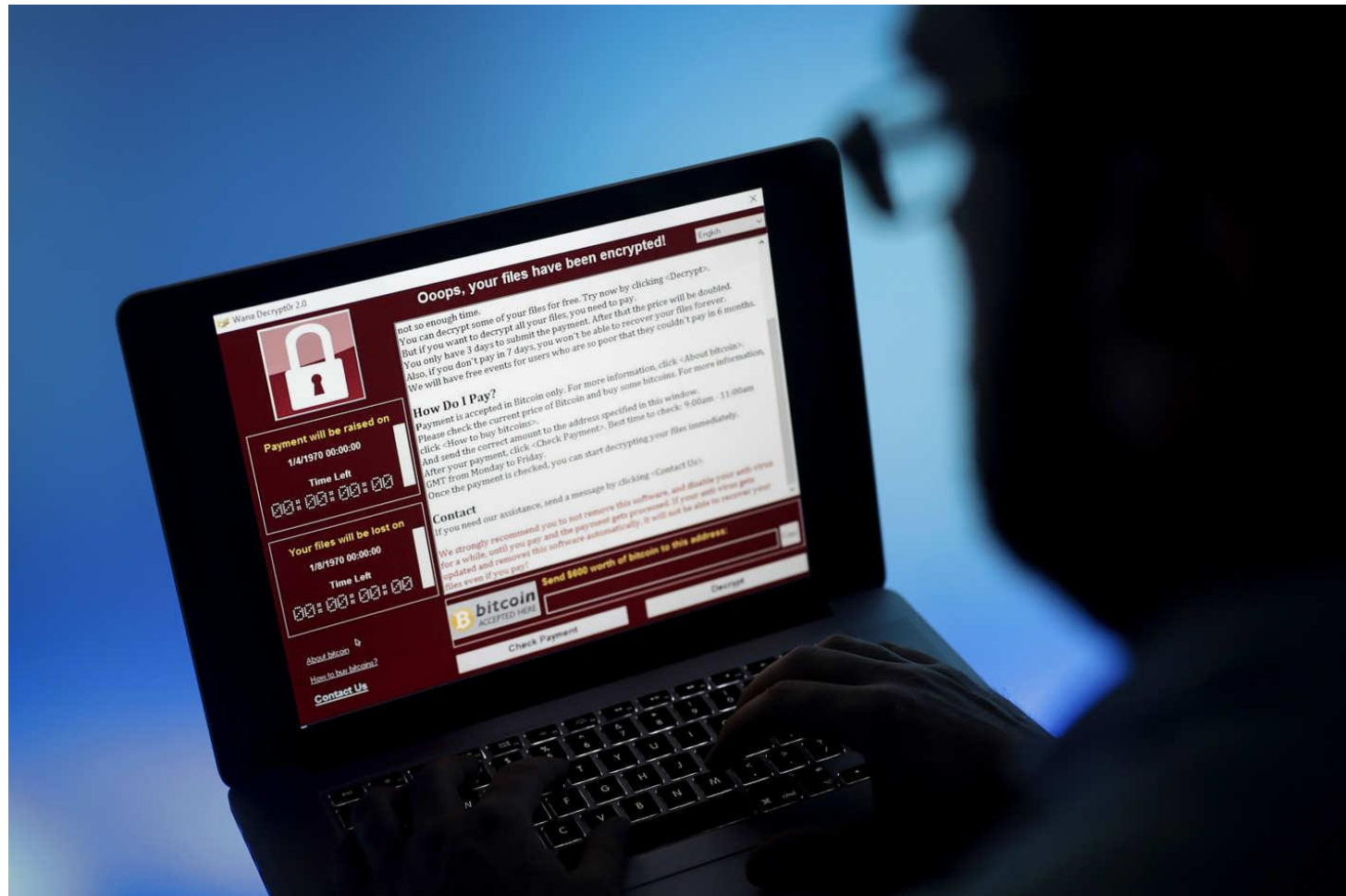


Nasze cyfrowe bezpieczeństwo



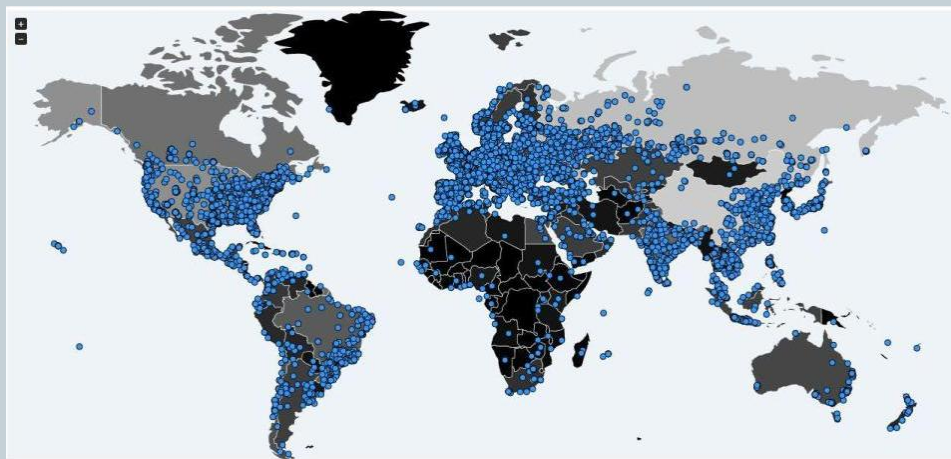
WannaCry



WannaCry – realne zagrożenie



- Jest to złośliwe oprogramowanie typu ransomware, które szyfruje zawartość dysku komputera i żąda zapłaty za przywrócenie dostępu do plików.
- Ogromna fala ataków rozpoczęła na początku maja i zainfekowanych zostało wiele komputerów w 99 krajach w tym i w Polsce.



Płać albo płacz



- Jeśli padniemy ofiarą ataku mamy trzy dni na zapłatę – w walucie Bitcoin.



Poprawki bezpieczeństwa Windows



- Windows XP SP3 – [pobierz](#)
 - Windows Vista x86 – [pobierz](#)
 - Windows Vista x64 – [pobierz](#)
 - Windows 8 x86 – [pobierz](#)
