12.10
Dzień Bezpiecznego Komputera

Dzień Bezpiecznego Komputera

Dzień Bezpiecznego Komputera obchodzony jest corocznie 12 października (od 2004 roku). Jego celem jest propagowanie wiedzy na temat bezpieczeństwa w sieci. Inicjatywa została objęta honorowym patronatem Prezydenta Rzeczypospolitej Polskiej.

Od 2004 roku wiele się zmieniło! Coraz częściej w domach posiadamy „inteligentne” żarówki, zamki, oczyszczacze powietrza i inne nowinki technologiczne. Dlatego warto wiedzieć, jak dbać o bezpieczeństwo swoich danych.

Niebezpieczeństwa w sieci!

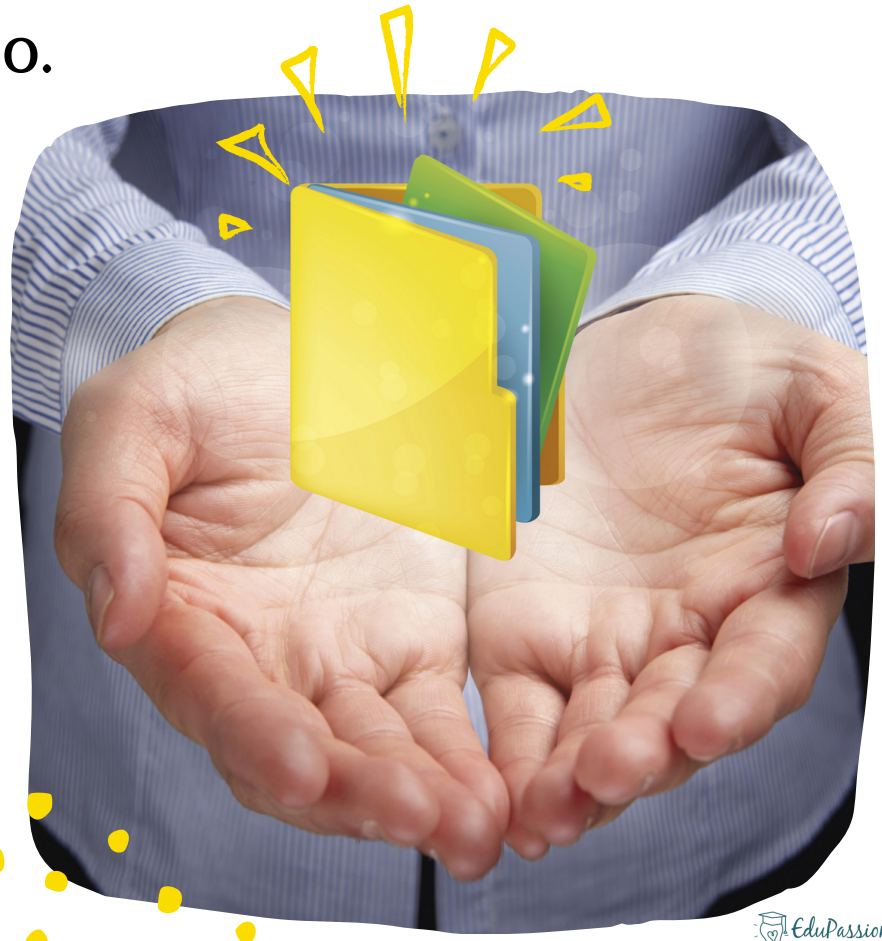
Głównymi zagrożeniami w sieci są:

- wycieki danych,
- ataki hakerskie,
- oprogramowanie złośliwe (malware):
  - wirusy komputerowe,
  - wormsy (robaki komputerowe),
  - ransomware,
  - adware,
  - wiper,
  - Koń Trojański / Trojan.

