Bezpieczeństwo **pracy zdalnej**

Kacper Szurek

https://security.szurek.pl

Nie publikuj **zdjęć** ekranu w mediach **społecznościowych**

Dla wielu osób praca zdalna jest czymś nowym – dlatego chcą się pochwalić swoim laptopem na mediach społecznościowych.

Na ekranie można znaleźć:

(pamiętaj o odbiciach w lustrze)

- adresy wewnętrznych stron
- dane kontrahentów
- fragmenty emaili
- dane osobowe
- kod źródłowy

Zdjęcie z ekranem zalogowanego użytkownika może wiele powiedzieć potencjalnemu włamywaczowi.
Mogą się tam znaleźć fragmenty rozmów na komunikatorach, adresy email czy inne – potencjalnie wrażliwe dane.

Nie zmieniaj **numeru konta** kontrahenta

Jeżeli otrzymałeś email, z której wynika, że kontrahent/współpracownik zmienił numer swojego konta bankowego – uważaj. Może to być oszustwo „na dyrektora” gdzie przestępca podszywa się pod prezesa firmy i prosi o wykonanie przelewu.

Atak „na prezesa”

(podszycie się pod ważną osobę)

1. Podszyj się pod dyrektora
2. Poproś o zmianę konta
3. Zleć przelew

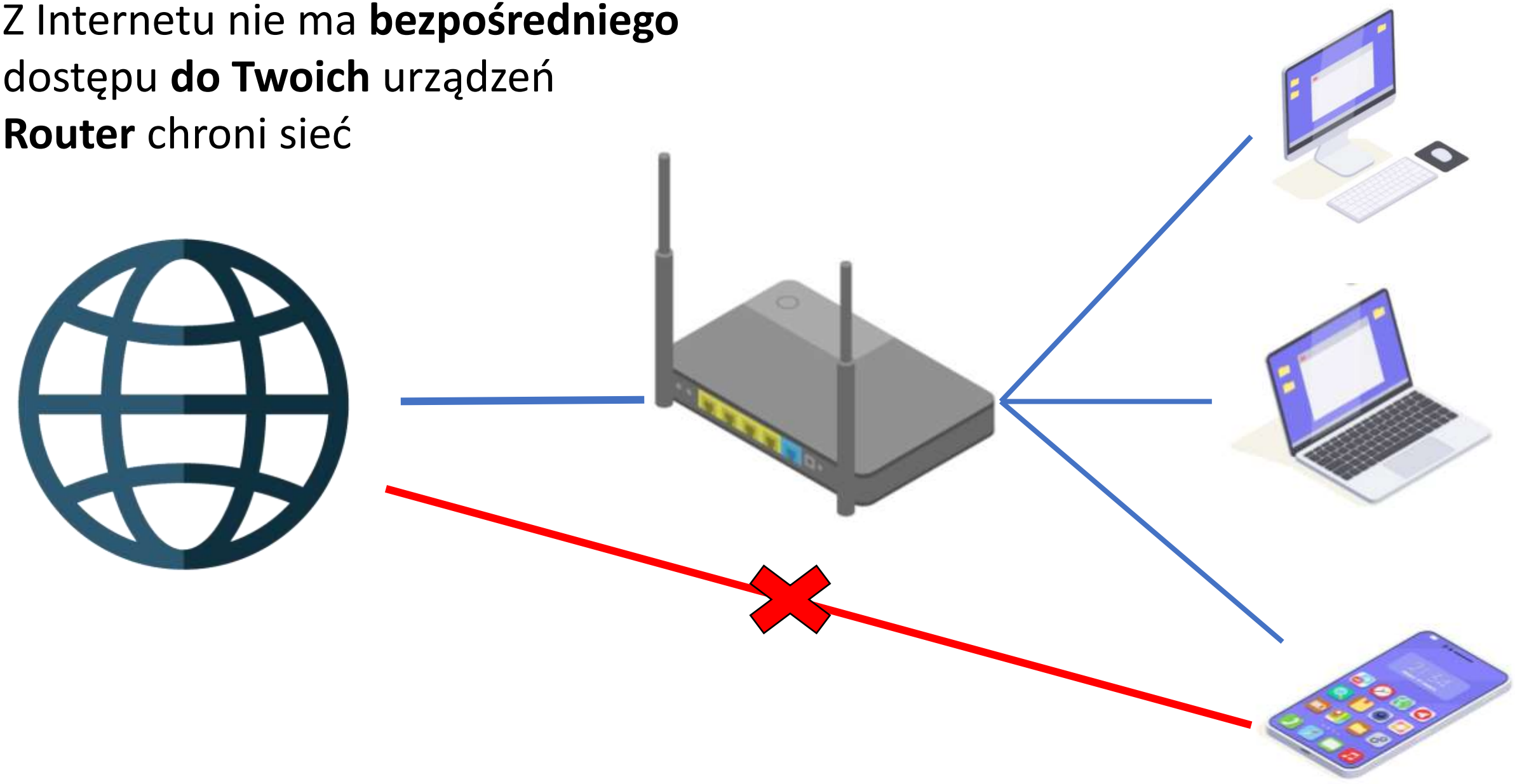
Jeżeli jesteś księgową odpowiedzialną za finanse w firmie – każda zmiana numeru konta powinna mieć ustaloną procedurę. Na przykład potwierdzenie zmiany poprzez kontakt na ustalony w umowie numer telefonu.

- Włącz **WPA2** z AES
- Wyłącz **WPS**
- Zmień **hasło** administratora

Bezpieczeństwo routera wpływa na bezpieczeństwo komputera firmowego, domowego, drukarki i wszystkich urządzeń IoT.

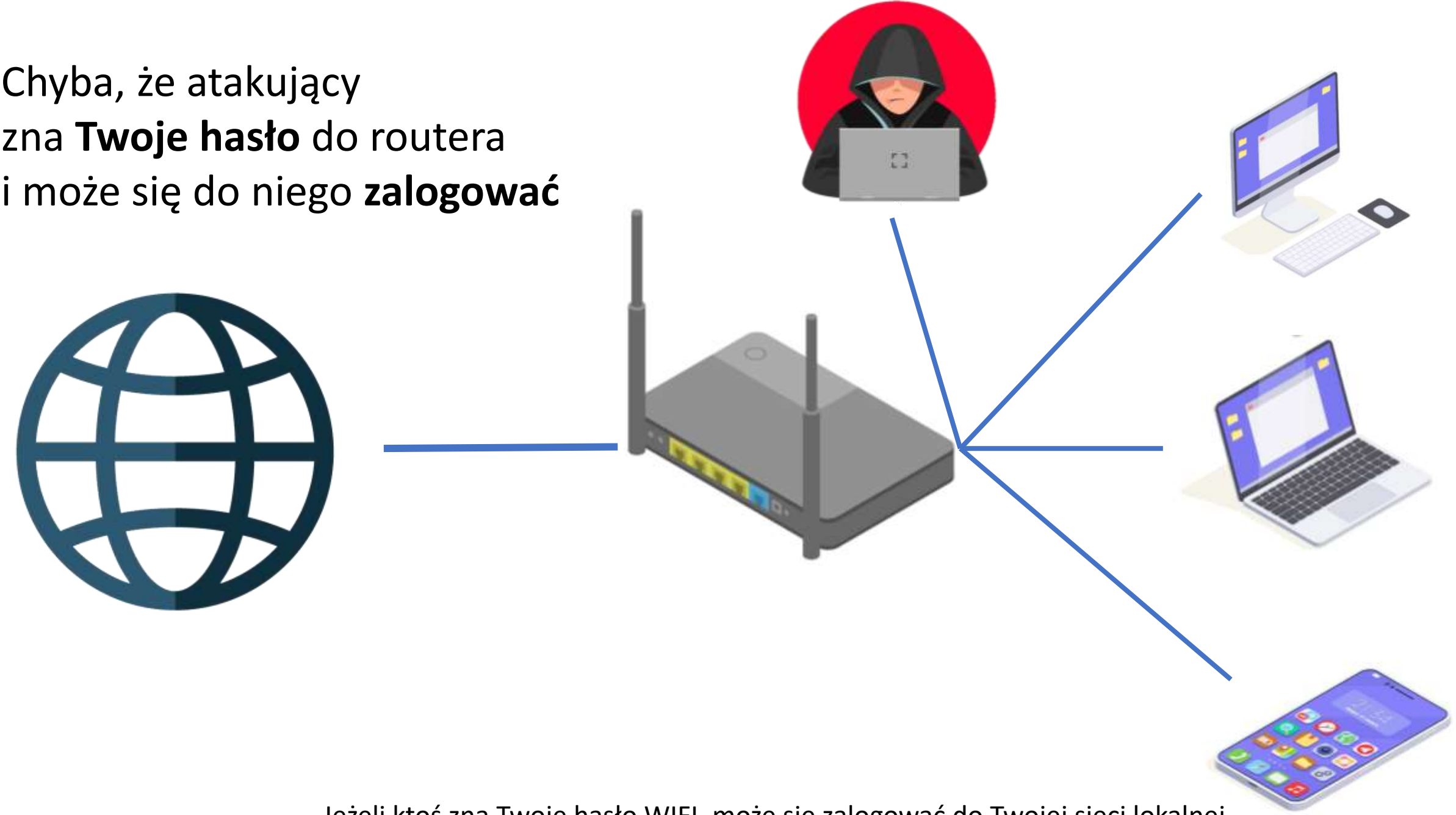
Z Internetu nie ma **bezpośredniego** dostępu **do Twoich** urządzeń

