojego komputera lub telefonu.
- Jeżeli obawiasz się, że możesz ich nie zapamiętać, skorzystaj z **Menadżera haseł**. Jest to często bezpłatny program, do pobrania w internecie, który zwolni Cię z konieczności zapamiętania wszystkich Twoich haseł, a także pomoże Ci w ich wygenerowaniu.
- Tam, gdzie jest to możliwe, włącz **dwuetapową weryfikację**, czyli podwójne sprawdzenie, czy to na pewno Ty próbujesz się zalogować. Program lub strona każe podać Ci, oprócz hasła, dodatkowy kod cyfrowy otrzymany w SMS-ie lub e-mailu.

Pamiętaj!

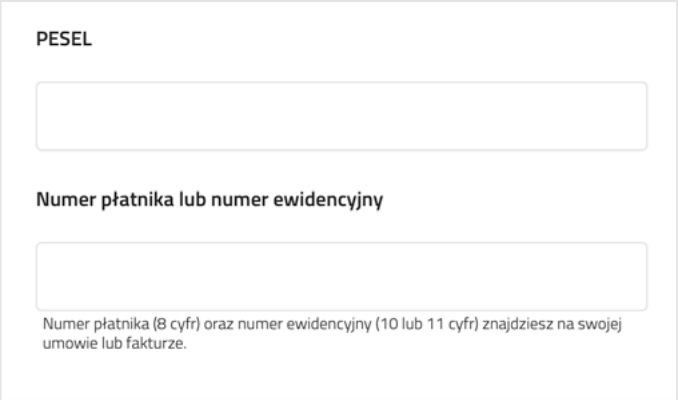
Jeśli zdarzyło Ci się kiedyś użyć hasła typu „Password", „qwerty" lub „imię123", miej świadomość, że nie chroni ono Twoich danych w wystarczający sposób. Proste, 8-znakowe hasło cyberprzestępca jest w stanie złamać w ciągu jednego dnia. Złamanie hasła zawierającego 10 znaków może się już znacząco wydłużyć i trwać nawet **prawie 2 lata**.

Staraj się więc tworzyć silne, długie i nieoczywiste hasła. Dzięki temu Twoje dane będą bezpieczne.

Jak dbamy o bezpieczeństwo hasła w serwisie Mój TAURON?

1

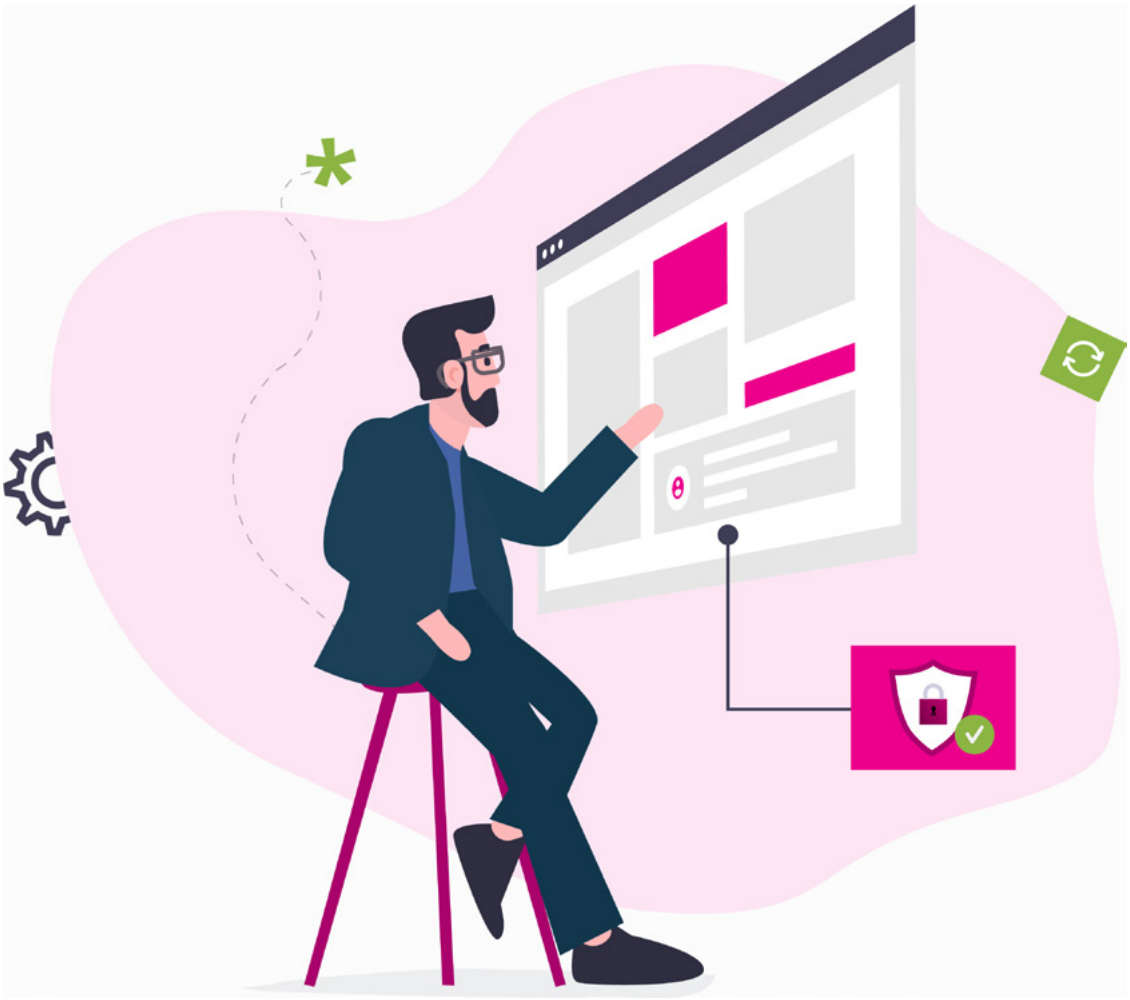
Aby zarejestrować się w serwisie Mój TAURON, będziemy wymagać od Ciebie, abyś podał swój PESEL oraz numer płatnika. Jest to niezbędne, abyśmy mogli zweryfikować, czy to na pewno Ty. Dzięki temu nikt inny nie będzie miał dostępu do Twojego konta, w którym znajdują się Twoje dane osobowe, takie jak adres, liczba punktów poboru, zużycie prądu i/lub gazu czy stan licznika.



