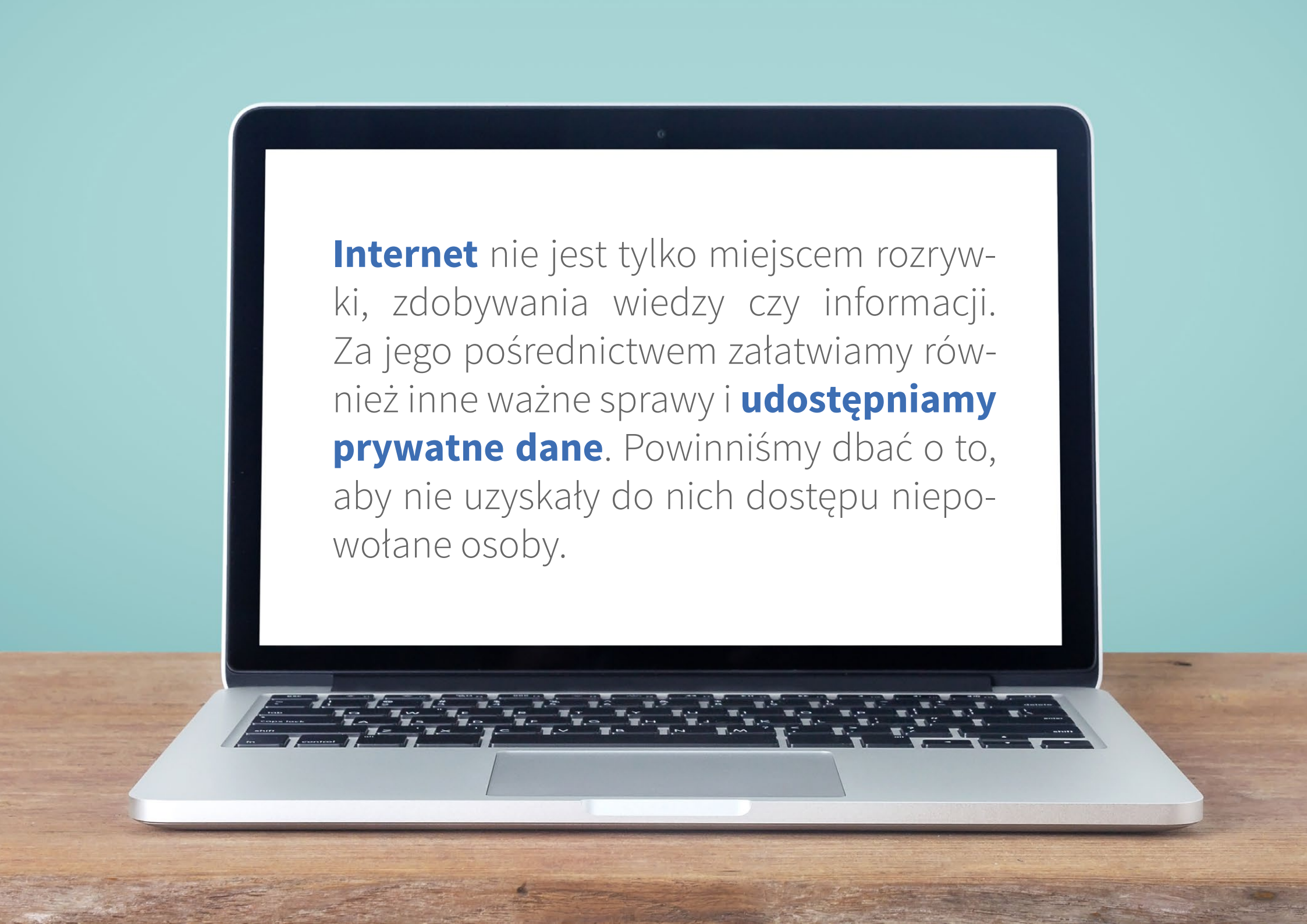
BEZPIECZEŃSTWO W **INTERNECIE**

Biblioteka W SZKOLE

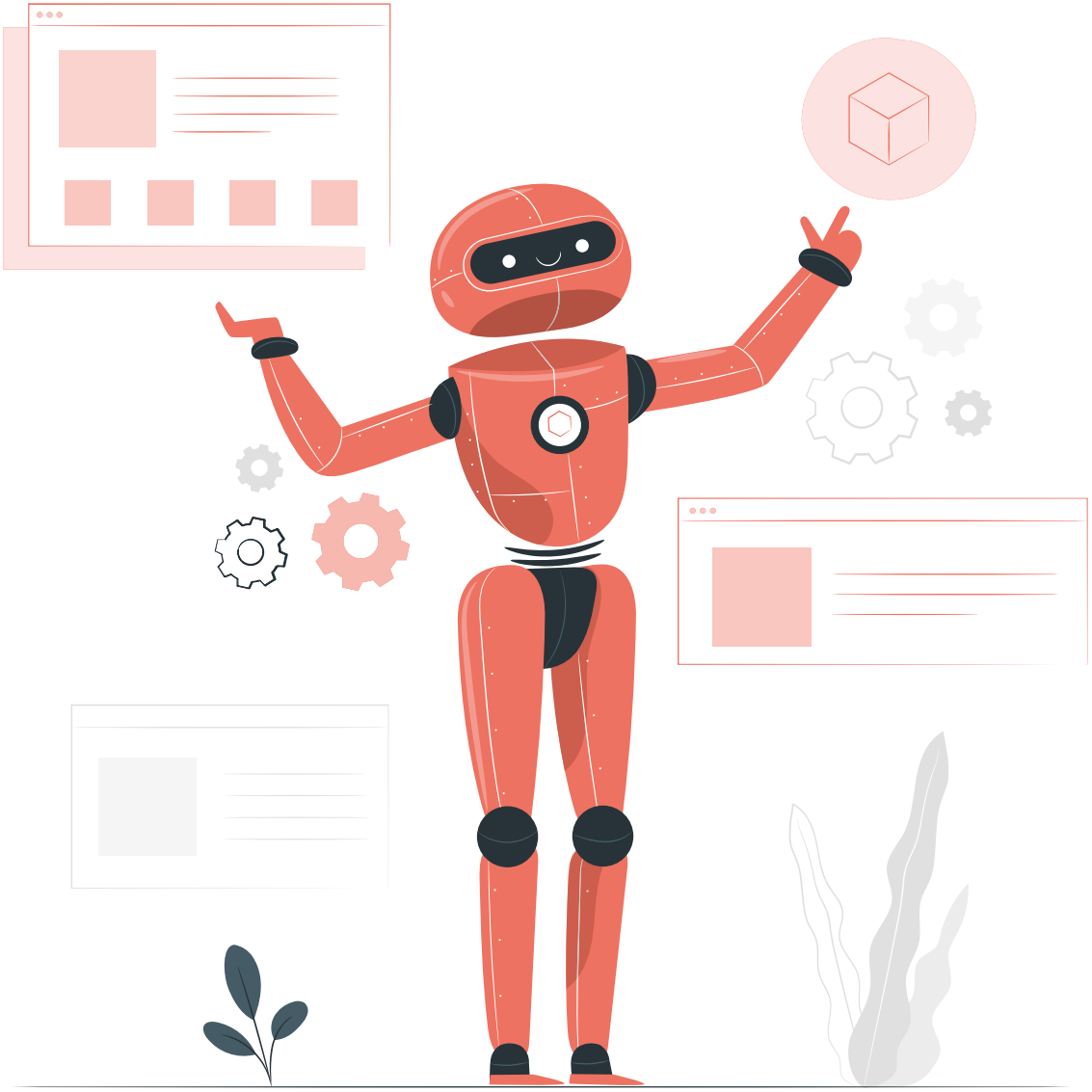
Biblioteka.pl


Internet nie jest tylko miejscem rozrywki, zdobywania wiedzy czy informacji. Za jego pośrednictwem załatwiamy również inne ważne sprawy i **udostępniamy prywatne dane**. Powinniśmy dbać o to, aby nie uzyskały do nich dostępu niepowołane osoby.

Słownik pojęć z zakresu **bezpieczeństwa w sieci**

Haker/cracker

Osoby dokonujące komputerowych włamań nazywane są hakerami. Jednak według społeczności hakerskiej haker to pasjonat o dużej wiedzy, który nie wykorzystuje jej do szkodzenia innym. Osobę łamiącą zabezpieczenia w celu dokonania przestępstwa powinno się nazywać crackerem.