Router chroni sieć



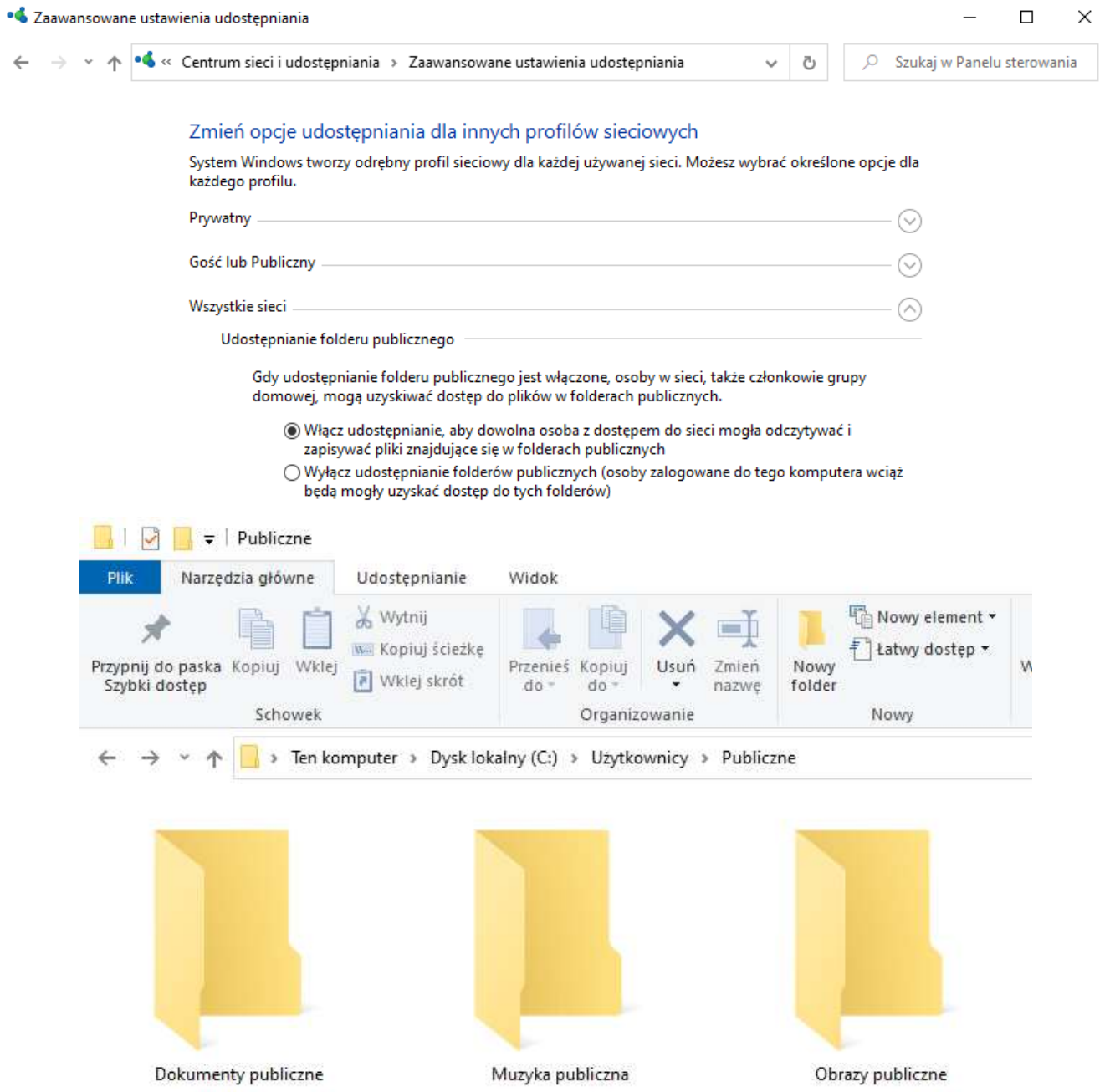
NAT i Firewall sprawiają, że z Internetu nie ma bezpośredniego dostępu do Twoich urządzeń.
Ty możesz się łączyć ze stronami ale one z Tobą już nie.

Chyba, że atakujący
zna **Twoje hasło** do routera
i może się do niego **zalogować**



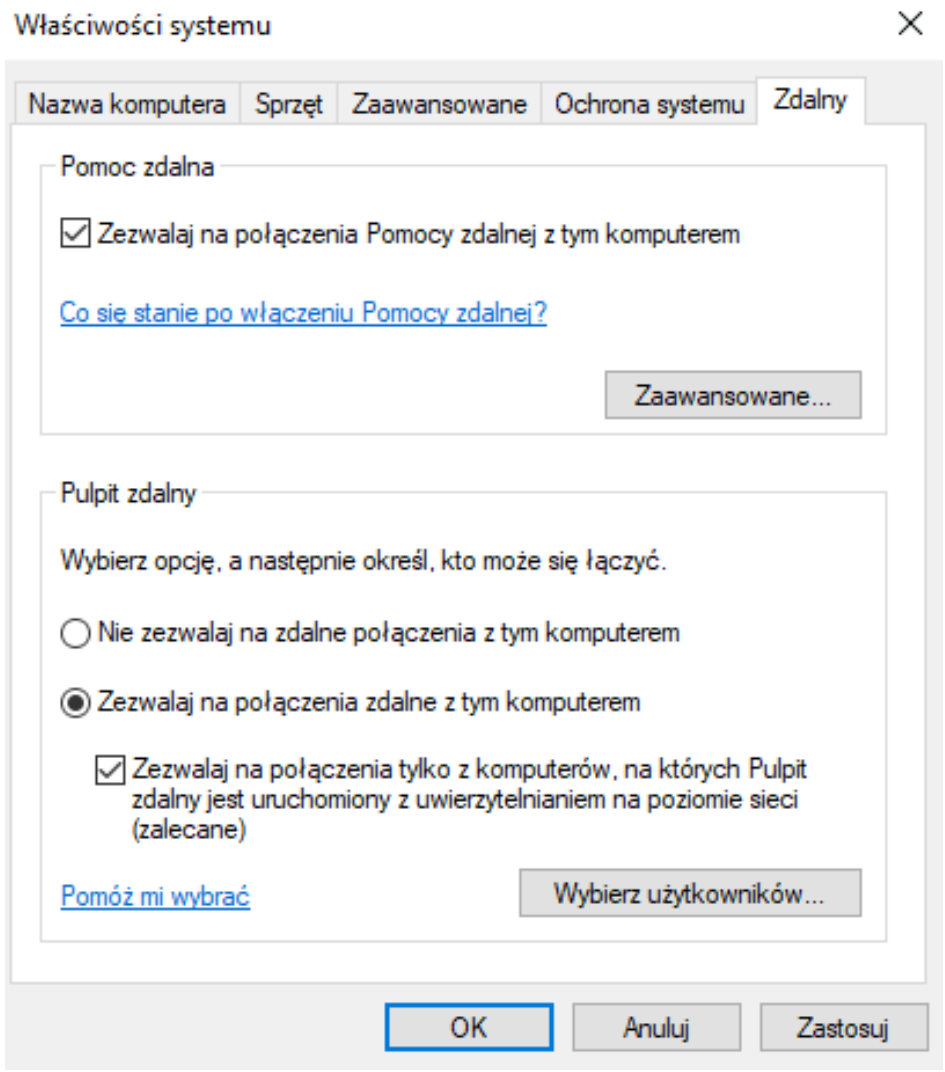
Jeżeli ktoś zna Twoje hasło WIFI, może się zalogować do Twojej sieci lokalnej.
Jest wtedy traktowany jak każde inne urządzenie domowe.

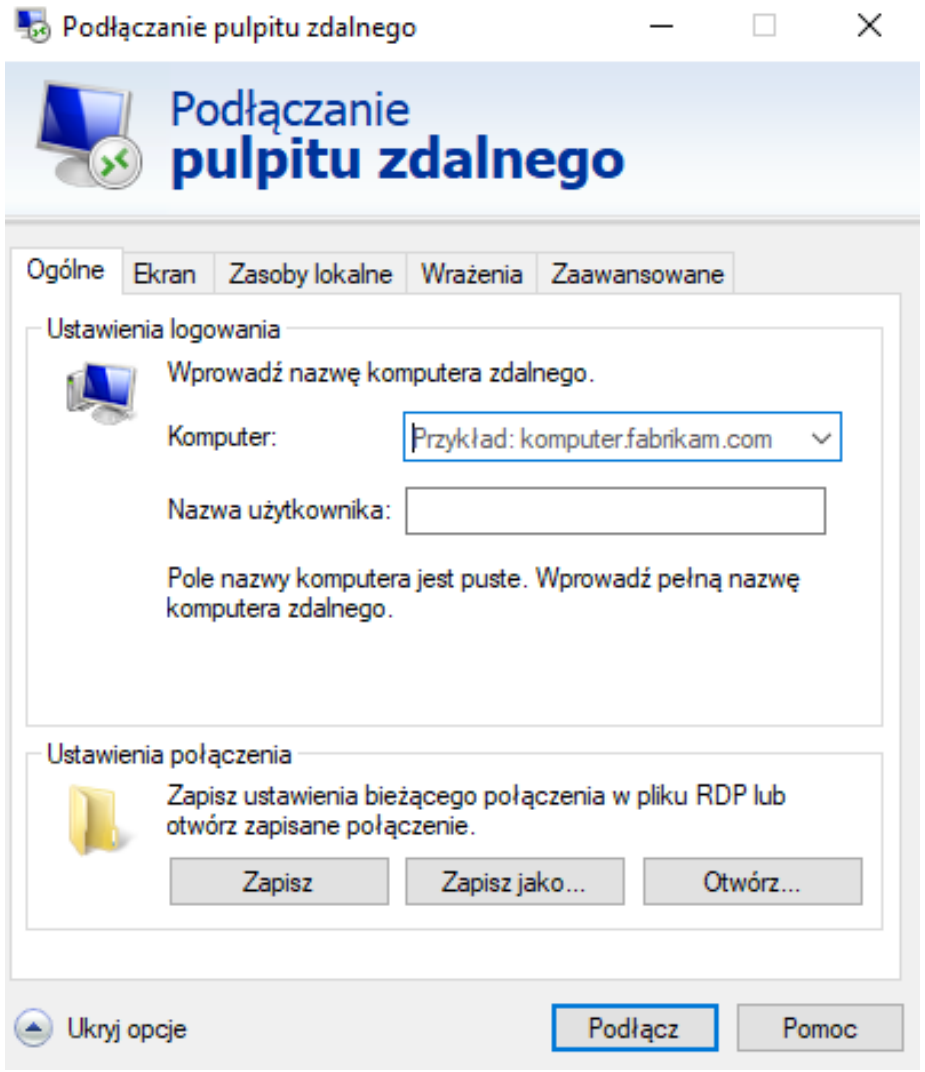
Może wtedy pobrać
pliki
z udostępnionych
publicznie **folderów**



W Windowsie można uruchomić udostępnianie plików z folderu publicznego.
Dzięki temu inne komputery w sieci lokalnej mają dostęp do Twoich plików – w tym atakujący, który podłączył się do WIFI.