2

Poprosimy Cię również, abyś podał swój adres e-mail, który będzie służył jako Twój login oraz abyś ustalił silne hasło. Po rejestracji otrzymasz od nas e-mail z linkiem aktywacyjnym, w który musisz kliknąć, aby dokończyć proces rejestracji. Jest to dodatkowy poziom zabezpieczenia, bo tylko Ty masz dostęp do swojej skrzynki pocztowej.

Gotowe, możesz już korzystać z Mojego TAURONA!



Rozdział 2:

Jak zabiezpieczyć swój komputer?

Podstawowe zasady bezpieczeństwa komputera

1. Dbaj o aktualizacje systemu operacyjnego i programów

Warto instalować zalecane przez producenta aktualizacje systemu na komputerze. Starsze wersje systemów mają luki bezpieczeństwa i są bardziej narażone na ataki przestępców – dlatego nie odkładaj aktualizacji na później, nawet jeśli wymaga to restartu komputera. Sprawdzaj też, czy używasz najnowszych wersji programu antywirusowego czy innych aplikacji, z których korzystasz (np. Adobe Reader czy pakiet Office).

2. Korzystaj z programu antywirusowego

Program antywirusowy skanuje komputer w poszukiwaniu złośliwego oprogramowania, zwalcza wirusy komputerowe i umożliwia ich usunięcie. Wiele programów antywirusowych jest dostępnych do pobrania całkowicie za darmo lub jest wbudowanych w system operacyjny komputera.

3. Używaj tzw. firewalla (zapory sieciowej)

Zapora sieciowa to program, który monitoruje aktywność w sieci i blokuje niepowołany dostęp do komputera. Większość systemów operacyjnych (np. Windows) posiada wbudowane zapory sieciowe. Upewnij się w ustawieniach swojego urządzenia, że Twój firewall jest aktywny. Zapory sieciowe są też częścią programów antywirusowych.

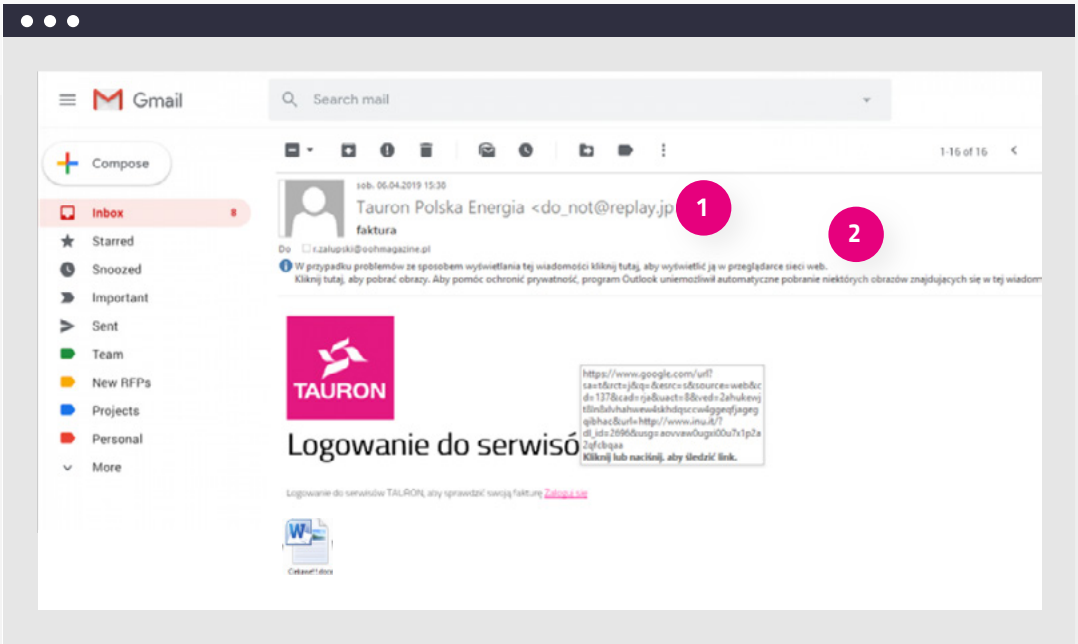
Rozdział 3:

Jak rozpoznać złośliwe e-maile?

Czym są złośliwe wiadomości?

Złośliwa wiadomość - to wiadomość wysłana przez cyberprzestępców, która zachęca Cię do kliknięcia w podejrzany link i zainstalowania na swoim komputerze złośliwego oprogramowania. Dzięki niemu cyberprzestępcy mają dostęp do Twojego komputera – mogą wykraść Twoje hasła, zniszczyć Twoje dane lub wysyłać wiadomości w Twoim imieniu.

Poznaj cztery cechy złośliwych wiadomości



1

Adres e-mail różni się od nazwy nadawcy - jest łudząco podobny lub zupełnie inny

Zwracaj uwagę na dokładny adres, z którego wysłano wiadomość. Twoją wątpliwość powinna wzbudzić każda, nawet drobna zmiana (np. literówka w nazwie lub inne niż zawsze rozszerzenie domeny – np. .jp zamiast .pl).