Bot

Program wykonujący czynności w zastępstwie człowieka. Korzystają z niego wyszukiwarki do indeksowania stron. Może jednak służyć do przejmowania kontroli nad komputerami, przeprowadzania ataków czy też kradzieży danych.

Spam

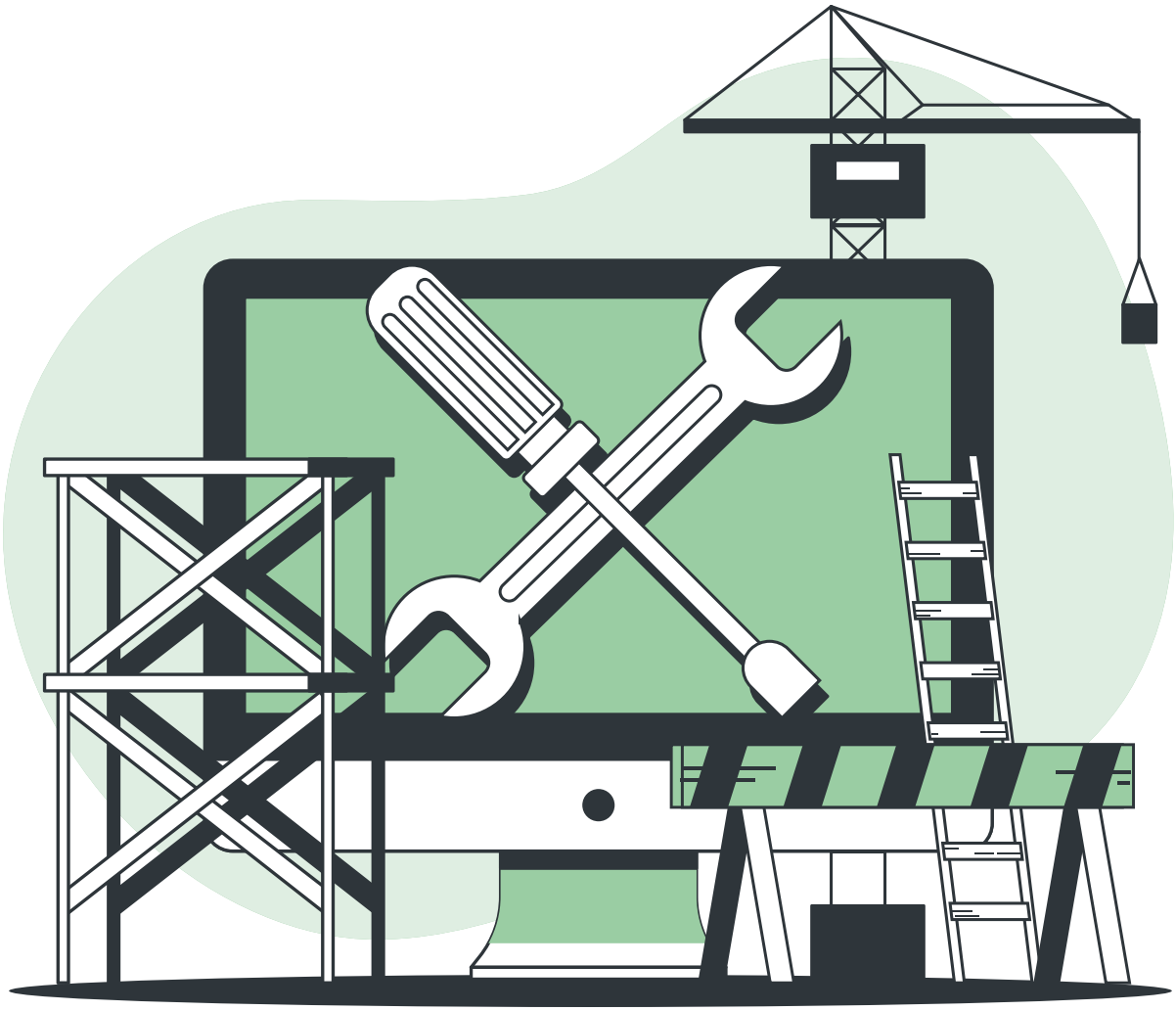
Niechciane wiadomości, na których otrzymanie odbiorca nie wyraził uprzedniej zgody. Kliknięcie na link w takiej wiadomości może uruchomić procedurę instalacji szkodliwego oprogramowania.

