KEVIN SAM W BANKU SGB

- **ZAGROŻENIA ZWIĄZANE Z BANKOWOŚCIĄ INTERNETOWĄ**

PROJEKT DOTYCZĄCY PODNIESIENIA POZIOMU BEZPIECZEŃSTWA PRZY KORZYSTANIU Z NOWOCZESNYCH USŁUG BANKOWYCH

INFORMACJE O SAMYM PROJEKCIE

„KEVIN SAM W BANKU SGB”

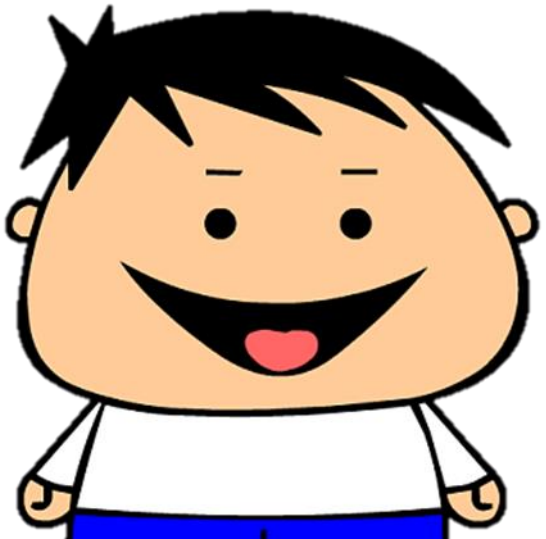
Znacie już naszego bohatera
z poprzednich lekcji.
Dziś postaramy się omówić jak
bezpiecznie korzystać z bankowości
internetowej oraz z Internetu.

CZEGO DOWIEMY SIĘ NA DZISIEJSZEJ LEKCJI

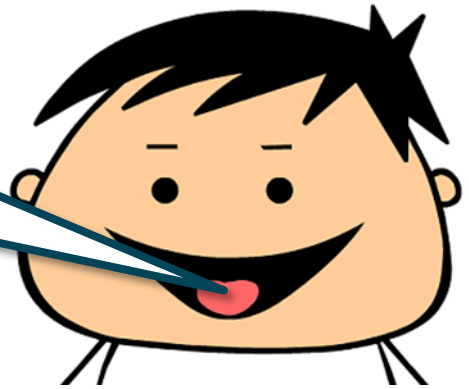
ZAGROŻENIA ZWIĄZANE Z BANKOWOŚCIĄ INTERNETOWĄ

Po dzisiejszej lekcji będziemy wiedzieć:

1. *Czym jest bankowość internetowa?*
2. *Jakie są zasady bezpiecznego korzystania z bankowości internetowej?*
3. *Co to jest bezpieczna strona?*
4. *Jakie są zasady dotyczące haseł?*
5. *Jak korzystać z sieci publicznych?*
6. *Po co nam ochrona antywirusowa?*
7. *Jakie są zagrożenia związane z bankowością internetową?*
8. *Jak postępować w przypadku zaistnienia zagrożenia?*