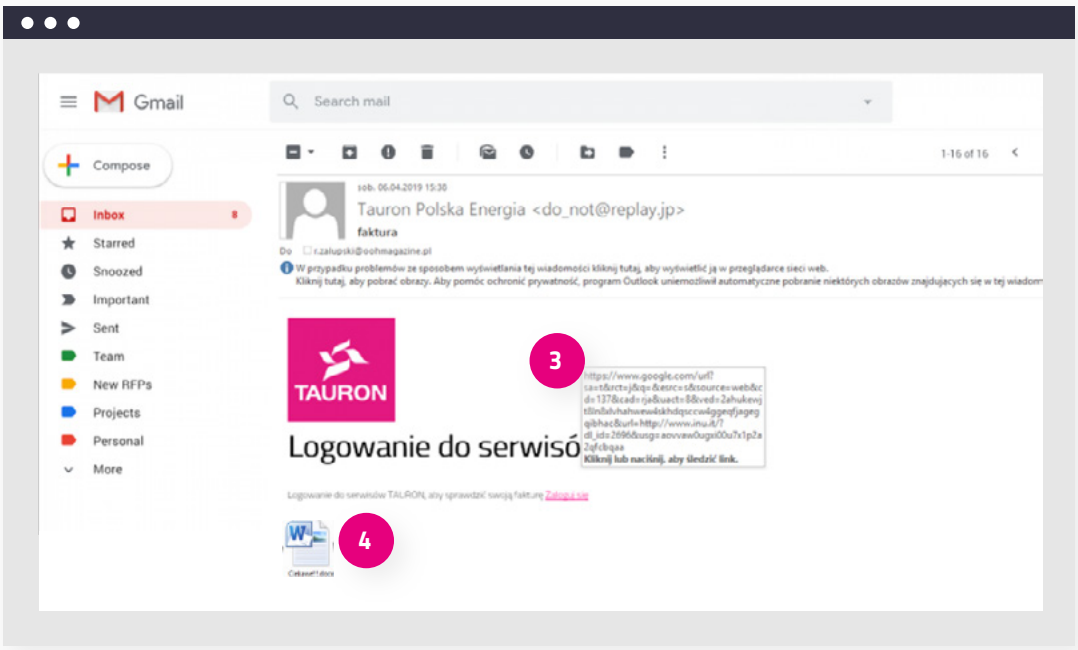
Przykład: otrzymałeś wiadomość od firmy TAURON, natomiast adres e-mail brzmi do_not@replay.jp

2

Treść wiadomości zawiera podejrzane błędy

Przyjrzyj się dokładnie, czy treść wiadomości nie zawiera błędów językowych lub czy nie brakuje w niej polskich znaków. Czytaj dokładnie treść e-maila, zanim otworzysz plik lub klikniesz w link.

Przykład: treść wiadomości zawiera błędy językowe, np. „Posiadaja panstwo zaleglosc nieuregulowana. Zaplac teraz”



3

Link prowadzi do adresu niezwiązanego z nadawcą wiadomości

Sprawdź, czy zamieszczony w wiadomości link nie prowadzi do strony, która jest niepowiązana z nadawcą wiadomości. Najedź kursorem na link, aby zobaczyć, do jakiego rzeczywistego adresu prowadzi.

Przykład: otrzymałeś wiadomość dotyczącą nieodebranej przesyłki z firmy kurierskiej, ale po najechaniu kursorem na link pojawił się zupełnie inny adres, np.: http://www.4sharedcom/1234567.jsp

4

Nie otwieraj załączników, które wzbudzają ciekawość i sugerują pilne otwarcie

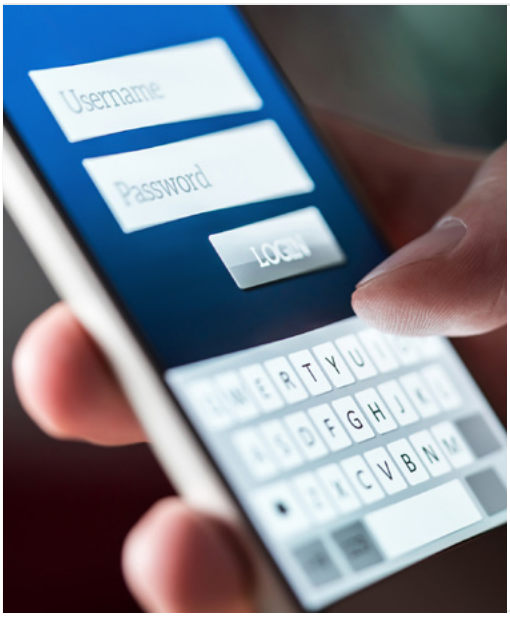
Uważaj na załączniki, których nazwa wskazuje, że ich treść może być bardzo ważna lub interesująca dla odbiorcy, jak np. niezapłacona faktura. Często są one wysyłane w postaci dokumentu Microsoft Word lub PDF. Nie otwieraj ich – mogą być zainfekowane złośliwym oprogramowaniem.

Przykład: „Ważna wiadomość!", „Ciekawostka", „Faktura", „Wezwanie do zapłaty", „Twoje saldo bankowe".

Więcej o próbach wyłudzeń i oszustw internetowych przeczytasz w kolejnym rozdziale.

Rozdział 4:

Wyłudzenia internetowe – jak nie dać się złapać?



Sieciowe łowy

Przestępcy za pomocą fałszywych e-maili, SMS-ów lub linków nakłaniają swoje ofiary do wejścia na fałszywą stronę internetową, najczęściej z panelem logowania.

Taka strona wyglądem bardzo przypomina prawdziwą stronę danej firmy, dlatego ofiara może nie zorientować się, że coś jest nie tak. Jeżeli zaloguje się na takiej stronie np. do portalu obsługowego i poda swoje dane, przestępca przejmie jej login, hasło czy inne wrażliwe informacje.

i

Phishing - (od ang. fishing - łowienie ryb) to jedna z metod wykorzystywana przez cyberprzestępców. Polega na podszyciu się pod firmę lub instytucję, żeby nielegalnie zdobyć poufne informacje. Przestępcy, na wzór wędkarzy, stosują różne przynęty, aby osiągnąć swój cel – a są nim Twoje loginy, hasła, PESEL czy numery kart bankowych.

Przestępcy najczęściej podszywają się pod dobrze znane instytucje, np.:

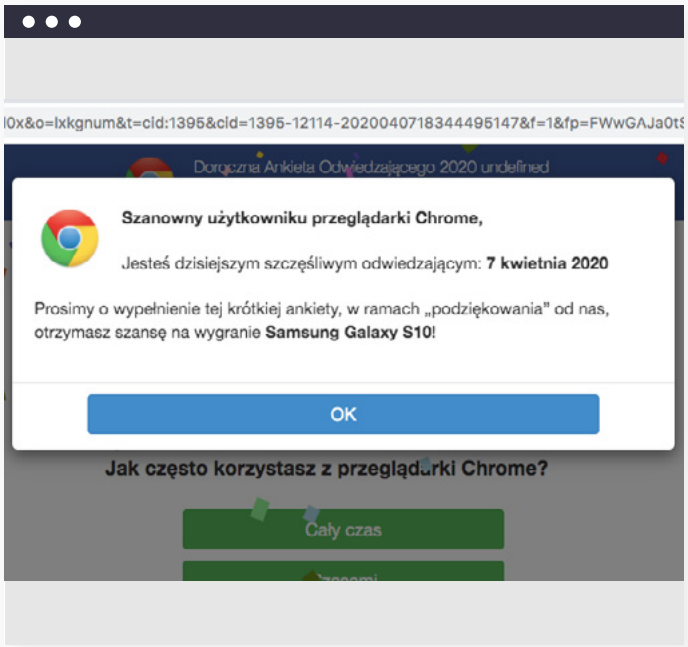
banki / urzędy / firmy kurierskie / firmy telekomunikacyjne / firmy energetyczne

Jak uchronić się przed phishingiem?