Firewall

Zapora sieciowa – jeden ze sposobów zabezpieczania sieci i systemów przed intruzami. Powstrzymuje hakerów przed włamywaniem się do komputera z zewnątrz.

Phishing

Metoda oszustwa, w której przestępca podszywa się pod inną osobę lub instytucję w celu wyłudzenia określonych informacji (np. danych logowania, szczegółów karty kredytowej) lub nakłonienia ofiary do określonych działań.



Ransomware

Złośliwe oprogramowanie, które po zainfekowaniu systemu szyfruje na nim pliki i foldery, uniemożliwiając dalsze z nich korzystanie. Następnie użytkownik otrzymuje żądanie okupu, którego opłacenie nie daje jednak żadnej gwarancji, że komputer zostanie odszyfrowany.

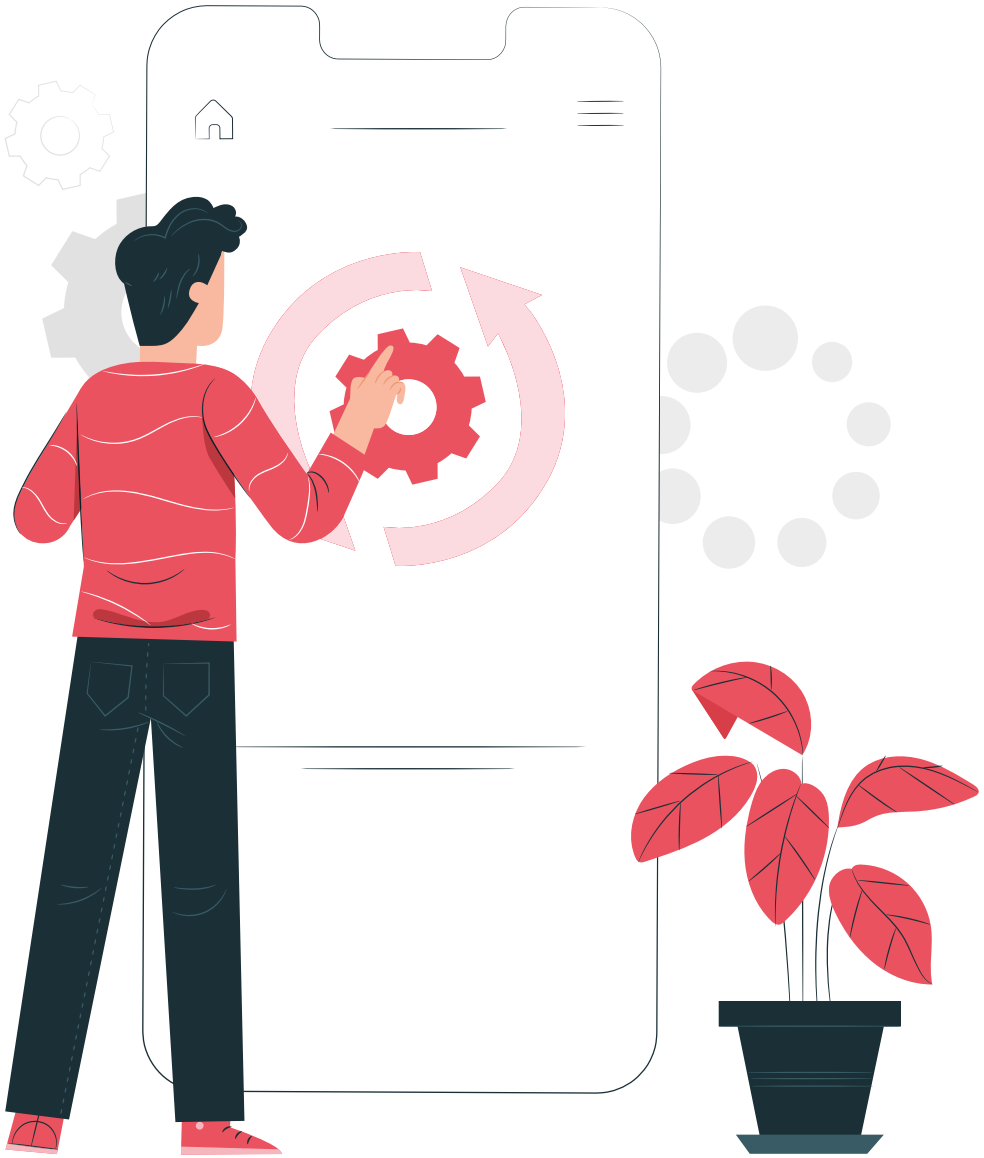
Malware

Każde złośliwe oprogramowanie, które stara się zainfekować komputer, telefon lub tablet. Wykorzystywane jest m.in. do rozprzestrzeniania wirusów, przejęcia kontroli nad maszyną i kradzieży poufnych danych.