Lub próbować **połączyć** się z komputerem przy użyciu **pulpitu zdalnego**





Znając IP komputera można się do niego zalogować przy pomocy pulpitu zdalnego.
Jeśli przestępca zna (lub odgadnie) Twoje hasło – może się zalogować do komputera.
Normalnie Twój komputer nie jest dostępny z Internetu – teraz jednak atakujący jest w Twojej sieci.

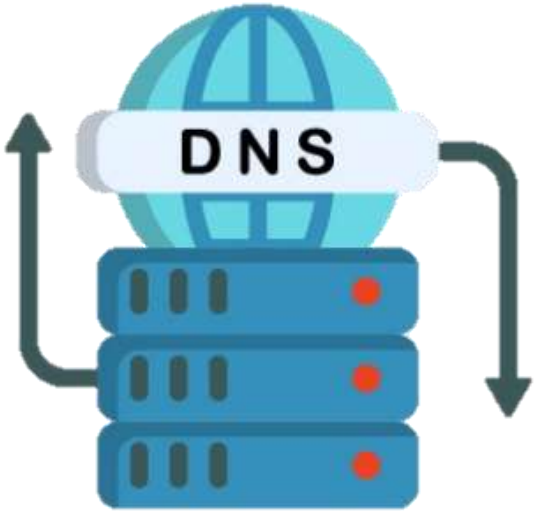
Zmieniając serwer DNS dowie się **jakie witryny** odwiedzamy

Jaki adres **IP** ma **google.pl**

216.239.32.117

Jaki adres **IP** ma **serwis_dla_dorosłych**

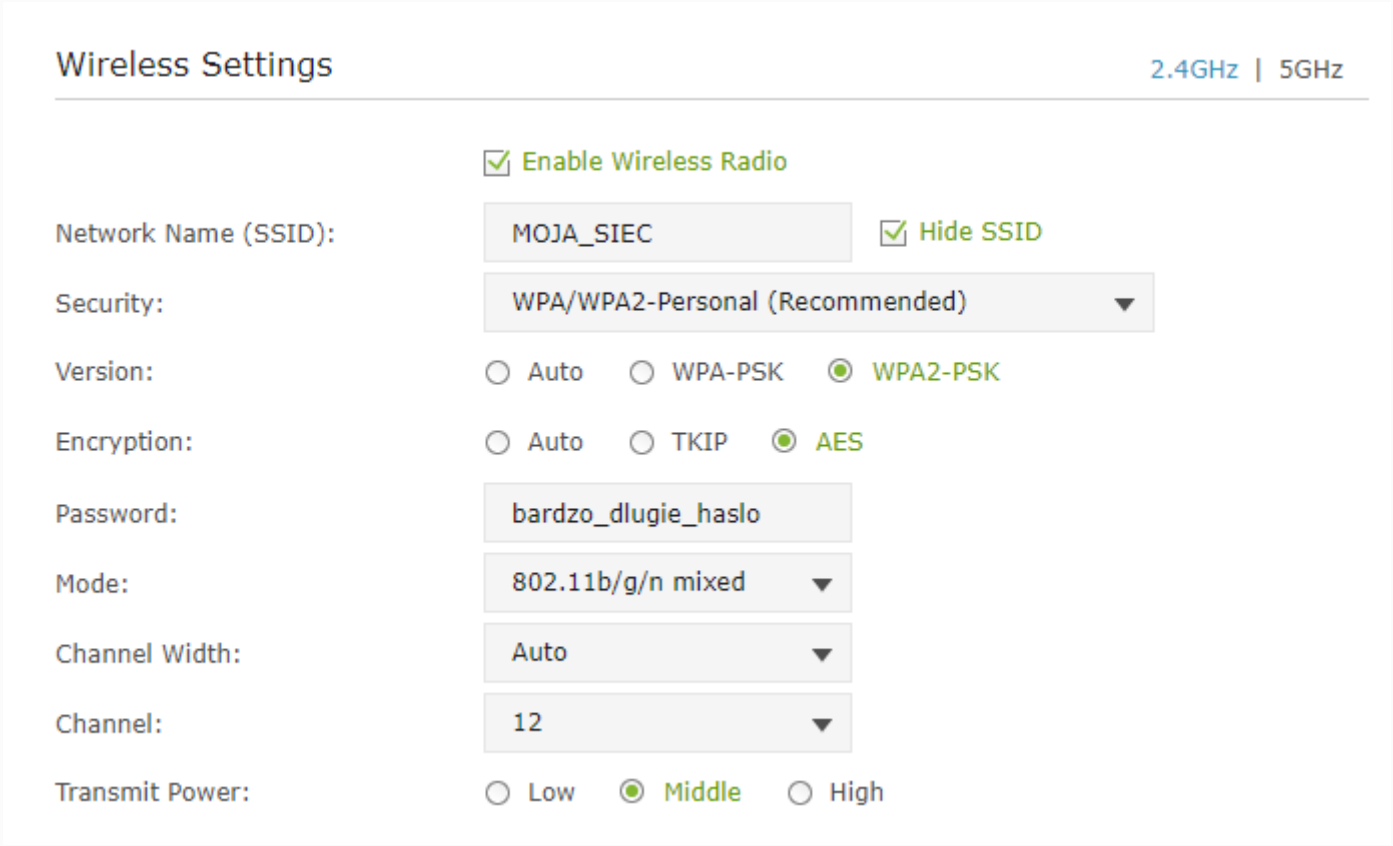
X.X.X.X



Cały nasz ruch Internetowy przechodzi przez domowy router.
Jeżeli atakujący zmieni na nim serwer DNS – to w automatycznej konfiguracji Windows zacznie używać go do sprawdzania domen.
Każde zapytanie o dowolną domenę (np. szurek.pl) trafi nie do naszego operatora – ale do przestępcy.

Ustaw **WPA2** z AES z długim i skomplikowanym **hasłem**

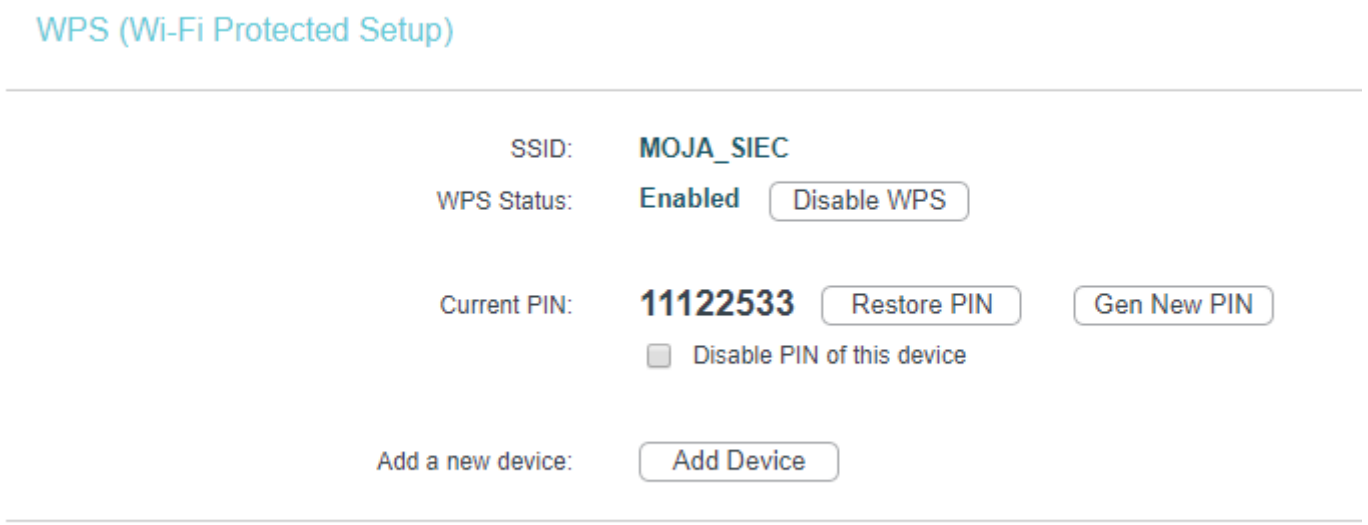
(żebyś tylko Ty korzystał ze swojego Internetu)



Ustawienia routerów różnią się w zależności od producenta.
Najpierw musimy zalogować się do panelu administratora – zazwyczaj znajdującego się pod adresem 192.168.1.1.
Ta konfiguracja określa jakiego hasła będziemy używać do połączenia się z naszą domową siecią WIFI.