1

Uważaj na linki do rzekomo ciekawych lub szokujących treści

„ZAROBIŁ 50 TYSIĘCY, SIEDZĄC W DOMU!" lub „TA KOBIETA SCHUDŁA 20 KG W 2 DNI! SPRAWDŹ JAK"... Takimi linkami cyberprzestępcy nakłaniają do odwiedzania podejrzanych stron internetowych. Linki do takich treści często znajdują się na portalach społecznościowych (np. w grupach na Facebooku) lub są wysyłane za pomocą e-maili.
Uważaj nawet na wiadomości od znajomych, którym ufasz! Ich komputery mogą być zainfekowane wirusem i rozsyłać fałszywe wiadomości automatycznie, bez ich wiedzy.

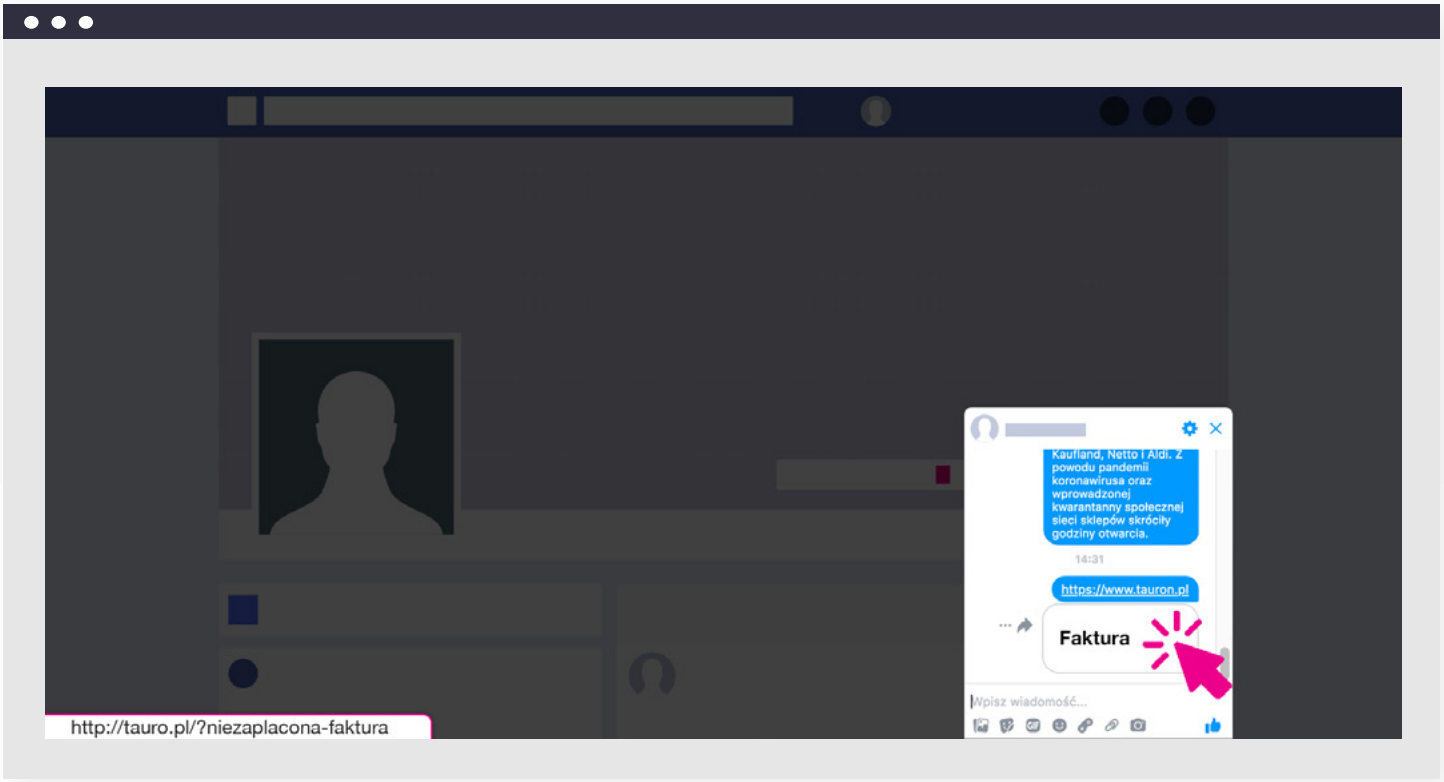


2

Sprawdź rzeczywisty adres linku przed jego otwarciem

Zawsze sprawdzaj adres strony, na którą chcesz wejść. Nawet drobna zmiana w adresie powinna wzbudzić Twoją nieufność. **Przykładowo: strona tauro.pl to nie to samo co tauron.pl!**

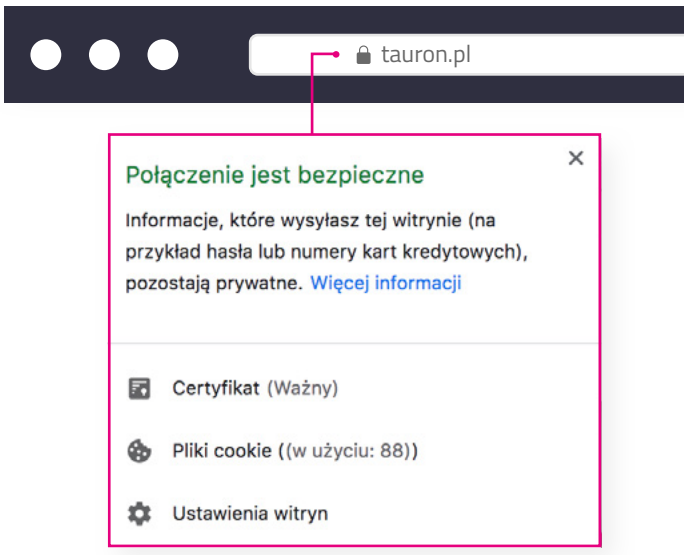
Cyberprzestępcy tworzą fałszywe strony internetowe do złudzenia przypominające te faktycznie istniejące. **Aby sprawdzić rzeczywisty adres strony, najedź najpierw kursorem na link lub przycisk do niej kierujący.** Wyświetli się wtedy prawdziwy link kryjący się pod tekstem.