CZĘŚĆ I



BANKOWOŚĆ INTERNETOWA

BANKOWOŚĆ INTERNETOWA

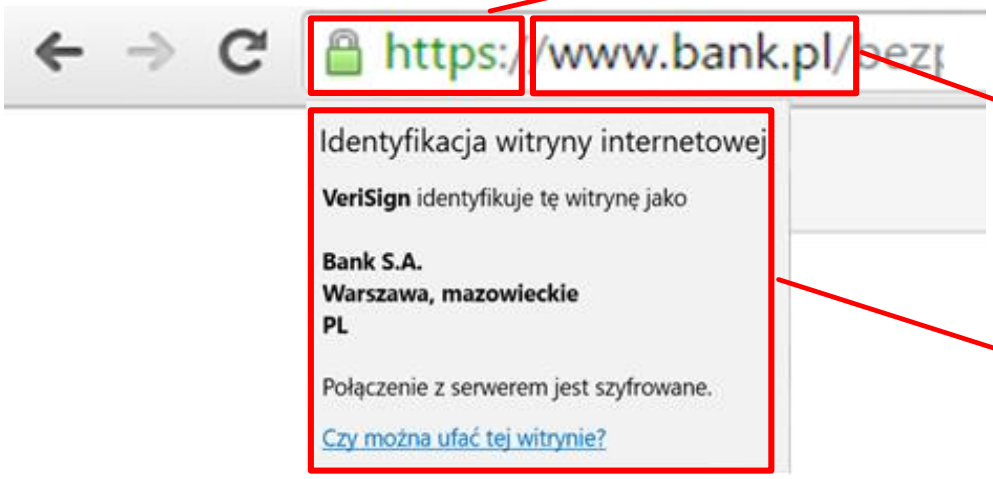
DOSTĘP DO NASZEGO RACHUNKU BANKOWEGO POPRZEZ INTERNET

NIE MUSIMY WYCHODZIĆ Z DOMU, ABY OPŁACIĆ RACHUNKI, ZAŁOŻYĆ RACHUNEK BANKOWY CZY ZWYCZAJNIE SPRAWDZIĆ STAN NASZYCH OSZCZĘDNOŚCI.

MOŻEMY TO ZROBIĆ O KAŻDEJ PORZE I Z KAŻDEGO MIEJSCA NA ŚWIECIE, W KTÓRYM DYSPONUJEMY DOSTĘPEM DO INTERNETU.

LOGOWANIE DO BANKOWOŚCI INTERNETOWEJ

BEZPIECZNA STRONA



POŁĄCZENIE SZYFROWANE
ZNAK „KŁÓDECZKI”
I HTTP**S**://

PRAWIDŁOWY ADRES STRONY

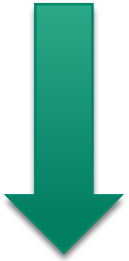
ZAUFANY WYSTAWCA CERTYFIKATU

LOGOWANIE DO BANKOWOŚCI INTERNETOWEJ

IDENTYFIKATOR KLIENTA

NADAJE BANK

AUTORYZACJA



****

HASŁO NADAJE UŻYTKOWNIK

HASŁO DOSTĘPU DO BANKOWOŚCI INTERNETOWEJ

JAKIE POWINNO BYĆ HASŁO

MINIMUM **8** ZNAKÓW

MAŁE DUŻE LITERY

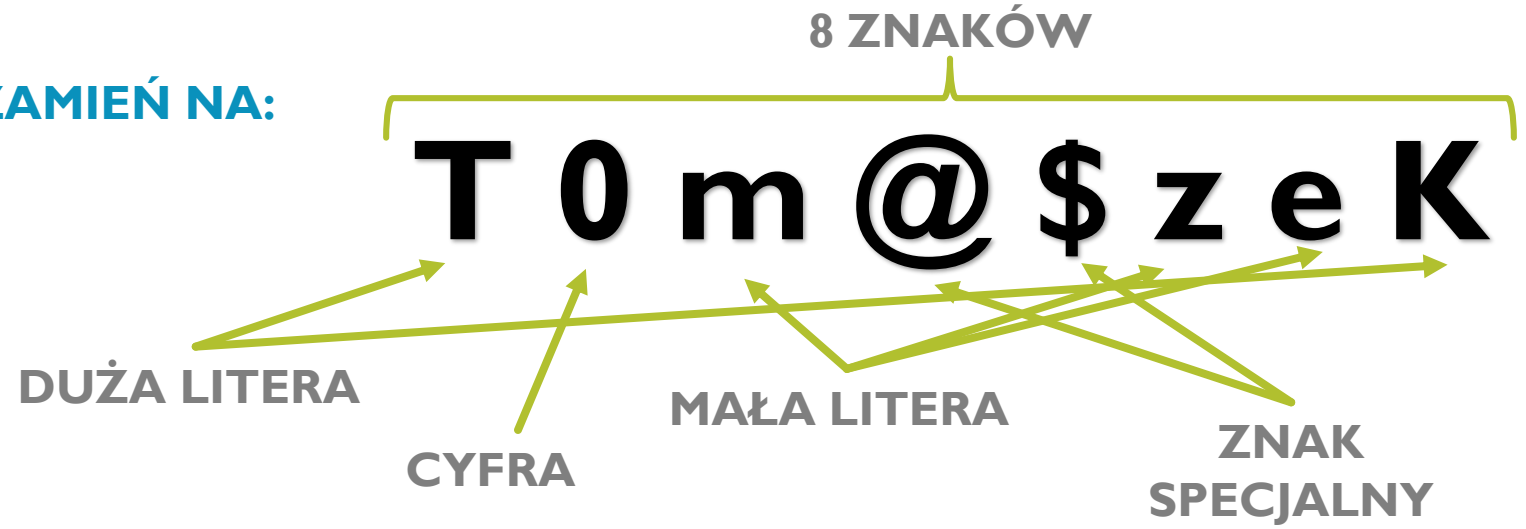
ZNAKI SPECJALNE (**!#$***) LUB CYFRY (**257**)