Wyłącz **WPS**

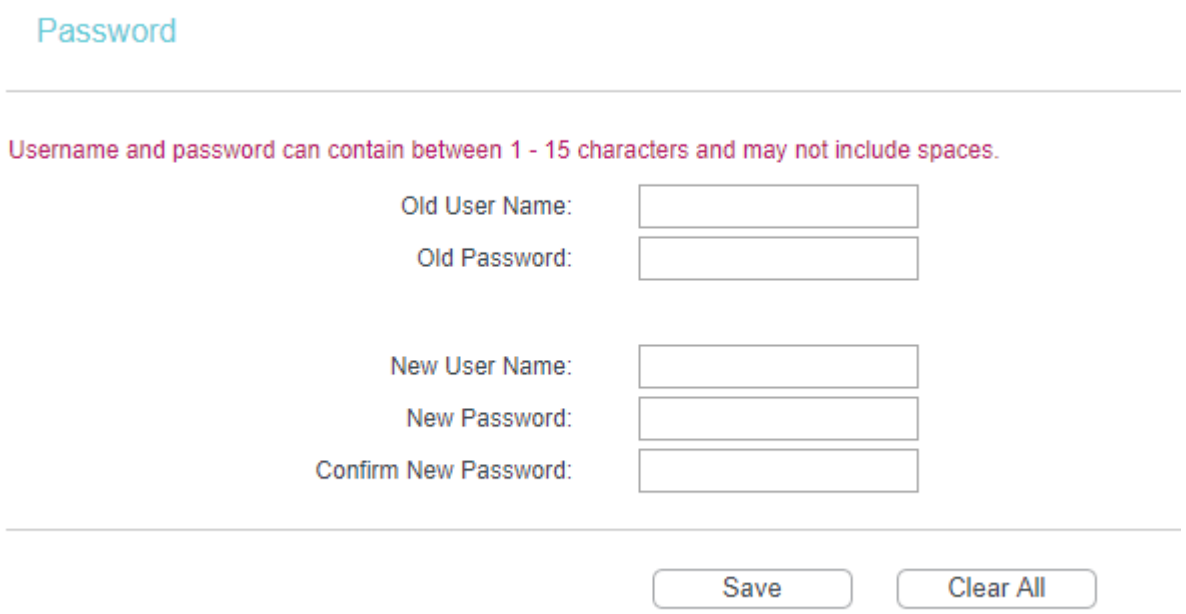
(to stara, niebezpieczna alternatywa dla hasła WIFI)



Wymyślono, że hasła WIFI są mało przyjazne dla użytkownika.
WPS pozwala na zalogowanie się do sieci przy pomocy kodu PIN lub wciśnięcia fizycznego guzika na obudowie routera.
Obecnie uznaje się to rozwiązanie za niebezpieczne i powinno się je wyłączyć.

Zmień hasło **administratora**

(tylko Ty powinieneś mieć dostęp do panelu admina)



Logując się do panelu administratora można zmienić wiele opcji – chociażby otworzyć niektóre porty.
Wtedy możliwy jest bezpośredni dostęp do komputera z Internetu.
Dlatego warto zmienić standardowe hasło w stylu (admin/admin) na bardziej skomplikowane.

Blokuj ekran gdy **odchodzisz** od komputera

Blokowanie komputera gdy od niego odchodzimy to dobry nawyk – nawet jeśli mieszkamy sami.
Sprawny atakujący potrzebuje jedynie kilku sekund, aby przy pomocy specjalnego pendrive’a zarazić nasz komputer.

Dzieci mogą:

(lub współlokatorzy)

- coś usunąć
- włączyć
- kliknąć

Jesteśmy odpowiedzialni za bezpieczeństwo firmowego komputera.
Dzieci (i inne nieupoważnione osoby) nie powinny mieć do niego dostępu.

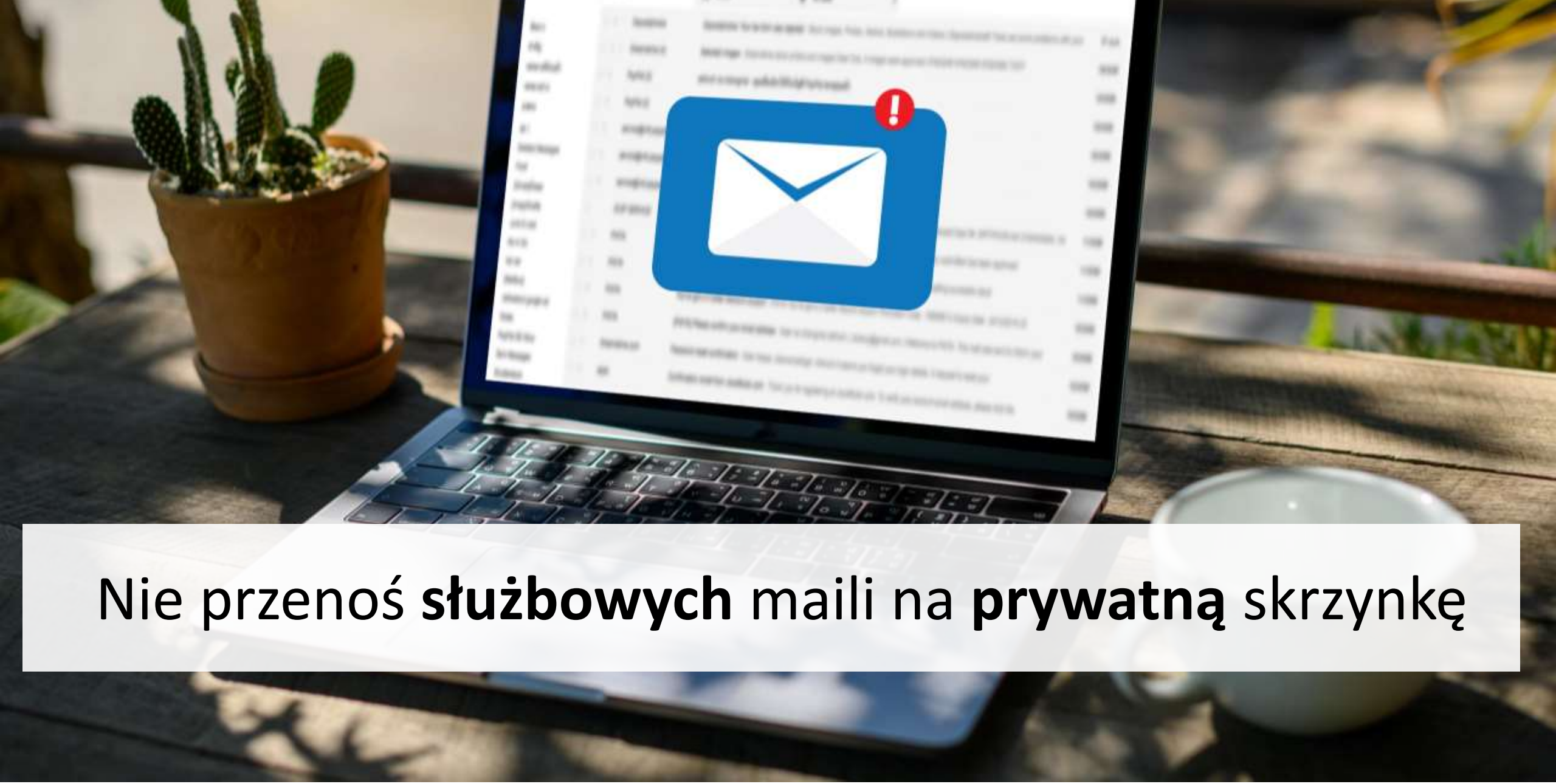
Nie **instaluj** na komputerze firmowym:

- gier
- nielegalnego oprogramowania
- nieautoryzowanych aplikacji

Nielegalne oprogramowanie można narazić nas (i firmę) na kary finansowe w przypadku kontroli legalności oprogramowania.
Aplikacje z niepewnych źródeł mogą również zawierać złośliwe oprogramowanie.

Nieautoryzowana aplikacja
może wywołać
alarm u kolegów
z działu **bezpieczeństwa**
(i może być złośliwa/niebezpieczna)

Jeżeli nasza firma korzysta ze specjalnego oprogramowania, każda instalacja (bądź uruchomienie) nowego programu powoduje pojawienie się specjalnego alertu w panelu działu bezpieczeństwa.
Dla nas gra może być niewinną formą rozrywki – dla firmy natomiast potencjalnym zagrożeniem.
Nie ma bowiem pewności czy takie oprogramowanie nie zawiera dodatkowej, złośliwej funkcjonalności.



Nie przenoś **służbowych** maili na **prywatną** skrzynkę

Jeżeli Twój komputer ma zablokowane porty USB, możesz próbować przenosić firmowe dokumenty poprzez prywatną pocztę. Nie powinieneś tego robić – dane firmowe nie powinny opuszczać autoryzowanych urządzeń.

Kopiując dane:

(poza infrastrukturę firmową)

- Ciężko je usunąć
- RODO/GDPR
- Możesz naruszać tajemnice przedsiębiorstwa

Dane raz wysłane do Internetu – bardzo ciężko z niego usunąć.
Korzystając z zewnętrznych darmowych usług nie masz pewności co dzieje się z wprowadzonymi tam danymi.
Dla przykładu, mogą być one przeglądane przez automaty w celu profilowania reklam.