3

Sprawdź bezpieczeństwo strony internetowej

Sprawdzaj zawsze, czy strona, którą chcesz odwiedzić, jest zabezpieczona certyfikatem. Jest to szczególnie ważne przy stronach, na których podajesz swoje dane lub dokonujesz płatności online.



Rozdział 5:

Jak zachować czujność przez telefon?

Uważaj na prośby podania swoich danych przez telefon

Aby wyłudzić dane osobowe, cyberprzestępcy niejednokrotnie wykorzystują rozmowę telefoniczną. Dzwonią do potencjalnej ofiary, przedstawiając się jako pracownicy np. banku, firmy kurierskiej czy energetycznej (lub innej instytucji albo firmy, która wzbudza zaufanie).

Jak wygląda wyłudzenie?

Przestępcy, w celu „weryfikacji", proszą o podanie np. numeru PESEL czy serii i numeru dowodu osobistego.

Jeżeli nie masz pewności, z kim rozmawiasz, nie przekazuj żadnych poufnych informacji na swój temat!

Konsekwencje mogą być poważne: zaciągnięcie na Ciebie kredytu czy nawet kradzież danych.

Pamiętaj!

Pracownicy TAURONA nigdy nie zapytają Cię o hasła dostępowe przez telefon.

- Jeżeli zdarzy Ci się taka sytuacja, miej świadomość, że ktoś podszywa się pod naszą firmę i jest to próba wyłudzenia od Ciebie danych.
- Odmów udzielenia odpowiedzi, rozłącz się i od razu poinformuj nas o incydencie. Numer na infolinię obsługową TAURONA to ***32 606 0 606.***
  Zgłoś sprawę również na policję.

Pamiętaj też, że numer infolinii sprzedażowej TAURONA to 555 444 555.

Rozdział 6:

Jak dbać o bezpieczeństwo smartfonu i tabletu?

Jak korzystamy z urządzeń mobilnych?

Telefony komórkowe nie służą już wyłącznie do prowadzenia rozmów, ale również do odbierania i przesyłania e-maili, robienia i przechowywania zdjęć czy przeglądania internetu. Podobnie jest z tabletami – korzystamy na nich z mediów społecznościowych lub robimy zakupy online.

Co nam grozi?

Na urządzeniach mobilnych (telefonach czy tabletach) znajduje się wiele informacji o Tobie lub Twojej firmie (jeżeli korzystasz też ze sprzętów służbowych), które mogą paść ofiarą hakerów. **Szczególnie dotyczy to np. aplikacji bankowych, które przechowują bardzo wrażliwe dane.**
Dlatego korzystanie z urządzeń mobilnych podlega podobnym zasadom bezpieczeństwa co używanie komputerów.

Jak więc dbać o swoje bezpieczeństwo na urządzeniach mobilnych?

1

Chroń dostęp do Twojego smartfonu lub tabletu.

Urządzenia mobilne posiadają funkcję uwierzytelniania za pomocą odcisku palca, wzoru rysowanego palcem lub kodu PIN – koniecznie z nich korzystaj! Tym sposobem tylko Ty będziesz mieć dostęp do swojego urządzenia.

2

Instaluj zalecane aktualizacje systemu operacyjnego.

Przestarzała wersja systemu operacyjnego może zawierać luki bezpieczeństwa. Dlatego instaluj zalecane aktualizacje i dbaj o to, by mieć najnowszą wersję systemu, bo zwiększa to poziom zabezpieczenia Twojego urządzenia.

3

Sprawdzaj oprogramowanie i aplikacje.

Instaluj wyłącznie aplikacje z wiarygodnych, autoryzowanych sklepów (Google Play lub AppStore). Dlaczego jest to takie ważne i co może się stać, jeśli pobierzesz złośliwą aplikację?

Jak to działa?

Pobierasz z niezaufanego źródła aplikację, która zawiera złośliwe oprogramowanie.

Po instalacji aplikacji na ekranie smartfona pojawia się ekran do złudzenia przypominający rzeczywisty. Wyświetla się komunikat proszący o podanie danych.

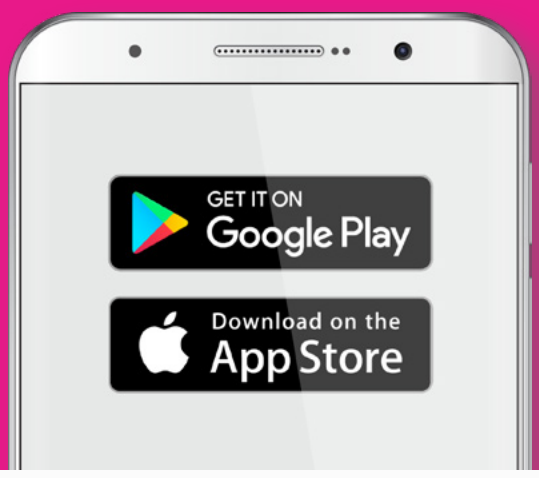
Jeżeli to zrobisz, cyberprzestępca uzyska Twój login i hasło oraz przejmie dostęp do Twojego smartfona. Takie aplikacje podczas instalacji wymuszają przyznanie im wszystkich uprawnień, czyli dostępu do Twoich zdjęć, kamery, mikrofonu czy kontaktów.

Pamiętaj!

Aplikacje na smartfon pobieraj tylko z autoryzowanych sklepów:

- Jeżeli masz telefon z **Androidem**, jest nim **Google Play**.
- Jeżeli masz telefon z **iOS**, jest nim **AppStore**.