HASŁO DOSTĘPU DO BANKOWOŚCI INTERNETOWEJ

JAK ZAPAMIĘTAĆ TRUDNE HASŁO

NP. PROSTE HASŁO: t o m a s z

ZAMIEŃ NA:

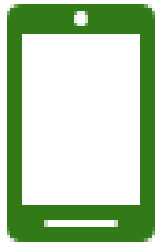


AUTORYZACJA OPERACJI

W CELU ZWIĘKSZENIA BEZPIECZEŃSTWA WYKONYWANYCH ZA POŚREDNICTWEM BANKOWOŚCI ELEKTRONICZNEJ OPERACJI, DLA WIĘKSZOŚCI Z NICH KONIECZNA JEST DODATKOWA AUTORYZACJA W FORMIE:

Lista haseł jednorazowych „zdrapka”

Token lub e-token



Kody SMS przesyłane na wskazany nr telefonu

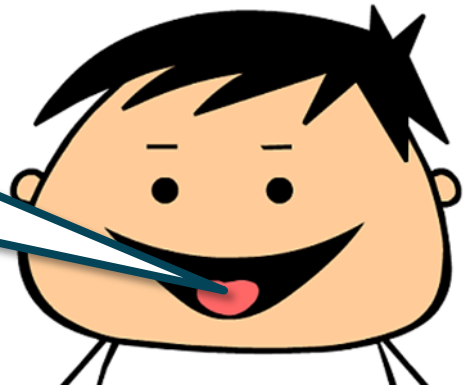
ZAGADKA

Jaka kłódeczka musi być widoczna przy adresie strony bankowości internetowej ?

ZAMKNIĘTA ?

OTWARTA ?

CZĘŚĆ II



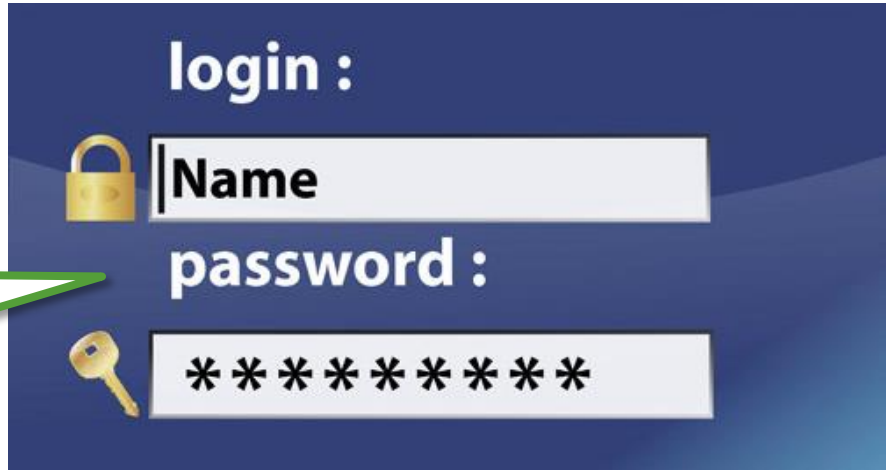
BEZPIECZEŃSTWO W SIECI

BANKOWOŚĆ INTERNETOWA

ZASADY BEZPIECZEŃSTWA W SIECI

ZASADA NR 1

NIE ZDRADZAJ NIKOMU SWOICH LOGINÓW I HASEŁ



Pod żadnym pozorem **nie udostępniaj nikomu loginu** (czyli unikatowego cyfrowego imienia, po którym jesteśmy rozpoznawani przez system internetowy banku) i **hasła dostępu** do bankowości internetowej.

BANKOWOŚĆ INTERNETOWA

ZASADY BEZPIECZEŃSTWA W SIECI

ZASADA NR 2

PAMIĘTAJ O OKRESOWEJ ZMIANIE HASEŁ

Hasło do bankowości internetowej powinno być zmieniane co najmniej raz na 3 miesiące. Tworząc nowe hasło miej na uwadze jego złożoność.