 - Windows 8 x64 – [pobierz](#)
-
- Dla Windows 7 należy uruchomić usługę aktualizacji automatycznej. Poprawka znajduje się w najnowszym pakiecie zabezpieczeń.



Bezpieczeństwo Wi-Fi



Czy Wi-Fi jest bezpieczne?

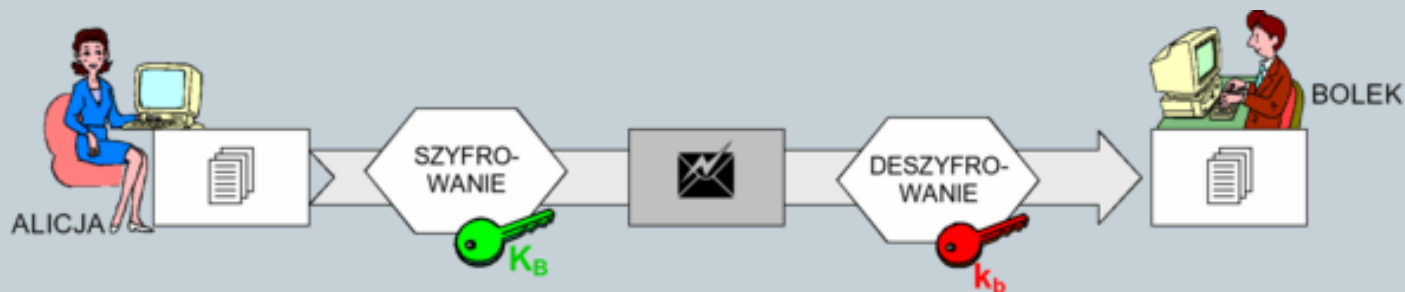


- Połączenie bezprzewodowe z Internetem jest bezpieczne jeśli jest szyfrowane!
 - To tak jakby rozmawiać przez radio lub walki-talki i dziwić się, że wszyscy wiedzą o czym była rozmowa.
- Jeśli łączymy się z siecią to musi ona mieć hasło oraz informacje o metodzie szyfrowanie WEP, WPA, WPA2, TKIP.
- Dla bezpieczeństwa nie łączymy się z bankiem, czy nie robimy zakupów przez Internet z kawiarni lub z pokoju hotelowego.