Upewnij się, że **dysk** twardy jest **zaszyfrowany**

Popularne rozwiązania to Bitlocker i FileVault.
W popularnej konfiguracji przed ekranem logowania musimy podać dodatkowy kod PIN do odszyfrowania dysku.

Komputer może zostać **skradziony**:

(lub zgubiony wraz z danymi)

- z mieszkania
- z autobusu
- z kawiarni
- z plecaka

Komputer może zostać skradziony – wraz ze wszystkimi znajdującymi się na nim danymi.
Szyfrowanie sprawia, że bez znajomości odpowiedniego hasła – odczytanie danych jest bardzo utrudnione.

Nie **drukuj** dokumentów bez **zezwolenia**

Pamiętaj o **niszczarce**

Niektóre drukarki mogą zapisywać wysyłane do nich dokumenty w swojej pamięci wewnętrznej.
W domu zazwyczaj nie posiadamy niszczarki, która pozwalałaby na bezpieczną utylizację dokumentów.

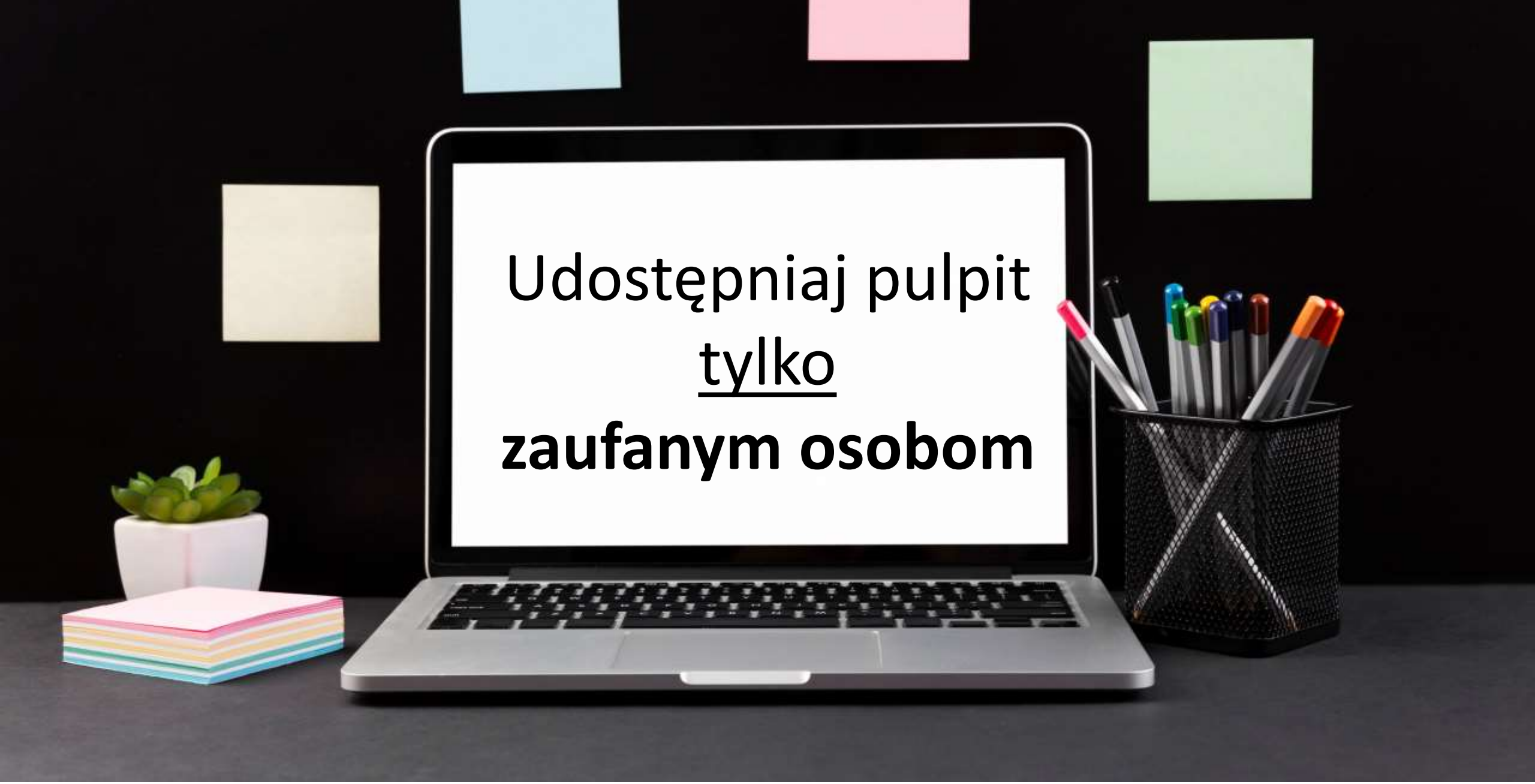
Na śmietniku

(lub starych pendrive'ach)

można znaleźć różne dane

(również osobowe)

Trwałe zniszczenie dokumentów (lub dysków twardych) nie jest takie proste.
Nie wyrzucaj firmowych danych do kosza na śmieci.



Niektóre aplikacje pozwalają na udostępnienie naszego ekranu osobie po drugiej stronie łącza.
Pozwala to na zdalną pomoc w przypadku problemów z komputerem.

Support może
zdalnie pomóc
łącząc się z Twoim
pulpitem
(tak samo przestępcy)
dlatego <u>weryfikuj</u>
***kto** prosi o dostęp*

Taka funkcja może zostać wykorzystana przez przestępców do przejęcia kontroli nad naszym komputerem.
Przed udzieleniem dostępu zawsze zweryfikuj czy osoba po drugiej stronie jest rzeczywiście tym za kogo się podaje.

Sprawdź, czy w telekonferencji uczestniczą tylko **autoryzowane osoby**

Podczas spotkań często dyskutujemy o wrażliwych kwestiach.
Sprawdź jak Twoje oprogramowanie do wideokonferencji przedstawia użytkowników w danym pokoju.

Niektóre serwisy wymagają jedynie **podania adresu URL** aby dołączyć do **rozmowy**

W niektórych aplikacjach żeby dołączyć do rozmowy wystarczy jedynie znać odpowiedni adres URL (nie potrzeba loginu i hasła). Jeżeli taki link wycieknie poza organizację – atakujący może spróbować niepostrzeżenie dołączyć do pokoju i nas podsłuchiwać.

Aktualizuj oprogramowanie

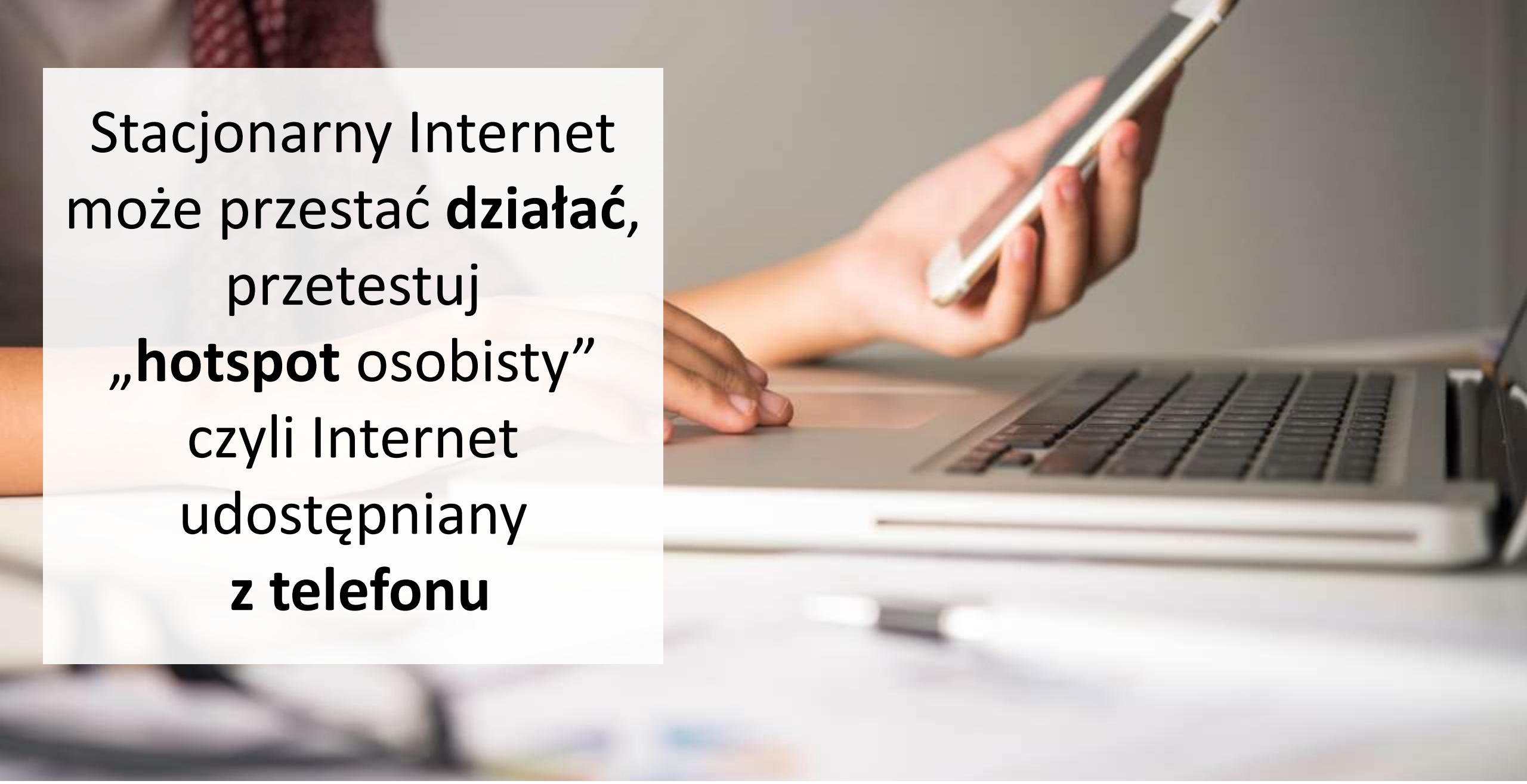
Błędy są odnajdywane cały czas – również podczas ogólnoświatowej epidemii.
Aktualizacja systemu operacyjnego i używanych aplikacji jest istotna z punktu widzenia bezpieczeństwa.