BANKOWOŚĆ INTERNETOWA

ZASADY BEZPIECZEŃSTWA W SIECI

ZASADA NR 3

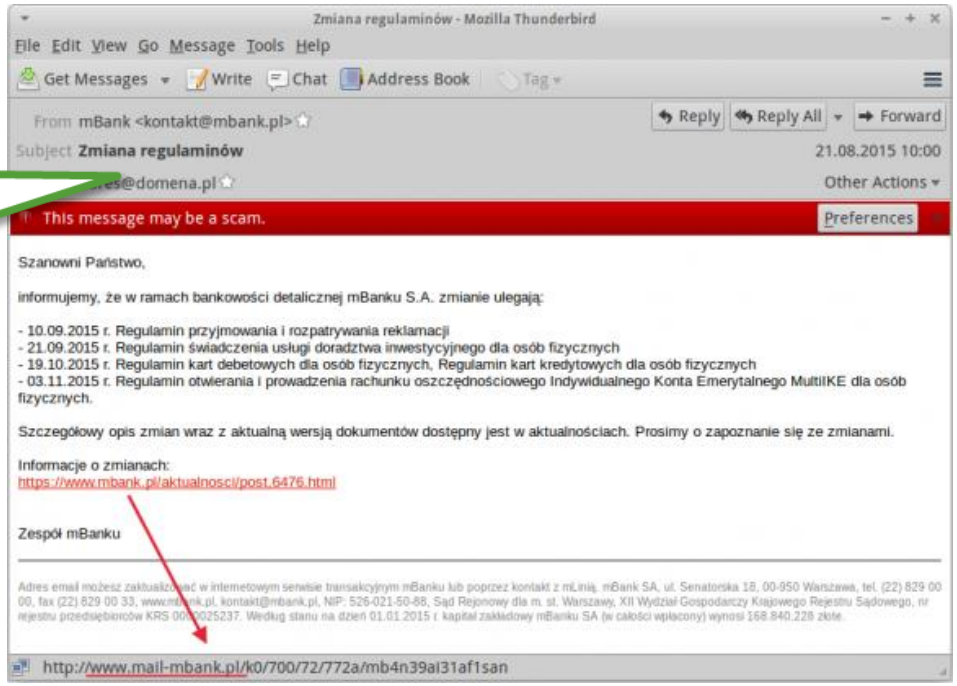
PODAWAJ HASŁA TYLKO NA SZYFROWANYCH STRONACH

Sprawdź, czy w przeglądarce pojawia się znak „**kłódeczki**”.

BANKOWOŚĆ INTERNETOWA
ZASADY BEZPIECZEŃSTWA W SIECI

ZASADA NR 4

ZASTANÓW SIĘ ZANIM KLIKNIESZ LINK Z NIEZNANEGO ŹRÓDŁA



Nie wolno nigdy korzystać z **odsyłaczy (linków)** do banku przesyłanych pocztą elektroniczną.

BANKOWOŚĆ INTERNETOWA

ZASADY BEZPIECZEŃSTWA W SIECI

ZASADA NR 5

iPKO

Twoje konto jest zablokowane

Otrzymaliśmy wiele nieudanych prób logowania ze swojego konta online.
Dla Twojego bezpieczeństwa, mamy zablokowane konta.

Aby przywrócić dostępu on-line kliknij: Zaloguj się do iPKO i kontynuować proces weryfikacji.

Prosimy nie odpowiadać bezpośrednio na tego automatycznie generowanych wiadomości e-mail.

Z powazaniem,
PKO Bank Polski

© 2015 PKO Bank Polski

NIE OTWIERAJ PODEJRZANYCH MAILI I WIADOMOŚCI W MEDIACH SPOŁECZNOŚCIOWYCH

Bank **<u>nigdy nie wymaga</u>** podawania poufnych danych w mailu.

BANKOWOŚĆ INTERNETOWA

ZASADY BEZPIECZEŃSTWA W SIECI

ZASADA NR 6

NIE SURFUJ PO INTERNECIE JEŻELI NIE POSIADASZ ODPOWIEDNIEGO PROGRAMU ANTYWIRUSOWEGO

Trzeba też brać pod uwagę **bezpieczeństwo własnego komputera** – mieć kontrolę nad tym, **kto z niego korzysta** oraz zadbać o odpowiedni **program antywirusowy.**

BANKOWOŚĆ INTERNETOWA

ZASADY BEZPIECZEŃSTWA W SIECI

ZASADA NR 7

Najlepiej logować się do banku tylko z komputerów, co do których mamy pewność, że są **bezpieczne**.
W przeciwnym wypadku istnieje ryzyko, że ktoś może **wykraść nasze dane** i próbować dostać się do naszego konta. Należy również unikać logowania się do bankowości internetowej w sieci, która jest **publiczna**.