Bezpieczeństwo komunikacji



- Bezprzewodowe połączenie do Internetu jest mniej więcej tak bezpieczne jak rozmowa telefoniczna, czy wysyłanie wiadomości SMS.



- Uważajmy zatem na niezabezpieczone sieci, bo często są one obserwowane przez złodzieji danych osobowych!**

Zapamiętane dane logowania



Co robimy gdy się logujemy?



- Często widzę, że podczas logowania się np. do poczty, zapamiętują Państwo swoje dane w komputerze.
- Nie ma w tym nic złego jeśli to nasz domowy laptop, leżący na biurku. Gorzej jeśli jest to komputer publiczny.
- Po zapamiętaniu hasła każda osoba, która siada do danego komputera może dostać się do naszej poczty.

LOGOWANIE

NAZWA UŻYTKOWNIKA

HASŁO

☒ Zapamiętaj mnie

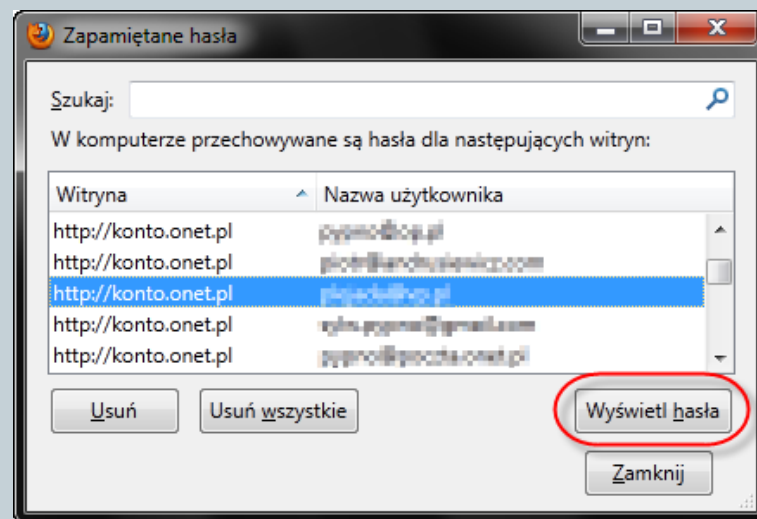
ZALOGUJ SIĘ

[Problem z hasłem?](#)

[Zarejestruj się już dziś!](#)

To nie koniec...

- Często mamy takie samo hasło do poczty i do innych usług np. bank, Facebook, Skype itp. Jeśli ktoś ma dostęp do naszej poczty spróbuje dostać się też do innych usług.
- **Opcje > Bezpieczeństwo > Zachowane dane logowania**



Tajemnica



Im mniej tym lepiej



- Często podajemy w Internecie nasze dane osobowe. Oczywiście jeśli robimy zakupy i chcemy, żeby kurier przywiózł zamówienie, to nie mamy wyjścia.
- Jeśli jednak zakładamy pocztę, logujemy się na forum czy do Skype-a, to nie musimy podawać wszystkich możliwych danych.
- Nasza prywatność i tak jest bardzo mocno naruszana w wielu sytuacjach, więc nie dokładajmy sobie jeszcze kolejnych.

Nie musimy się na wszystko zgadzać



- Często podczas rejestracji czy logowania do różnych usług zgadzamy się na przetwarzanie naszych danych osobowych.
- Nie musimy tego robić. Spróbujmy się nie zgadzać tam gdzie tylko jest to możliwe.
- Po co nam maile z reklamami, telefony od akwizytorów itp.?