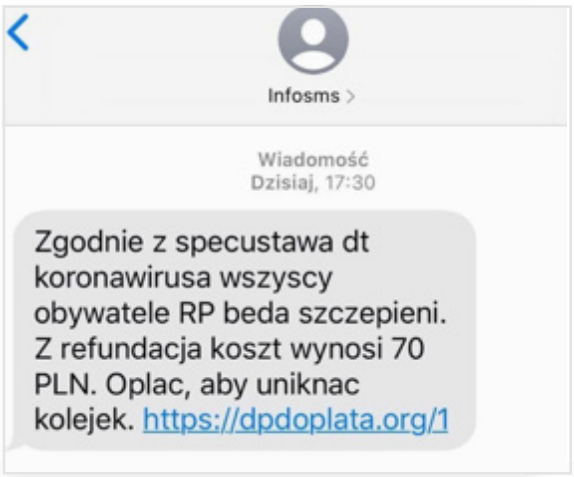
Przed pobraniem dokładnie zapoznaj się z ich oceną oraz komentarzami i recenzjami innych użytkowników. To wartościowa wiedza, która pomoże Ci szybko zweryfikować bezpieczeństwo aplikacji. Nie daj się skusić aplikacjom, które mają niskie oceny i negatywne recenzje.

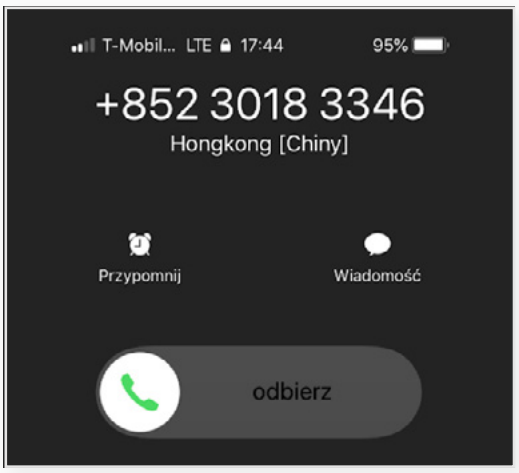


4

Uważaj na podejrzane SMS-y.

Zawsze sprawdzaj nadawcę SMS-a (jego nazwę i numer). Nie ufaj wiadomościom tekstowym, które są napisane z błędami. Nie klikaj w linki, jeśli nie jesteś w stanie ich najpierw zweryfikować. Zasady są bardzo podobne do weryfikowania podejrzanych wiadomości e-mail – przypomnij je sobie tutaj.

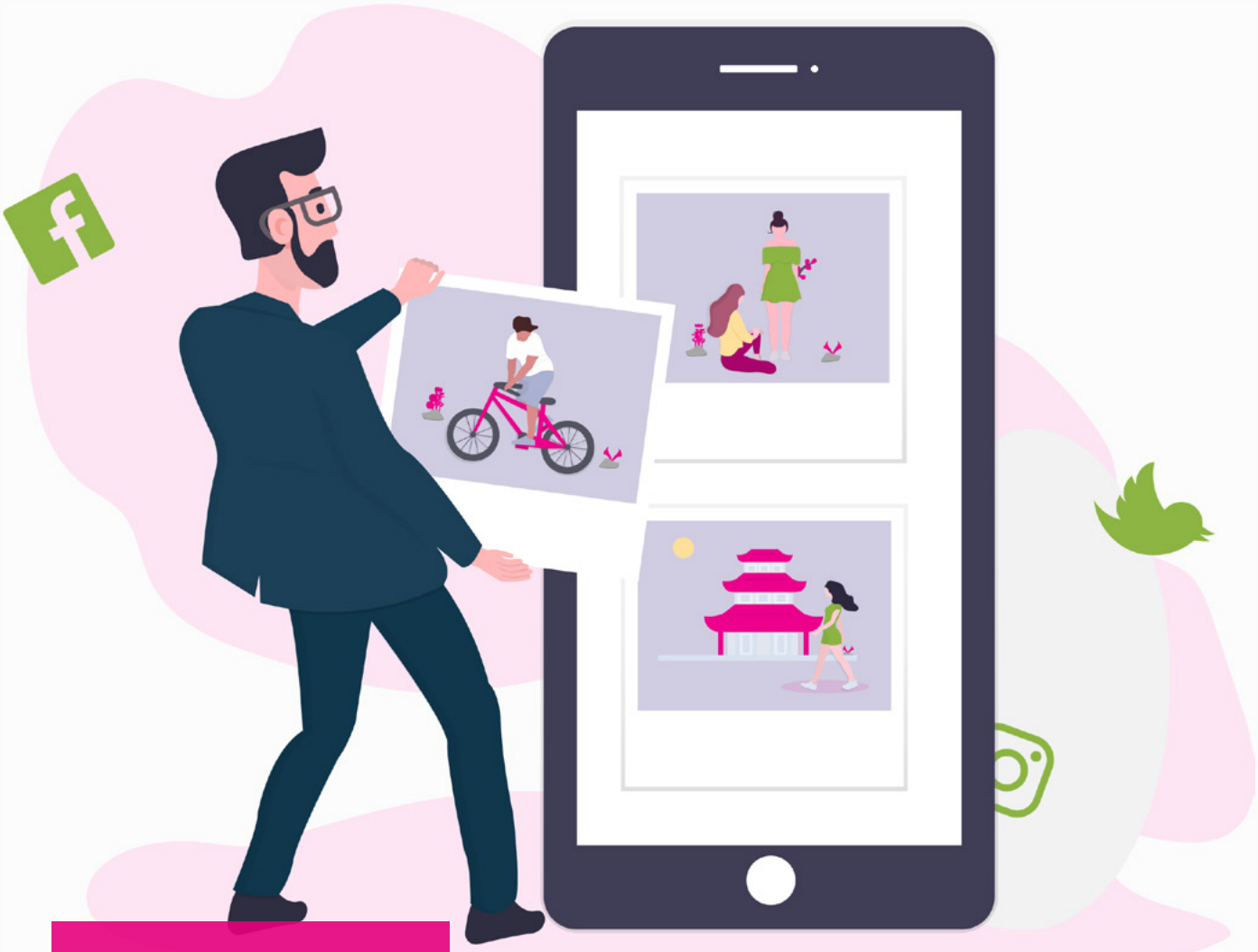




5

Miej ograniczone zaufanie do nieznanych numerów.