Zarażony komputer
(podłączony do firmowego VPN-a)
może zarażać inne
komputery
(podłączone do firmowego VPN-a)

Złośliwe aplikacje (podobnie jak wirusy) mogą próbować zarażać inne urządzenia.
Jeżeli korzystamy z firmowego VPN-a, malware może próbować infekować inne, niezaktualizowane systemy operacyjne.

Przygotuj **zapasowe** połączenie z **Internetem**

Do pracy zdalnej często konieczny jest dostęp do Internetu.
Przygotuj się na sytuacje awaryjną – kiedy to Twoje standardowe łącze może przestać działać (lub będzie bardzo wolne).



Stacjonarny Internet może przestać **działać**, przetestuj „**hotspot** osobisty” czyli Internet udostępniany **z telefonu**

Większość telefonów komórkowych pozwala na udostępnienie Internetu LTE poprzez sieć WIFI.
Wtedy nasz komputer łączy się z telefonem, który udostępnia mu Internet mobilny.

Nie **instaluj** zbędnych aplikacji na **służbowym** telefonie

Jeżeli oprócz laptopa otrzymałeś firmowy telefon – ogranicz liczbę instalowanych na nim aplikacji.
Każda dodatkowa gra/aplikacja zwiększa prawdopodobieństwo infekcji złośliwym oprogramowaniem.

Ikony, **opisy**, **oceny** i recenzje aplikacji (w Google Play) o niczym nie świadczą

(mogą być fałszywe i kupione)

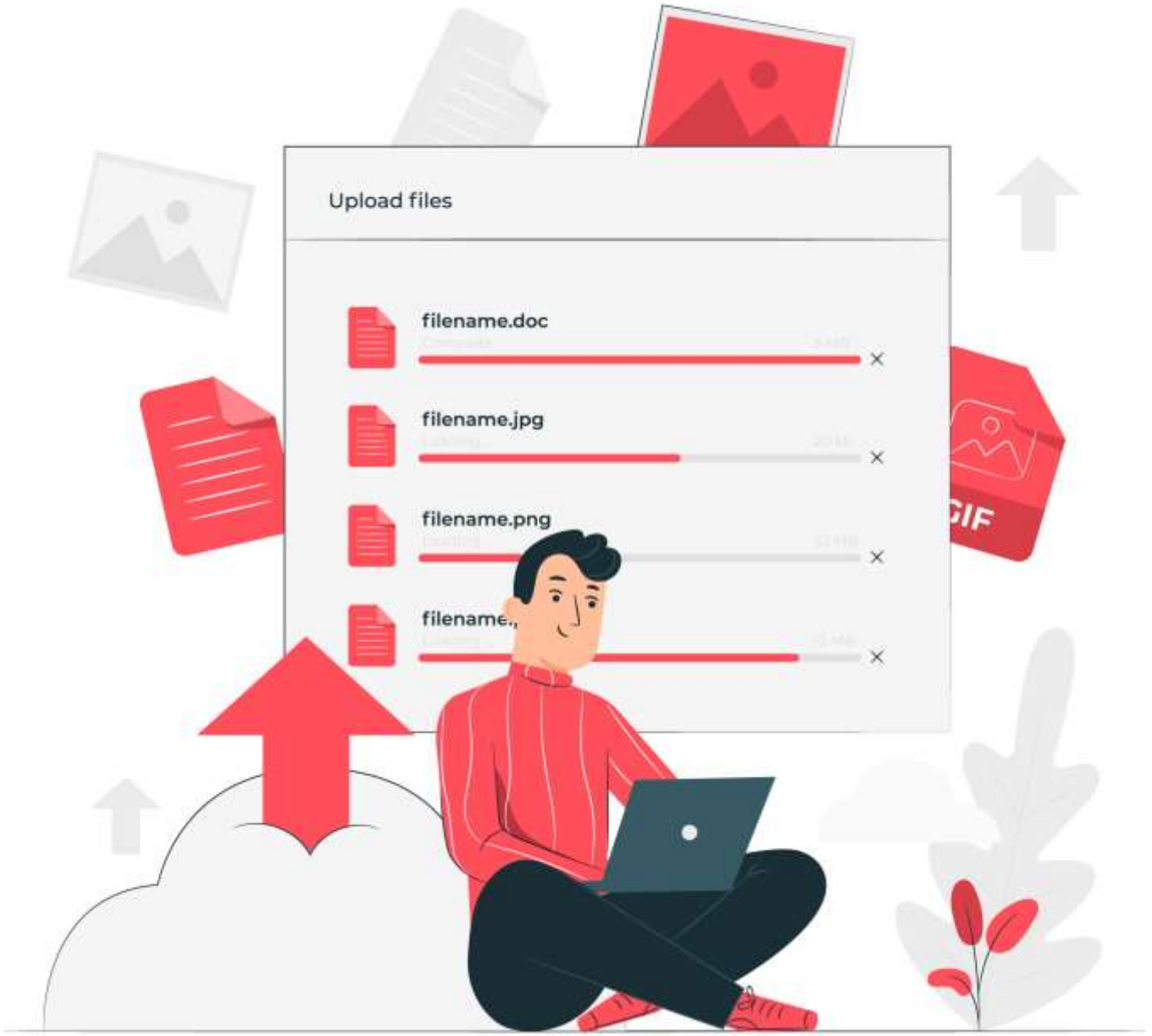
Złośliwe aplikacje próbują wyglądać identycznie jak oryginalne programy – dlatego kopiują ich opisy oraz ikony.
Recenzje aplikacji mogą zostać kupione na czarnym rynku.
Odróżnienie prawdziwej gry od tej fałszywej może nie być takie proste jak myślisz.

Unikaj **skanowania** dokumentów **telefonem**

Nowoczesne telefony pozwalają na szybkie i proste skanowanie dokumentów służbowych.
Należy jednak zwrócić uwagę na ich odpowiednią konfigurację.

Telefon może **automatycznie** wysyłać takie zdjęcia <u>do chmury</u>

(więc sprawdź ustawienia)



Sprawdź czy zdjęcia (i dokumenty) nie są automatycznie wysyłane do chmury producenta telefonu.
Może to być sprzeczne z firmową polityką bezpieczeństwa.

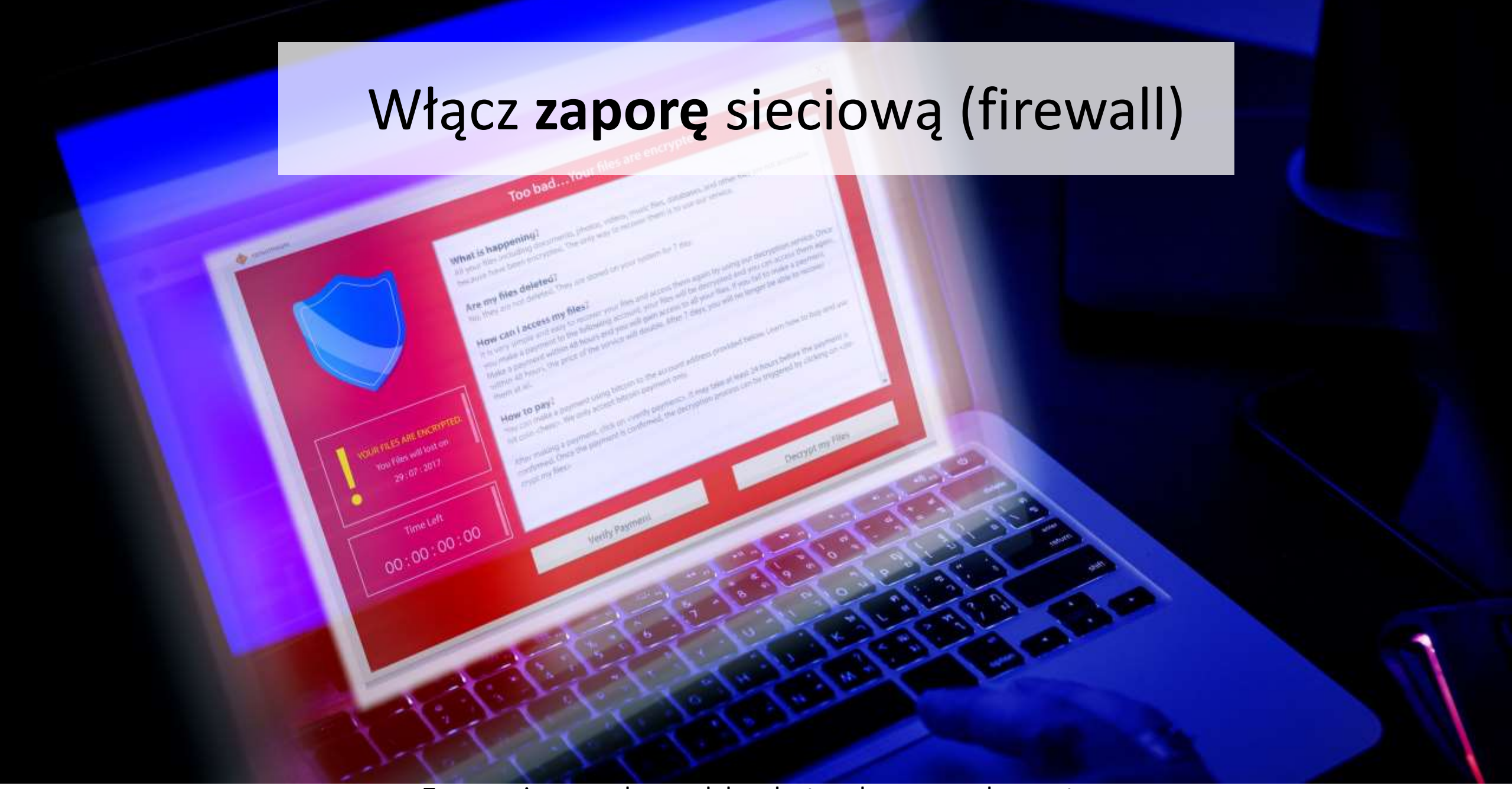
Nie wysyłaj **plików** na prywatne serwery

Email posiada limit wielkości przesyłanego pliku.
Jeżeli musisz przesłać większy plik, unikaj używania darmowych serwisów do wysyłania plików.