Wyciek danych

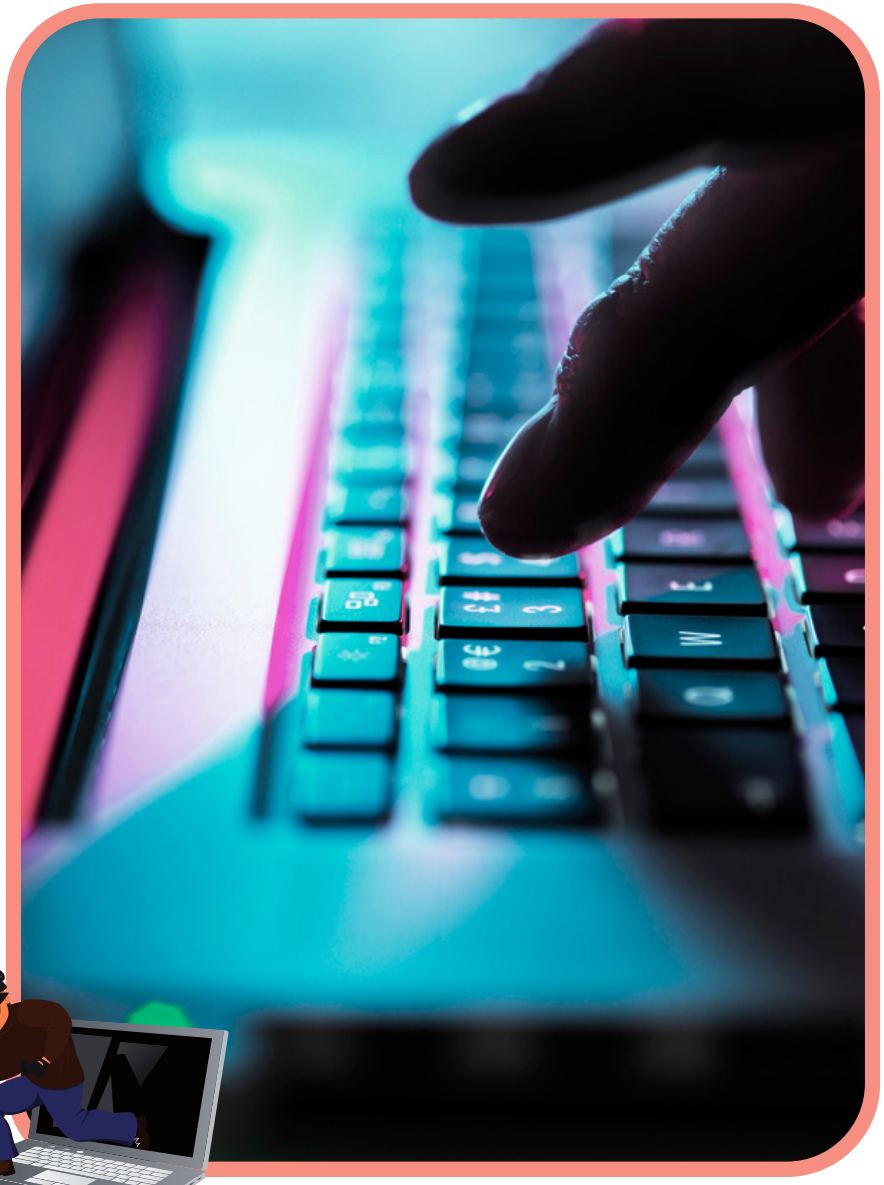
Wyciek danych następuje, kiedy strona internetowa przez pomyłkę udostępni wrażliwe dane lub padnie ofiarą ataku hakerskiego.

Najczęściej dochodzi do wycieków haseł, dlatego ważne jest posiadanie unikalnego hasła do każdej strony internetowej, na której mamy konto!



Ataki hakerskie

Atakiem hakerskim nazywamy celowe złamanie zabezpieczeń wybranej firmy lub użytkownika. Atak ten może mieć różne cele: pozyskanie danych, uszkodzenie sprzętu albo wgranie wirusa.



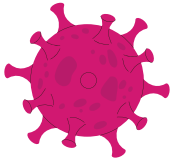
Przeciętny użytkownik nie musi obawiać się ataku hakerskiego. Najczęściej ofiarami ataku hakerskiego są duże firmy.

Malware

Malware [czytaj: malwer] to inaczej oprogramowanie złośliwe. Każdy program celowo stworzony do uszkadzania sprzętu, działania bez wiedzy użytkownika bądź nielegalnych operacji jest nazywany malware.

Malware ma wiele odmian:

WIRUSY



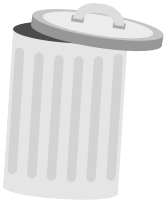
WORMSY (ROBAKI KOMPUTEROWE)

KONIE TROJAŃSKIE (TROJANY)

RANSOMWARE

ADWARE

WIPER



Wirusy

Wirus to program, który został wgrany bez wiedzy użytkownika i może mieć kilka celów:

- uszkodzenie sprzętu,
- wymuszanie otwierania stron,
- powielanie się (tworzenie kopii wirusa),
- używanie sprzętu do nielegalnych działań.