ZAGADKA

W jakich przypadkach, w drodze wyjątku, możemy podać nasze hasło do bankowości internetowej?

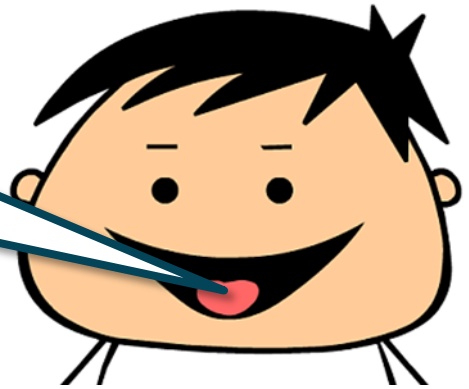
GDY DZWONI ZAUFANY PRACOWNIK NASZEGO BANKU.

GDY PROSI NAS O TO PRACOWNIK BANKU NA MIEJSCU W PLACÓWCE BANKU.

GDY BANK WYSTOSOWAŁ W OFICJALNEJ KORESPONDENCJI E-MAILOWEJ TAKĄ PROŚBĘ.

GDY ZE WZGLĘDU NA AWARIĘ SERWERA DOSTĘP DO BANKOWOŚCI INTERNETOWEJ NIE JEST SZYFROWANY.