Nie odbieraj połączeń od podejrzanych, nieznanych Ci wcześniej numerów (ani nie oddzwaniaj na nie). Uważaj szczególnie na numery zagraniczne, np. z Afryki. Odebranie złośliwego połączenia może się wiązać z pobraniem z Twojego konta pieniędzy lub dalszymi wymuszeniami.
Pamiętaj też o bezpieczeństwie podczas rozmowy przez telefon! Zajrzyj jeszcze raz do rozdziału „Jak zachować czujność przez telefon?"



Rozdział 7:

Jak bezpiecznie korzystać z portali społecznościowych?

Media społecznościowe a Twoje bezpieczeństwo

Chociaż Facebook, Instagram czy Twitter kojarzą się z zabawą i relaksem, korzystanie z nich nie zwalnia Cię z bycia czujnym, ponieważ i tam mogą pojawić się zagrożenia ze strony cyberprzestępców.

Poznaj zasady bezpieczeństwa w mediach społecznościowych

01

Stosuj bezpieczne hasła: używaj różnych haseł do różnych portali społecznościowych, często zmieniaj kombinacje znaków, nikomu nie udostępniaj danych do logowania.

02

Weryfikuj profile, od których otrzymujesz zaproszenia do grona znajomych – nie przyjmuj zaproszeń od obcych.

03

Nie odpowiadaj na wiadomości otrzymane w social mediach, jeżeli nie znasz odbiorcy lub treść wiadomości od znajomego wyda Ci się podejrzana. Nie pobieraj plików załączonych do takich wiadomości ani nie klikaj w linki w nich zawarte.

04

Nie wierz w wysłane przez znajomych prośby, że potrzebują pilnego przelewu – zadzwoń do nich i zweryfikuj, czy wiadomość została przez nich faktycznie wysłana.

05

Informację, że wybierasz się na urlop, zachowaj dla siebie i nie chwal się tym w mediach społecznościowych – pusty dom to świetna informacja dla złodziei.

06

Pamiętaj, aby nie publikować na swoich profilach zdjęć innych osób, od których nie masz zgody na udostępnianie wizerunku.

07

Nie publikuj zdjęć swoich dzieci. Nie wiadomo, kto i w jakim celu będzie je oglądać lub pobierać.

Rozdział 8:

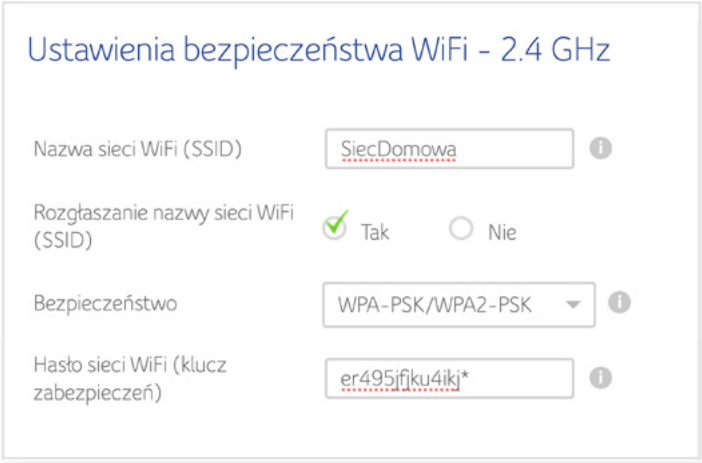
Jak bezpiecznie korzystać z sieci Wi-Fi?

Jak zadbać o bezpieczeństwo domowej sieci Wi-Fi?

1

Zmień nazwę sieci Wi-Fi z domyślnej na własną, ustaw silny protokół bezpieczeństwa (WPA2) i stwórz silne hasło.

W pierwszym rozdziale naszego ebooka dowiedziałeś się, jak stworzyć silne hasło.



2

Zadbaj o dostęp do routera Wi-Fi

- zmień dane logowania do routera (producenci często nadają identyczne login i hasło administratora, np. admin i admin),
- instaluj zalecane aktualizacje oprogramowania wewnętrznego routera (tzw. firmware),
- ogranicz w ustawieniach adresy IP, z których można zarządzać routerem,
- wyłącz zdalne zarządzanie routerem, jeśli nie jest Ci potrzebne.

3

Stwórz osobną sieć dla odwiedzających

Twoi goście nie mają złych zamiarów, ale ich urządzenia mogą być zarażone złośliwym oprogramowaniem, które może zaszkodzić Twojej sieci domowej i urządzeniom do niej podłączonym.

Jak bezpiecznie korzystać z Wi-Fi poza domem?

1

Wyłącz automatyczne łączenie się z sieciami Wi-Fi w ustawieniach swojego telefonu, tabletu czy komputera.
To da Ci kontrolę nad tym, do jakich sieci się podłączasz.

2

Nie łącz się z publicznymi, niezabezpieczonymi hasłem sieciami Wi-Fi (np. w hotelu, kawiarni, na lotnisku czy dworcu).

Jeżeli jednak musisz skorzystać z takich sieci, to **nie loguj się do kont w serwisach obsługowych** (bank, operator sieci komórkowej, sprzedawca prądu) **ani nie dokonuj płatności, podając swoje wrażliwe dane** (numer karty kredytowej, PESEL itd.). Dane przesyłane za pomocą niezabezpieczonej sieci Wi-Fi są widoczne dla przestępców i mogą zostać przechwycone!

3

Miej ograniczone zaufanie do publicznych sieci Wi-Fi, nawet jeśli są zabezpieczone hasłem.

Nie wiesz, kto oprócz Ciebie poznał hasło, a administratorzy otwartych sieci rzadko dbają o ich bezpieczeństwo (trudne do odgadnięcia hasła i częste jego zmiany).