Najsłynniejszy wirus, MyDoom, spowodował straty na wysokość 38.5 miliarda dolarów!

Wormsy

Robaki komputerowe to mniej groźna odmiana wirusa - ich jedynym zadaniem jest tworzenie kopii na jak największej liczbie urządzeń. Nie oznacza to, że nie są szkodliwe! Działający w tle worm, mimo bycia niewidocznym dla użytkownika, spowalnia sprzęt.

Najsławniejszym wormsem jest Morris. Stworzony w latach osiemdziesiątych 20. wieku zainfekował wtedy ponad 10% całego internetu!

Ransomware

Ransomware to malware, który blokuje dostęp do plików na komputerze do momentu zapłaty twórcy tego złośliwego oprogramowania.

W 2020 roku ransomware spowodowało stratę na ponad 29.1 milionów dolarów!

Adware

Adware jest jednym z najmniej szkodliwych dla sprzętu malware - jego zadaniem jest wyświetlanie reklam, najczęściej przy otwieraniu przeglądarki lub po włączeniu komputera.

Adware jest jedynym złośliwym oprogramowaniem, które nie łamie prawa, ale jest wciąż nieetyczny.

Wiper

Warto zabezpieczyć swoje dane także na innym nośniku lub dysku sieciowym.

Wiper jest oprogramowaniem usuwającym wszystkie dane z komputera. Nie posiada on żadnego wyższego celu - powstał wyłącznie po to, żeby tworzyć jak największe szkody na urządzeniach użytkownika.

Trojany

Trojany swoją nazwę zawdzięczają koniowi trojańskiemu. Jest to oprogramowanie, które udając bezpieczny program, dostaje się do komputera. Trojany zawierają często inne malware (np. wirusy i adware).

Trojany podszywają się często pod popularne programy i najczęściej infekują komputery przy próbie zainstalowania nielegalnego oprogramowania.

Jak dbać o bezpieczeństwo w sieci?

Niestety żadne zabezpieczenia komputera nie są w stanie w 100% zabezpieczyć nas, jeżeli korzystamy z sieci w sposób niewłaściwy. Tak więc najlepszą ochroną naszego urządzenia jesteśmy my sami.

Stosując się do kilku zasad, będziesz w stanie ochronić swój komputer!

Nie wyłączaj zapory systemowej!

i Zapora i antywirus to programy mające na celu chronić Cię przed atakami i złośliwym oprogramowaniem.

Zawsze aktualizuj bazę danych zapory i antywirusa!

Nie pobieraj nielegalnego oprogramowania!

Zamiast pobierać nielegalną kopię oprogramowania, pobierz darmowy odpowiednik!

Korzystaj z darmowych odpowiedników!

Nie otwieraj linków z wiadomości od nieznanych osób!

Nie ufaj bezgranicznie adresom e-mailowym - zawsze dokładnie przyjrzyj się od kogo przyszła wiadomość.

Zawsze weryfikuj adres nadawcy!

Nie używaj jednego hasła!

i

Jeżeli masz możliwość, skorzystaj z dwuetapowej weryfikacji danych (np. hasło i e-mail, hasło i telefon), w celu zwiększenia bezpieczeństwa w sieci.

Posiadaj choćby kilka różnych haseł!

Nie wpisuj kluczowych danych bez weryfikacji!

i

Kluczowe dane to twoje imię, nazwisko, adres zamieszkania, PESEL, dane bankowe. Pamiętaj, że bank nigdy nie prosi o takie dane!

Zawsze weryfikuj adres strony i potrzebę podania danych!

Nie przechowuj swoich danych w jednym miejscu!

i Kopie zapasowe swoich dokumentów możesz tworzyć na zewnętrznych dyskach (USB) lub w chmurze.

Regularnie twórz kopie zapasowe!

Nie pobieraj plików z linków bez ich weryfikacji!

i Uważaj na częste próby wyłudzenia danych - jeżeli nic nie zamawiałeś, nie powinieneś klikać linków od pseudokuriera!

Zawsze sprawdzaj adres linku, nie otwieraj nieznanych plików!


Zadbaj
o bezpieczeństwo!
EduPassion
UCZ SIĘ Z PASJĄ