

# 1, 2, 3 bezpieczny jesteś Ty!

## Dane osobowe

### Przyczyny zagrożeń

Falshywe maile.



Zapisywanie danych w tylko jednym miejscu.

Stosowanie łatwych haseł do wielu kont.



Brak programów chroniących komputer przed niebezpieczestwami.

Fizyczna kradzież sprzętów elektronicznych.

Udostępnianie danych wrażliwych w sieci (szczególnie na portalach społecznościowych).

Korzystanie z niezabezpieczonych sieci publicznych (np. hotspotów).

Korzystanie z niezawierających stron internetowych.

Korzystanie z niezawierających stron internetowych.

Korzystanie z niezawierających stron internetowych.

Korzystanie z niezawierających stron internetowych.

### Skutki zagrożeń

1 na 500 maili wysyłanych na skrzynki pocztowe na całym świecie został wysłany w celu wyłudzenia danych osobowych!

Utrata danych z komputera.

W ciągu minuty - 20 nowych ofiar kradzieży tożsamości w sieci.

W ciągu minuty - 232 komputery zostają zainfekowane wirusami, robakami, trojanami.

Instalacja keyloggerów na komputerze.

Manipulacja - uzyskiwanie dostępu do danych i integrowanie w ich treść przez osoby nieupoważnione.

Włamania do komputera poprzez internet.

Włamania do komputera poprzez internet.

Włamania do komputera poprzez internet.

Włamania do komputera poprzez internet.

Włamania do komputera poprzez internet.

Włamania do komputera poprzez internet.

### Sposoby zapobiegania zagrożeniom

Nie otwieraj podejrzanych maili.



Aby bezpiecznie przechowywać dane twórzmy kopie zapasowe lub zapisujemy je w chmurach.

Twórz długie, skomplikowane hasła. Używaj dużych i małych liter, a także cyfr i znaków. Nie stosuj tego samego hasła do wielu kont. Pamiętaj by często zmieniać hasła.

Instaluj i aktualizuj antywirusy, firewalles, antyspyware.

Warto szyfrować cały dysk twardy: HASŁO + DWUSKŁADNIOWE UWIETRZYNIANIE

Podawaj tylko najistotniejsze informacje. Nie udostępniaj swoich danych wrażliwych

Ostrożnie korzystaj z hotspotów. Staraj się korzystać jedynie z zabezpieczonych sieci publicznych.

Ostrożnie korzystaj z hotspotów. Staraj się korzystać jedynie z zabezpieczonych sieci publicznych.

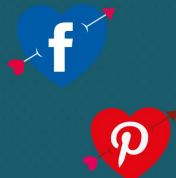
Ostrożnie korzystaj z hotspotów. Staraj się korzystać jedynie z zabezpieczonych sieci publicznych.

Ostrożnie korzystaj z hotspotów. Staraj się korzystać jedynie z zabezpieczonych sieci publicznych.

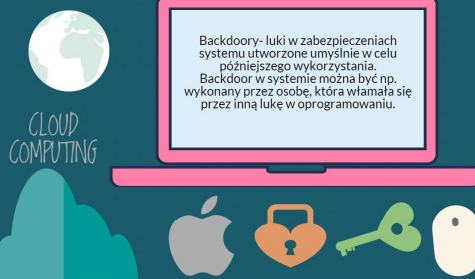
Ostrożnie korzystaj z hotspotów. Staraj się korzystać jedynie z zabezpieczonych sieci publicznych.

Co to jest keylogger?

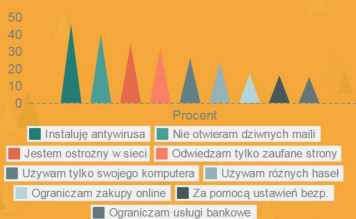
Keyloggery to sprzętowe lub programowe moduły, które zainstalowane na komputerze użytkownika (ofiary), potrafią odczytać i przechowywać w pamięci historię wciśniętych przez niego klawiszy.



Dwuskładniowe uwietrzywanie. Aby uzyskać dostęp np. do telefonu komórkowego musimy potwierdzić swoją tożsamość poprzez np. skanowanie linii papilarnych lub podanie ustalonych danych wrażliwych.



CLOUD COMPUTING



Jak poprawiasz swoje bezpieczeństwo?

Analiza na podstawie Eurobarometr 2013