Do wysyłania
dużych plików
(i kawałków kodu)
używaj tylko
zatwierdzonych
witryn

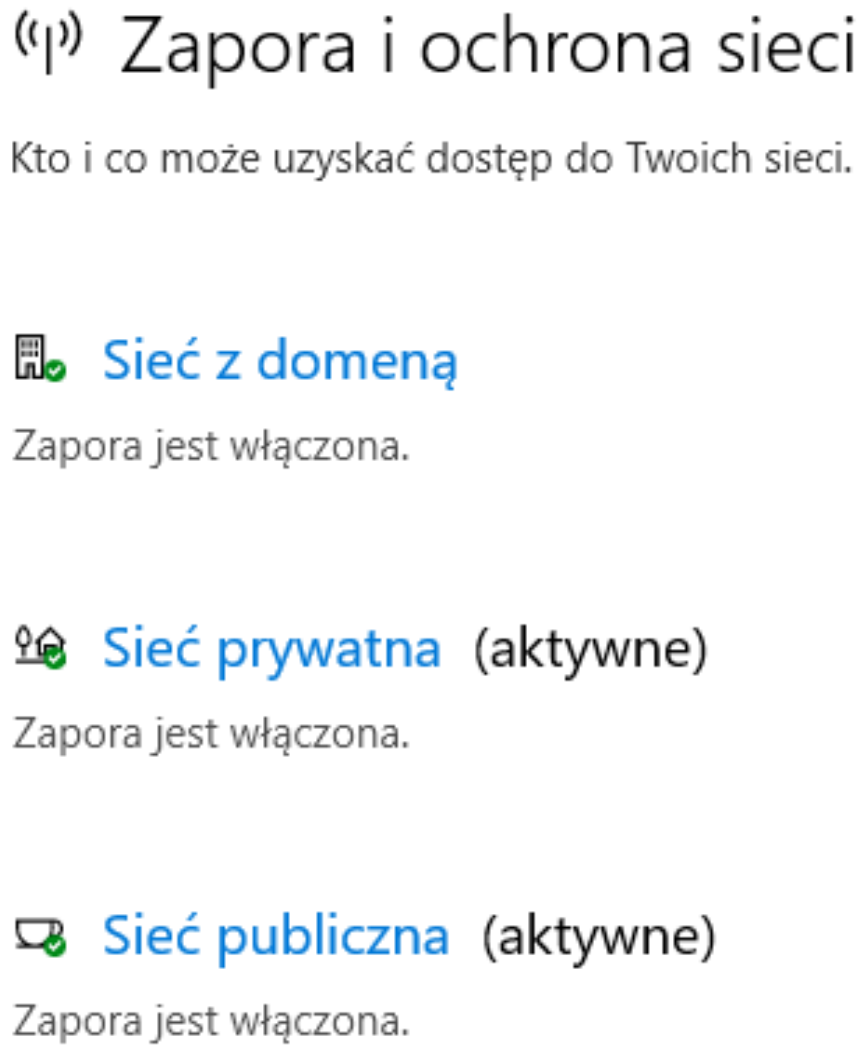
Korzystając z darmowych rozwiązań nie masz pewności co zrobią z przesłanymi tam danymi.
Zapytaj swojego pracodawcę czy posiada wykupioną odpowiednią usługę przeznaczoną do przesyłania plików.

Włącz **zaporę** sieciową (firewall)



Zapora nie pozwala na zdalny dostęp do naszego komputera.
W większości przypadków powinniśmy zablokować wszystkie połączenia przychodzące.

Zapora określa kto *(i jak)* może się **łączyć** z Twoim **komputerem**

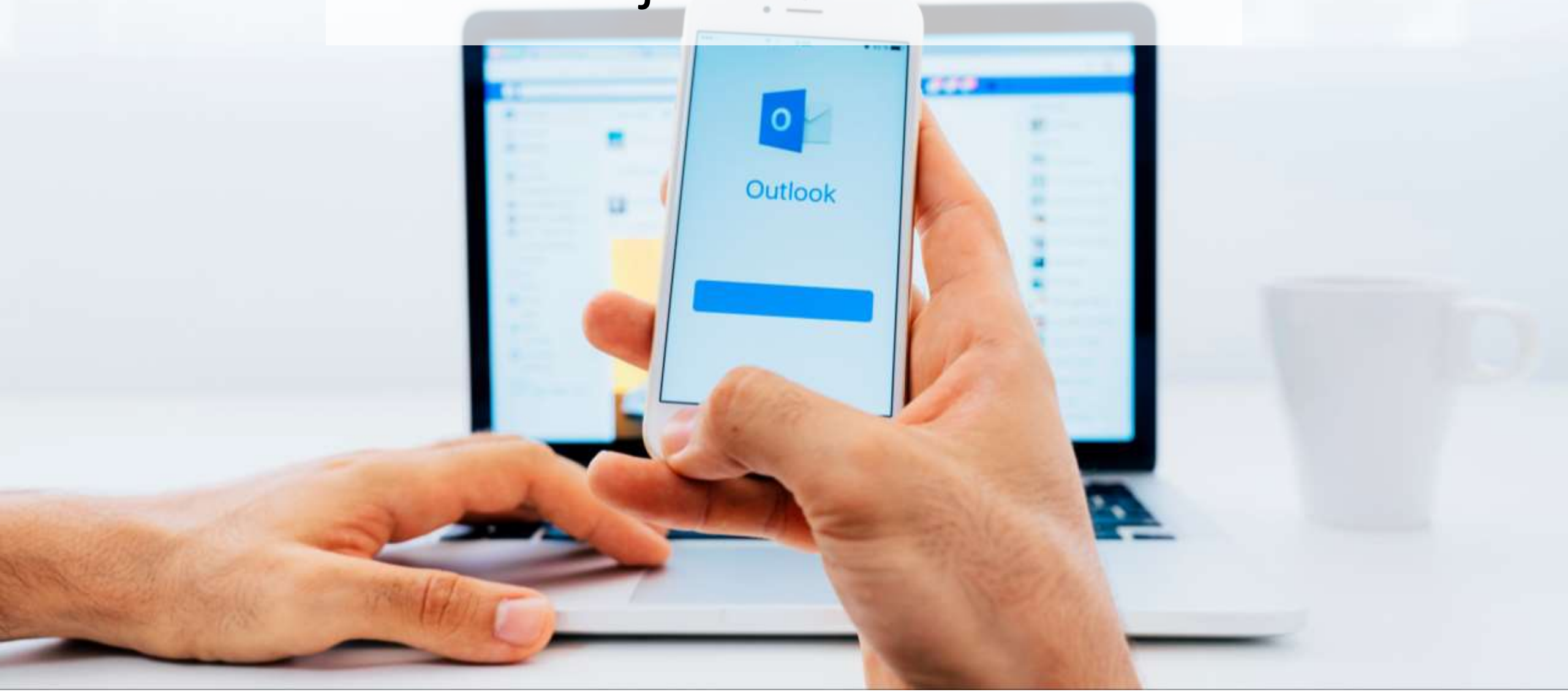


Jeżeli na naszym komputerze jest złośliwe oprogramowanie – zaklejenie kamery niewiele nam pomoże.

Żeby uniknąć wysyłania
prywatnych rozmów
i/lub
zdjęć w **dresach**
i szlafrokach

Może jednak pomóc uniknąć sytuacji w których nasi współpracownicy widzą nas wtedy kiedy tego nie chcemy.

Nie klikaj w **linki** w **mailach**



Jeżeli w emailu znajduje się odnośnik do strony, która prosi o login i hasło – może to być przykład phishingu.

Rozróżnisz GOOGLE.pl od G00GLE.pl ?