Jak bezpiecznie korzystać **z internetu**?

Aktualne oprogramowanie

Każdy system operacyjny i oprogramowanie posiada błędy bezpieczeństwa. Są one odnajdowane i łatane na bieżąco, ale to użytkownik musi zainstalować aktualizację lub wyrazić zgodę na aktualizacje automatyczne. Jest to jedna z najskuteczniejszych metod na zabezpieczenie urządzenia, za pomocą którego łączymy się z siecią, przed niepowołanym dostępem.

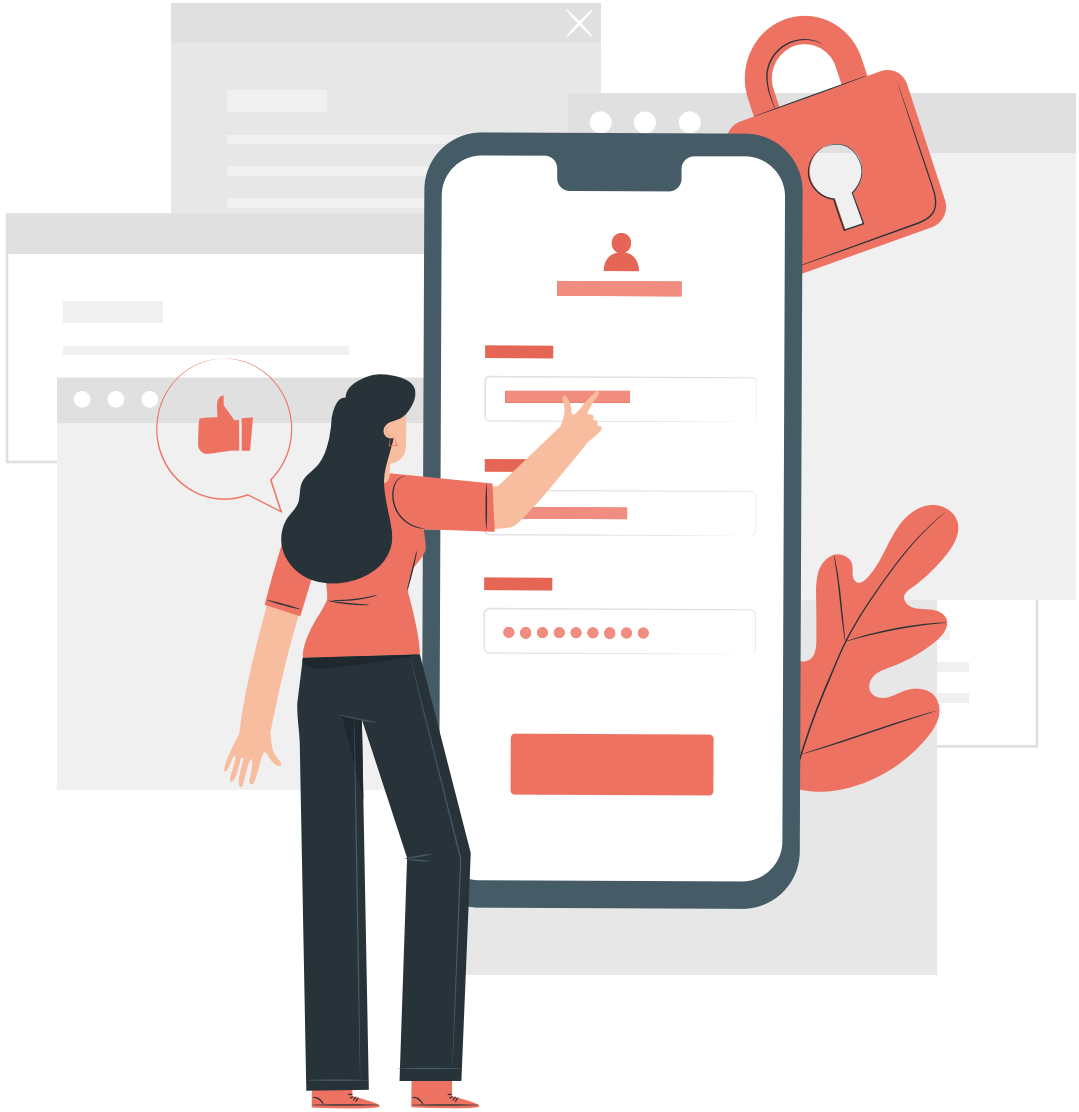


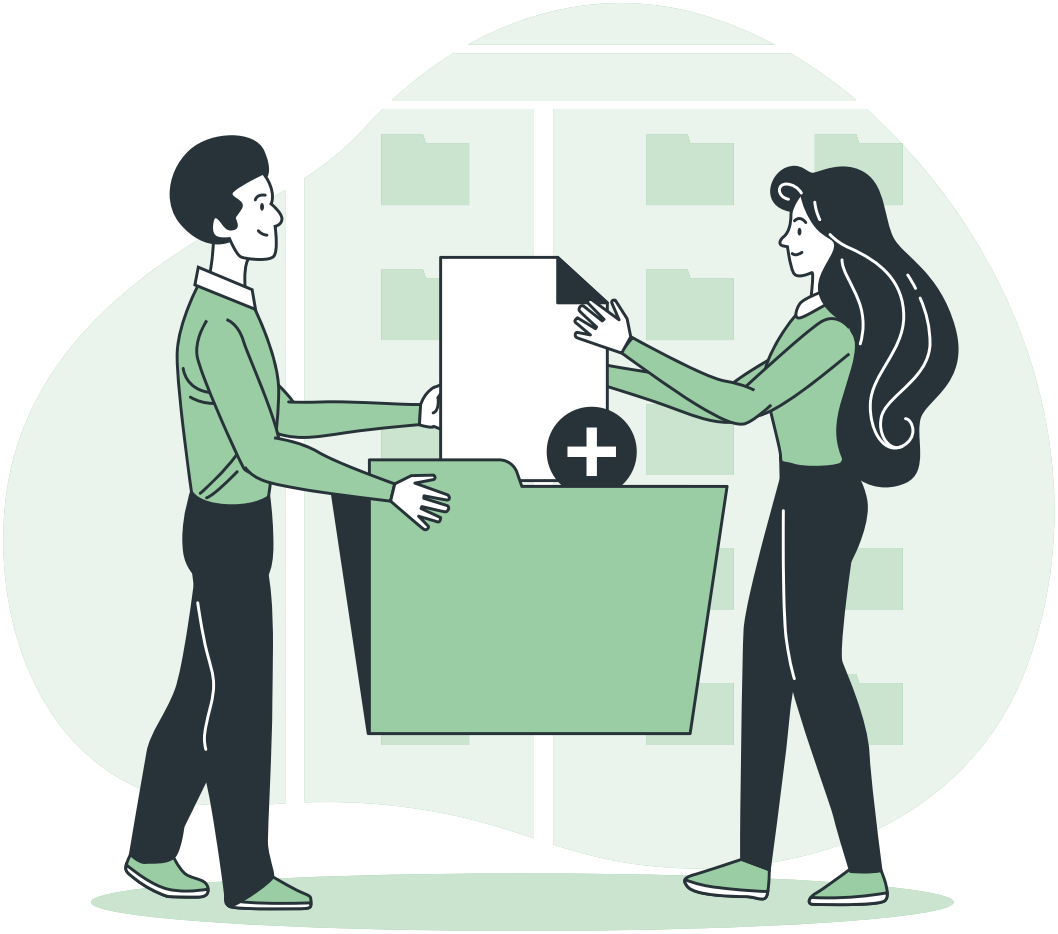
Firewall i antywirus

Hakerzy bezustannie skanują ruch w sieci w poszukiwaniu maszyn podatnych na włamanie. Oprogramowanie typu firewall pozwala ustawić blokadę wszystkich połączeń przychodzących do twojego komputera. Antywirus nie daje stuprocentowej gwarancji bezpieczeństwa, ale skutecznie odsiewa stare i masowe zagrożenia.