CZĘŚĆ III

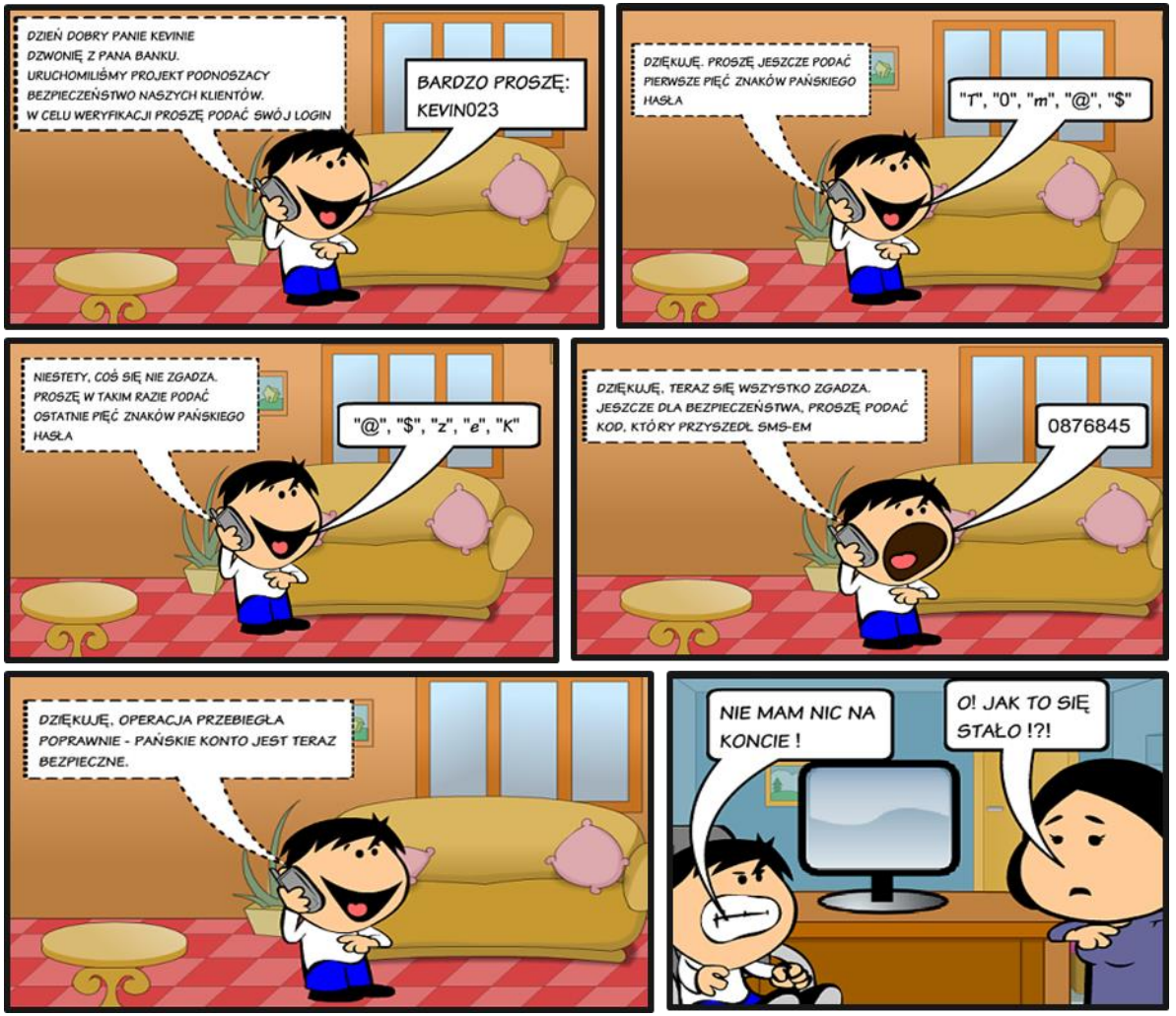


ZAGROŻENIA ZWIĄZANE Z BANKOWOŚCIĄ INTERNETOWĄ

PHISHING – CO TO JEST ?

METODA OSZUSTWA, W KTÓREJ PRZESTĘPCA **PODSZYWA SIĘ POD INNĄ OSOBĘ** LUB ORGANIZACJĘ W CELU **WYŁUDZENIA OKREŚLONYCH INFORMACJI** (NP. DANYCH DO LOGOWANIA) LUB NAKŁONIENIA OFIARY DO REALIZACJI OKREŚLONYCH DZIAŁAŃ.

PHISHING - TELEFONICZNY

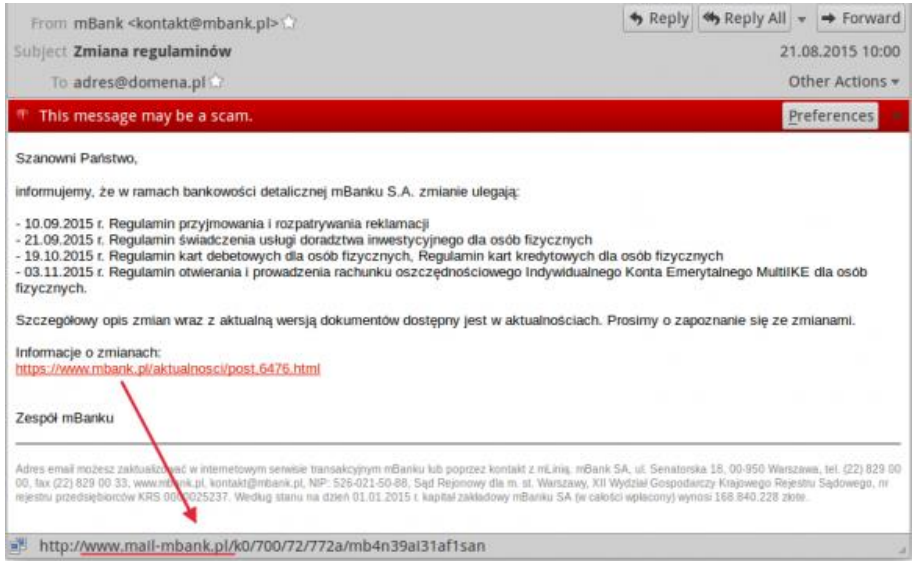


PHISHING

KEVINIE! ZAPAMIĘTAJ !
ŻADEN BANK I ŻADNA INSTYTUCJA NIGDY, POD ŻADNYM POZOREM NIE PROSI O PODANIE ŻADNYCH DANYCH DO LOGOWANIA
CZY TO TELEFONICZNIE, CZY POPRZEZ POCZTĘ ELEKTRONICZĄ CZY W JAKIKOLWIEK INNY SPOSÓB

PHISHING – E-MAILOWY

Sposobem często wykorzystywanym przez przestępców jest **przesyłanie w wiadomościach e-mail linków** rzekomo prowadzących do serwisów bankowości internetowej, a w praktyce będących stronami internetowymi na **serwerach przestępców, które zwykle do złudzenia przypominają te serwisy**.



SPYWARE – CO TO JEST ?