4

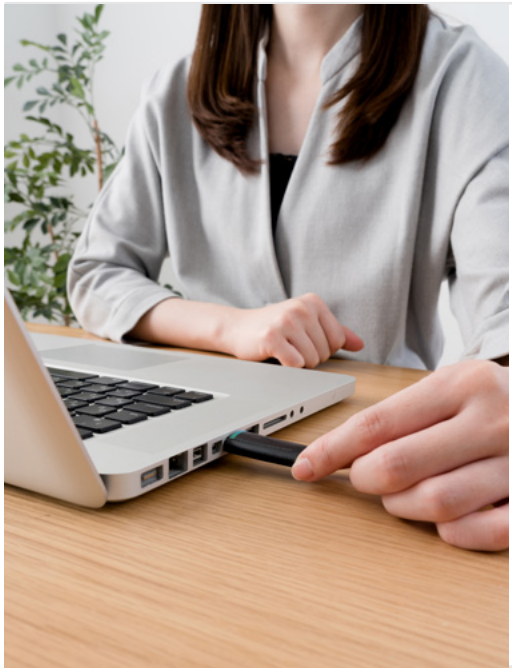
Jeżeli chcesz zalogować się do banku czy skorzystać z płatności internetowej, **użyj internetu mobilnego zamiast połączenia Wi-Fi.**

i

Jeśli używasz publicznego Wi-Fi, możesz zabezpieczyć się także za pomocą połączenia przez tzw. VPN. *Tunel VPN* szyfruje przesyłane w sieci dane, dlatego przestępcy nie są w stanie ich przechwycić.
Na rynku istnieją darmowe usługi VPN. Przy wyborze dostawcy upewnij się, że jest on godny zaufania.

Rozdział 9:

Jak bezpiecznie korzystać z urządzeń USB?



Urządzenia USB mogą przenosić niebezpieczne wirusy

Zewnętrzne nośniki USB mogą przenosić niebezpieczne wirusy, które są w stanie pozyskać hasła, loginy oraz dane osobowe przechowywane na Twoim komputerze.
Złośliwe oprogramowanie instaluje się na komputerze od razu po podłączeniu nośnika do urządzenia.

Dlatego miej ograniczone zaufanie do nośników nieznanego pochodzenia, np. znalezionych w kawiarni na stoliku czy otrzymanych od nowo poznanej osoby.

Przenośnym nośnikiem danych może być:

- dysk przenośny
- pendrive
- myszka
- bank energii
- cyfrowa ramka na zdjęcia
- lampka
- podgrzewacz do kubków
- wiatraczek
- inny gadżet podłączany do portu USB

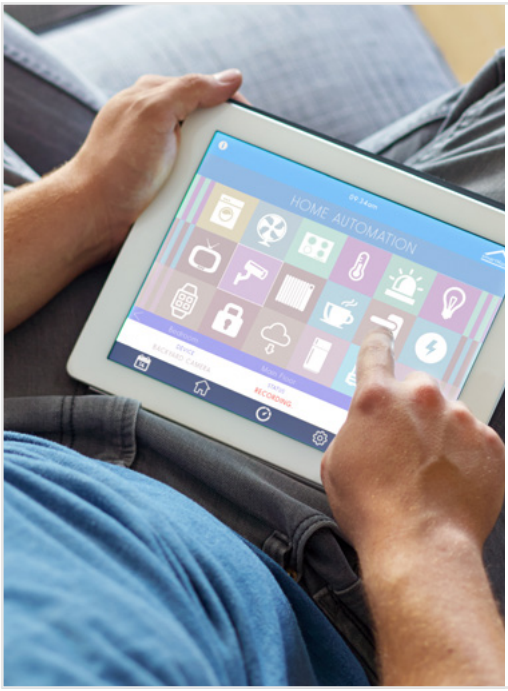
Pamiętaj!

Nieznane urządzenia USB to zawsze urządzenia niezaufane, a więc potencjalnie groźne. Dlatego nigdy nie podłączaj do swojego komputera żadnych urządzeń nieznanego pochodzenia!

Rozdział 10:

Jak zabezpieczyć urządzenia domowe?

Internet rzeczy - (z ang. Internet of Things, w skrócie IoT) urządzenia domowe, które są podłączone do internetu.



Bezpieczne urządzenia domowe

Jeśli coś jest podłączone do internetu, jest automatycznie narażone na cyberatak. Jeżeli źle zabezpieczysz swoje urządzenia IoT, ułatwisz przestępcom możliwość wykradania danych domowników, którzy korzystają z tej samej sieci.

Słabe zabezpieczenia w sprzętach IoT cyberprzestępcy wykorzystują do przestępstw, za które odpowiedzialność mogą ponosić właściciele urządzeń. Dlatego zawsze dokładnie czytaj instrukcje użytkowania sprzętów IoT, ponieważ znajdują się w nich informacje dotyczące sposobu konfiguracji i bezpieczeństwa.

Przykładowe urządzenia domowe, które są podłączone do internetu:

lodówka / telewizor (tzw. smart TV) / inteligentne czujniki

Jak zabezpieczyć urządzenia IoT?

- Podczas podłączania urządzeń do internetu, korzystaj z sieci, do której masz zaufanie, np. z własnego dobrze zabezpieczonego Wi-FI lub karty SIM.
- Jeśli możesz, oddziel swoje urządzenia IoT od sieci dla domowników. Możesz wykorzystać Wi-Fi dla gości zabezpieczone zaporą firewall. W ostateczności skorzystaj z rozwiązań GSM/kart SIM. Upewnij się jednak, czy producent urządzenia zapewnia odpowiednie zabezpieczenia.
- Nie udostępniaj nikomu numerów seryjnych ani modeli swoich sprzętów IoT.
- Zamień domyślne login i hasło do urządzenia na własne i nikomu ich nie przekazuj.
- Wyłącz opcję zdalnego dostępu oraz zdalnego zarządzania, aby nikt poza Tobą nie miał kontroli nad Twoim sprzętem.

- Aktualizuj oprogramowanie urządzenia IoT. Aktualizacje zawsze zwiększają bezpieczeństwo sprzętu.
- Sprawdź dokładnie domyślne ustawienia urządzenia i ustal własne. Zapoznaj się z ustawieniami prywatności i bezpieczeństwa – znajdziesz tam informacje, jakie dane są gromadzone i czy urządzenie może je udostępniać w sieci. Zdarza się, że producent ustawia zgodę na przesyłanie mu informacji na temat funkcjonowania urządzenia np. w celach statystycznych – może to naruszać Twoją prywatność, dlatego, jeśli się na to nie zgadzasz, zweryfikuj ustawienia sprzętowe.
- Po zakończeniu konfiguracji urządzenia pamiętaj, aby wylogować się z panelu administracyjnego.
- Nie korzystaj z niezaufanych urządzeń IoT, które nie spełniają kryteriów bezpieczeństwa (np. wymagają instalacji aplikacji spoza oficjalnych stron Google Play lub AppStore).

TAURON Polska Energia S.A.
ul. ks. Piotra Ściegiennego 3
40-114 Katowice

tauron.pl