Silne i unikatowe hasła

Aby utrudnić złamanie hasła, powinno ono być: niesłownikowe, nieszablonowe i skomplikowane – każdy dodatkowy znak zwiększa trudność złamania hasła. Kiedy to możliwe, korzystaj z dwuetapowej weryfikacji – aby się zalogować nie wystarczy podanie hasła, trzeba jeszcze wpisać kod przesłany na telefon lub maila.





Ostrożnie z załącznikami

Wygrałeś w konkursie, w którym nie brałeś udziału? Otrzymałeś spadek od krewnego z Afryki? Jeżeli otrzymujesz wiadomość o podobnej treści, powinna zapalić ci się lampka ostrzegawcza. Gdy dostaniesz niespodziewaną wiadomość z załącznikiem lub podejrzanym linkiem, powstrzymaj ciekawość i nie otwieraj go.

Tryb prywatny (incognito)

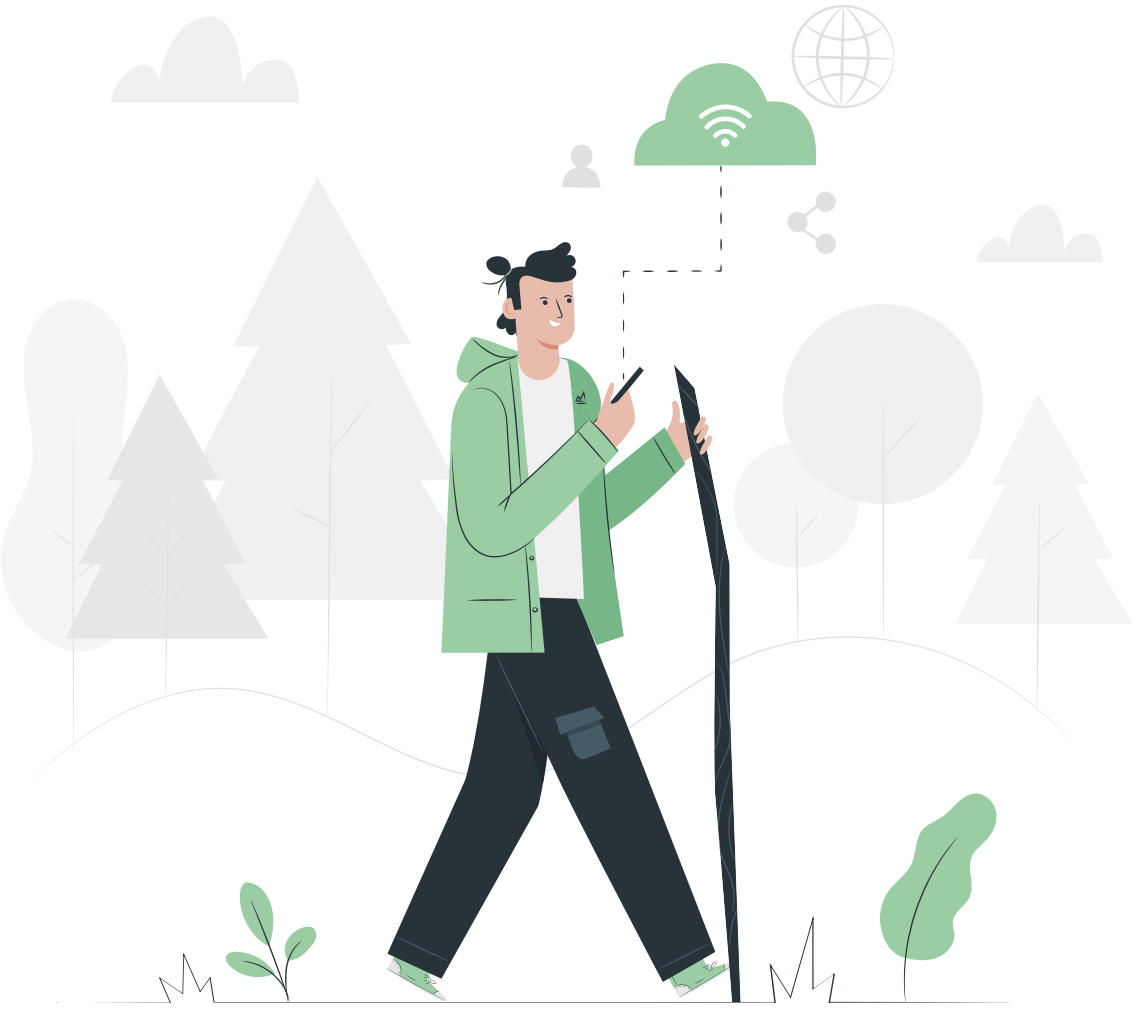
Jeżeli korzystasz z internetu na czyimś komputerze, włącz tryb prywatny, w który wyposażona jest każda nowoczesna przeglądarka. Po aktywowaniu tej funkcji użytkownik ma pewność, że wszystkie dane wytworzone od tego momentu zostaną usunięte natychmiast po przejściu w normalny tryb lub zamknięciu przeglądarki.