OPROGRAMOWANIE SZPIEGUJĄCE - PROGRAMY KOMPUTEROWE, KTÓRYCH CELEM JEST **GROMADZENIE INFORMACJI O UŻYTKOWNIKU** ORAZ **PRZESYŁANIE DANYCH** I INFORMACJI UŻYTKOWNIKA LUB O UŻYTKOWNIKU **BEZ JEGO WIEDZY** AUTOROWI PROGRAMU LUB INNEJ OSOBIE.

SPYWARE – JAK DZIAŁA?

SKĄD GO MAMY NA KOMPUTERZE:

BRAK OCHRONY ANTYWIRUSOWEJ

NIELEGALNE OPROGRAMOWANIE

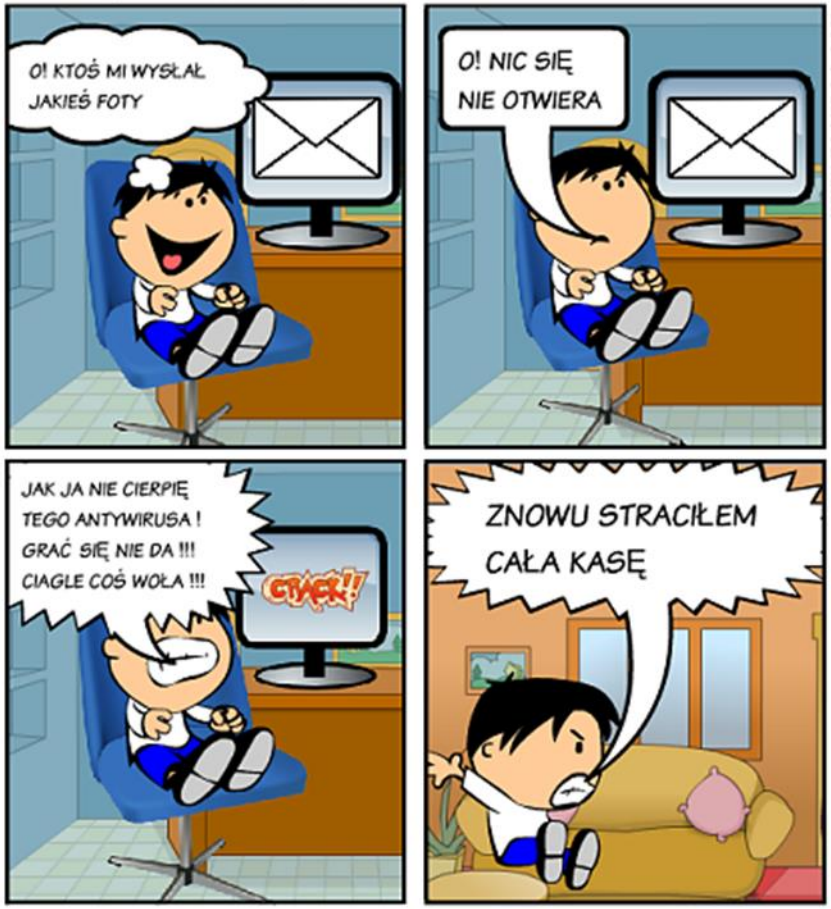
OTWIERANIE ZAŁĄCZNIKÓW E-MAIL NIEZNANEGO POCHODZENIA

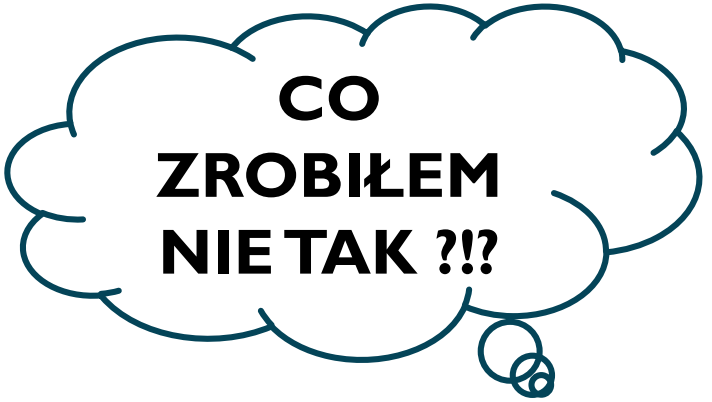
SPYWARE – JAK DZIAŁA?