(pisane z użyciem zer)

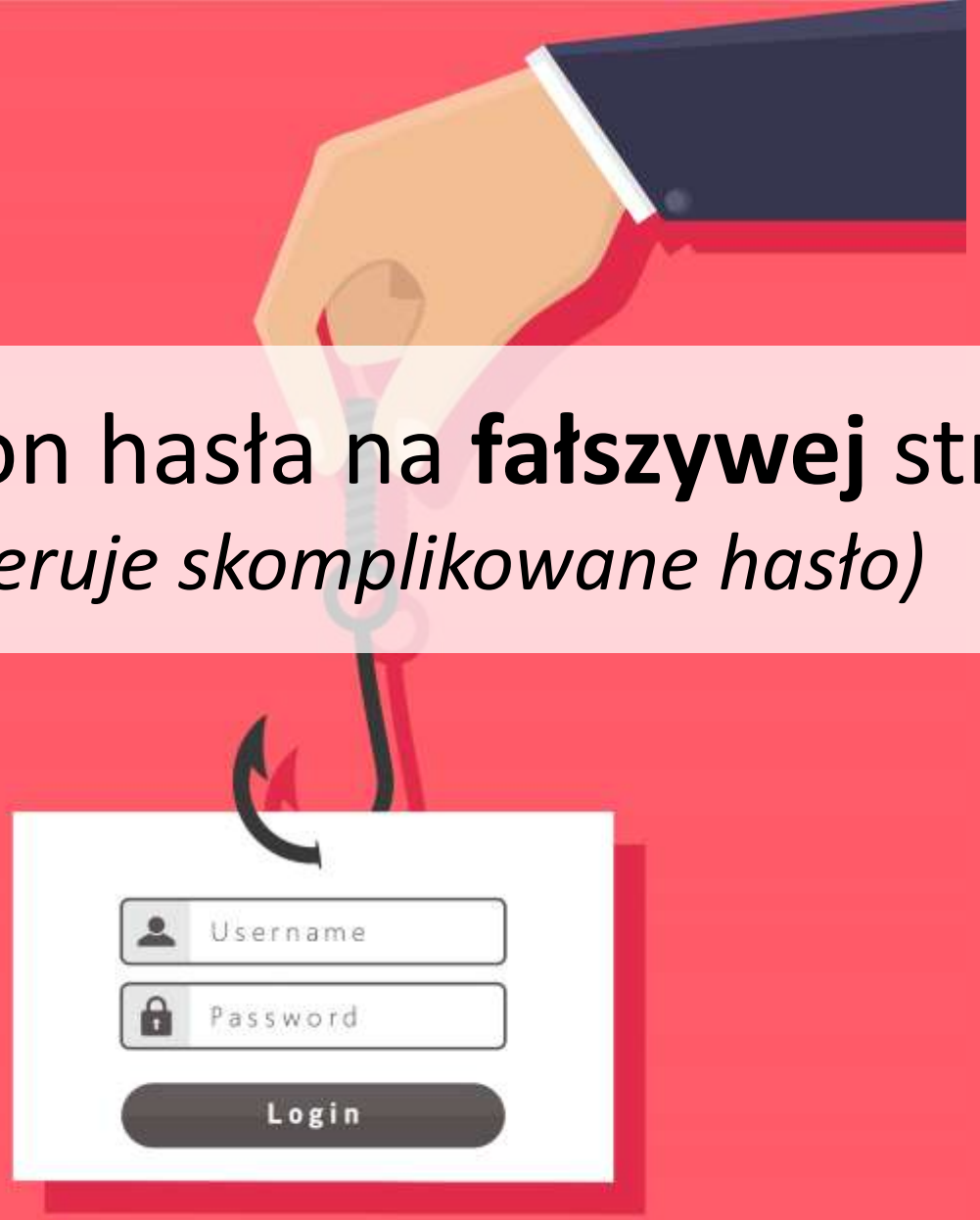
Przestępcy próbują w ten sposób podszyć się pod znane strony i wykraść nasze loginy i hasła.

Zacznij korzystać z **menadżera haseł**

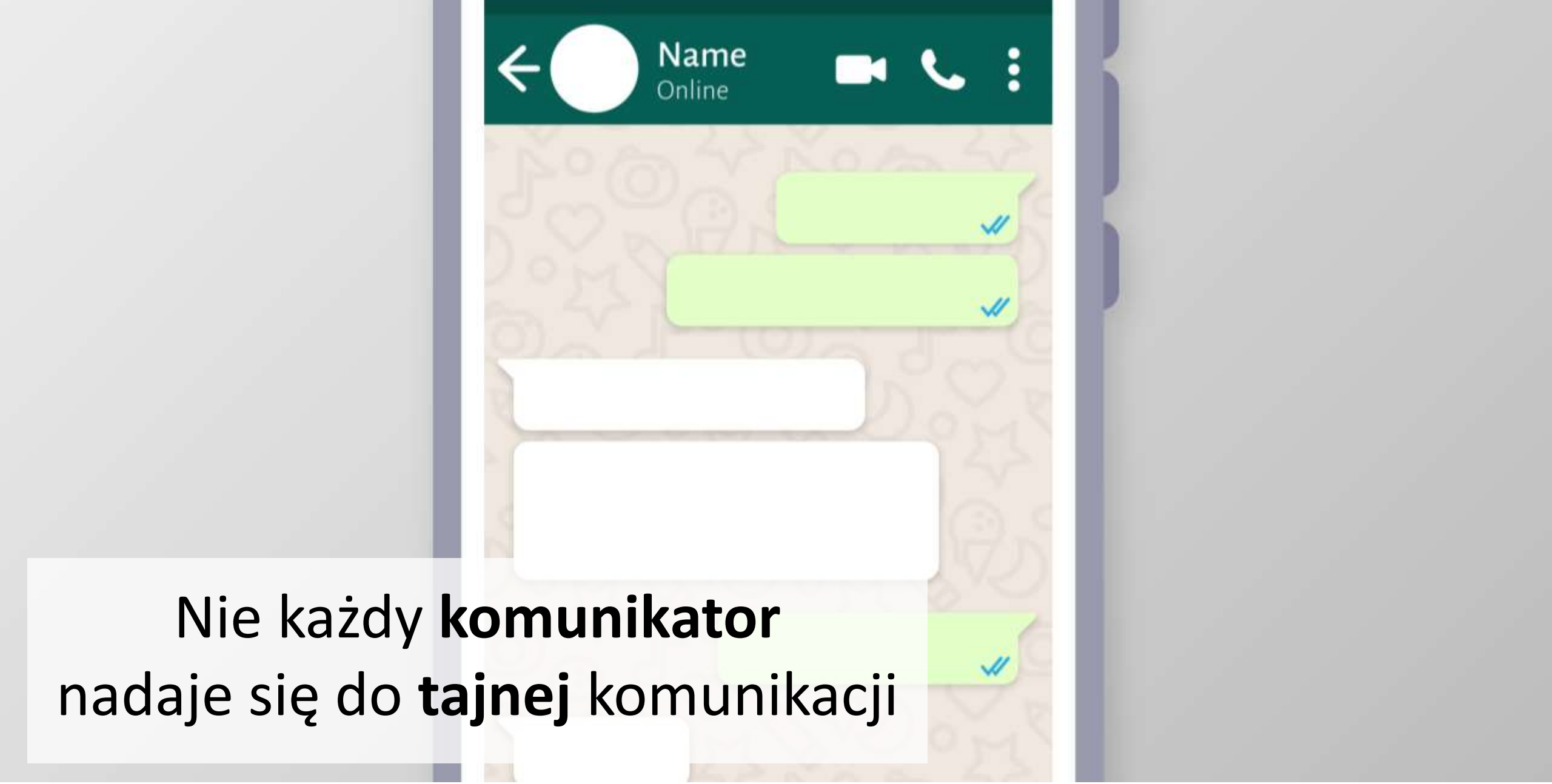
Jedną z metod obrony przez phishingiem może być menadżer haseł.

Nie wypełni on hasła na **fałszywej** stronie

(i wygeneruje skomplikowane hasło)



Gdy raz zalogujemy się do witryny – menadżer zapisze nasze hasło oraz jej adres.
Gdy ktoś spróbuje się podszyć pod taką stronę – menadżer nie wypełni na niej naszego hasła – ponieważ nie zgadza się adres.



Nie każdy **komunikator** nadaje się do **tajnej** komunikacji

Nie każdy komunikator używa szyfrowania end-to-end czyli takiego, w którym treść zna tylko nadawca i odbiorca. Niektóre z nich w standardowej konfiguracji synchronizują nasze kontakty – dzięki temu wiedzą, z kim się przyjaźnimy.

Nie wiadomo co piszesz
(ale wiadomo kiedy i z kim)

Szyfrowanie zabezpiecza tylko treść wiadomości – ale nie jej metadane.
Na podstawie informacji dodatkowych (na przykład z kim i kiedy piszemy) można wyciągnąć wiele interesujących wniosków.

https://security.szurek.pl

postMessage

Zabezpiecz **wymienianie danych** pomiędzy różnymi domenami przy użyciu **JavaScript**.

PODCAST

BadWPAD

Atak BadWPAD, dzięki któremu można podsłuchiwać i modyfikować niezaszyfrowany ruch internetowy na twoim komputerze.

16-03-2020 8 MINUT

PODCAST

Skutki XSS

Jak wytłumaczyć błąd typu XSS prezesowi firmy? Może pokazując jego skutki dla organizacji? Opowiedz o XSS worm – czyli kawałku kodu, który zaraża innych użytkowników, podobnie jak grypa w świecie rzeczywistym.

09-03-2020 9 MINUT

ODODOPENTESTERA

Problematyczne znaki UTF - Unicode Case Mapping Collisions

Zamiana liter z dużych na małe to prosta operacja, no chyba, że korzystasz z UTF 8. Czy może być niebezpieczna? Czy słyszałeś o Unicode Case Mapping Collisions?

24-02-2020 4 MINUT

PODCAST

XS-leaks - Cross Site Leaks

Błędy tego rodzaju w specyficznych okolicznościach pozwalają na odpowiedź tak/nie na zadane wcześniej pytanie. Na pozór wydaje się zatem, że to nic nie znacząca klasa podatności. Ale czy aby na pewno?

17-02-2020 9 MINUT