W internecie nic nie ginie

Wszystko, co umieszczasz w sieci lub udostępniasz nawet jednej zaufanej osobie, traktuj jako publicznie dostępne. Konto twojego odbiorcy może zostać upublicznione na skutek ataku. Prywatna galeria zdjęć na portalu społecznościowym może nagle stać się dostępna dla każdego internauty na skutek błędu w serwisie.

Nie łącz się z Wi-Fi z nieznanego źródła

Napotykasz otwartą sieć wi-fi, nie znasz jej źródła, a mimo wszystko się z nią łączysz? Hakerzy mogą rozmieszczać hotspoty w publicznych miejscach, aby przechwytywać dane. Zdarza się, że tworzą fałszywe sieci, które udają zaufane. Sieć o nazwie „Warszawa Zachodnia” nie musi być prawdziwą siecią w okolicy dworca.



Szanuj swoje dane osobowe

Gdy zakładasz maila lub rejestrujesz inne konto, nie podawaj adresu zamieszkania. Żadna internetowa usługa nie ma prawa wymagać od ciebie podania danych, które nie są niezbędne do jej działania. Adres zamieszkania nie jest tylko informacją na twój temat. Ustal z rodzicami, którymi danymi możesz dysponować, a które chcą chronić.

”

Ludzie dzielą się
na tych, którzy robią
backupy lub dopiero
będą to robić.

Rób częste kopie bezpieczeństwa

Można paść ofiarą przestępców komputerowych, nawet jeśli jest się ostrożnym. W ostatnim czasie popularnym atakiem jest szyfrowanie dysku przez hakerów, którzy w zamian za odszyfrowanie żądają wysokiego okupu. Nawet jego zapłacenie nie gwarantuje odzyskania plików. Najlepiej mieć aktualną kopię istotnych danych.

Mity na temat **bezpieczeństwa w sieci**

Korzystam ze smartfona, nic mi nie grozi

Smartfony i tablety to idealne środowisko do przeprowadzenia ataku typu phishing. W przeciwieństwie do komputera nie możesz najechać myszką na link, aby podejrzeć jego adres, więc nigdy nie wiesz, do jakiej strony zostaniesz przeniesiony, gdy klikasz w odnośnik.

Używam Maca/iPhona, nie ma na nim wirusów

Obecnie najwięcej złośliwego oprogramowania jest skierowane przeciwko użytkownikom Windowsa czy Androida, ale nie oznacza to, że korzystający z innych systemów operacyjnych (np. Apple albo Linux) mogą czuć się bezpieczni. Każde urządzenie mające połączenie z internetem może być podatne na atak.

Nie jestem nikim ważnym, nikt mnie nie zaatakuje

Nie musisz być prezesem banku czy sławną piosenkarką. W sieci jest mnóstwo wandali, którym wystarczy sama satysfakcja z wyrządzonych strat. Hakerzy rzadko wybierają indywidualne cele, zwykle działają na dużą skalę za pomocą zautomatyzowanych narzędzi skanując internet w poszukiwaniu podatnych urządzeń.

Znajomy udostępnił link, więc jest bezpieczny

Wśród złośliwych aplikacji możemy spotkać i takie, które do swojej dystrybucji wykorzystują portale społecznościowe. Po infekcji na naszym koncie automatycznie rozsyłają się linki w formie wiadomości lub komentarzy.

Ikona kłódki oznacza, że strona jest bezpieczna

Sama ikona kłódki nie jest wyznacznikiem bezpieczeństwa witryny. Przed wprowadzeniem swoich danych należy się upewnić, czy adres strony jest prawidłowy.

Bezpiecznego korzystania z internetu

życzy

Biblioteka
W SZKOLE

Biblioteka.pl

Ilustracje użyte w prezentacji pochodzą
z mixkit.com oraz stories.freepik.com