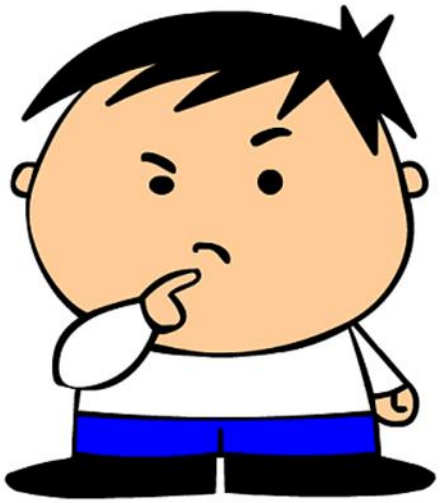
PO INSTALACJI BEZ NASZEJ WIEDZY PRZESYŁA:

- **ADRESY WWW**
- **DANE OSOBOWE**
- **NUMERY KART PŁATNICZYCH**
- **LOGINY I HASŁA**
- **ZAINTERESOWANIA UŻYTKOWNIKA**
- **ADRESY POCZTY ELEKTRONICZNEJ**

SPYWARE


O! KTOŚ MI WYSŁAŁ JAKIEŚ FOTY
O! NIC SIĘ NIE OTWIERA
JAK JA NIE CIERPIĘ TEGO ANTYWIRUSA ! GRAĆ SIĘ NIE DA !!! CIAGLE COŚ WOŁA !!!
CYK CYK!!
ZNOWU STRACIŁEM CAŁA KASĘ


CO ZROBIŁEM NIE TAK ?!?



SPYWARE

KEVINIE! MUSISZ PAMIĘTAĆ O TYM, ŻE DO KORZYSTANIA Z BANKOWOŚCI INTERNETOWEJ NALEŻY ZAWSZE UŻYWAĆ ZNANYCH SOBIE, **ZAUFANYCH URZĄDZEŃ**, KTÓRE MUSZĄ BYĆ ZABEZPIECZONE AKTUALNYM **OPROGRAMOWANIEM ANTYWIRUSOWYM**

SPYWARE

DODATKOWO ZAWSZE INSTALUJ NAJNOWSZE **AKTUALIZACJE BEZPIECZEŃSTWA**, ZARÓWNO SAMEGO SYSTEMU OPERACYJNEGO, JAK I INNEGO OPROGRAMOWANIA, **NIE IGNORUJ ALERTÓW** BEZPIECZEŃSTWA ZGŁASZANYCH PRZEZ OPROGRAMOWANIE ANTYWIRUSOWE, NIE KORZYSTAJ Z **PIRACKIEGO OPROGRAMOWANIA**

SNIFFING – CO TO JEST ?

PRZECHWYTYWANIE
PRZEZ NIEUPRAWNIONE OSOBY
INFORMACJI PRZESYŁANYCH W
NIEZABEZPIECZONYCH PUBLICZNYCH SIECIACH, A TAKŻE **SIECIACH WIFI**

SNIFFING – JAK DZIAŁA ?

SNIFFING


JAKA PIĘKNA POGODA !!!
O! I WI-FI DOSTĘPNE !
ZOBACZĘ ILE MAM KASY NA KONCIE
NIE !!!!
GDZIE MOJA KASA !!!


CO ZROBIŁEM NIE TAK ?!?

SNIFFING

KEVINIE! ZAPOMNIAŁEŚ ŻE PRZY LOGOWANIU DO BANKOWOŚCI NIE WOLNO KORZYSTAĆ Z **NIEZABEZPIECZONYCH SIECI** I WŁAŚNIE KTOŚ PRZECHWYCIŁ TWOJE DANE.

JAK REAGOWAĆ

A CO MAM ZROBIĆ
GDY PIENIĄDZE
ZNIKNĘŁY
Z MOJEGO KONTA
W WYNIKU
PRZESTĘPSTWA ?

JAK REAGOWAĆ

1. **NALEŻY POINFORMOWAĆ RODZICÓW LUB OPIEKUNÓW**

2. **NALEŻY ZGŁOSIĆ REKLAMACJĘ DO BANKU**

BANK ZASTRZEŻE KARTĘ I ZABLOKUJE DOSTĘP DO BANKOWOŚCI ELEKTRONICZNEJ

DZIĘKUJĘ ZA UWAGĘ

IMIĘ I NAZWISKO PREZENTERA

Miejscowość, data