Wyrażam zgodę na przetwarzanie moich danych osobowych, wskazanych w powyższym formularzu przez ABC Sp. z o.o. z siedzibą przy ul. Ulicznej 1, 00-000 Miasto w celu:

- ☐ przesyłania mi bezpłatnych promocyjnych opakowań kosmetyków naturalnych, z oferty sklepu www.stosuj-ziola.pl,
- ☐ przekazania danych osobowych do producentów kosmetyków naturalnych w celu przeprowadzenia badania poziomu satysfakcji z otrzymanych bezpłatnych opakowań,
- ☐ wysyłania na mój adres e-mail informacji handlowych o produktach dostępnych w sklepie: www.stosuj-ziola.pl.

Zalecana ostrożność



UWAGA!

Logowanie się, wpisywanie haseł, PIN



- Czy zastanawiali się Państwo po co nasze hasło jest zamieniane na gwiazdki „*****”?
- Na pewno nie dla utrudnienia, ale dlatego, by nikt patrzący nam przez ramię nie poznał naszego hasła.
- Takie mechanizmy jednak nic nie dadzą jeśli sami nie będziemy ostrożni.
- Często hasło mamy zapisane na kartce obok komputera lub podczas wpisywania wymawiamy je szeptem. To nie jest bezpieczne!

Zasłaniajmy klawiaturę – to pomaga



- Podczas wizyty w bankomacie, czy gdy kupujemy coś w sklepie, powinniśmy zasłonić klawiaturę, gdy wpisujemy PIN.



To samo dotyczy telefonu



- Jeśli piszemy lub czytamy SMS-y, albo jeśli przeglądamy pocztę czy Facebook nie róbmy tego tak, że pól autobusu widzi nasze prywatne dane.



Hasła



Każda usługa – inne hasło



- Dla naszego bezpieczeństwa każda usługa do której się logujemy np. poczta, bank, Facebook, sklep – powinna mieć oddzielne hasło.
- Jeśli ktoś dostanie się do naszej poczty to z łatwością sprawdzi z jakich usług korzystamy (mail rejestracyjny).
- **Jeśli mamy podejrzenie, że ktoś zna nasze hasło, to najlepiej od razu je zmienić i to wszędzie tam, gdzie go używamy!**

Komunikacja z bankiem



Czego nie robi bank?



- Nie wysyła do nas mail z prośbą o dane osobowe.
- Nigdy nie pyta o numer karty, jej datę ważności czy kod CVC/CVV (te numerki na odwrocie)
- Nigdy nie pyta także o nasz PIN, nie prosi o jego potwierdzenie, ani o zmianę!
- Jeśli dostaniemy maila proszącego o powyższe dane powinniśmy powiadomić o tym bank. Dowiemy się wtedy, że nasze pieniądze są bezpieczne i poinformujemy pracowników banku o próbie oszustwa i może ktoś inny zostanie ochroniony.

Fałszywe komunikaty – PKO BP



Twój dostęp on-line została zablokowana

Dla Twojego bezpieczeństwa, mamy zablokowane konta.

Aby przywrócić dostęp do swojego konta, kliknij: [Zaloguj się do iPKO](#) i przystąpić do procesu weryfikacji.

© 2014 PKO Bank Polski

Fałszywe komunikaty – mBank



Wiadomość dotycząca bezpieczeństwa. Twoje konto mBank zostało tymczasowo zablokowane. Odebrane x



mBank przez s7.jupe.pl
do mnie ▾

14:15 (7 minut temu) ☆



Szanowny kliencie,



Twój dostęp do serwisu transakcyjnego mBank Online został tymczasowo zablokowany ze względów bezpieczeństwa.

Wykryliśmy podejrzane działania związane z Twoim kontem bankowym.

Aby uzyskać więcej informacji oraz odblokować dostęp online, należy przejść na stronę mBanku <https://online.mbank.pl/pl/odblokuj> i zweryfikować swoje dane.

Fałszywe komunikaty – Bank Zachodni



Bank Zachodni WBK S.A.

Uaktywnij konto BZ WBK 24

Aby uaktywnić konto BZ WBK 24, należy kliknąć poniższe łącze i wprowadzić Numer karty na wyświetlonej stronie w celu potwierdzenia BZ WBK 24.

[Kliknij tutaj, aby uaktywnić konto](#)

BZ WBK 24 możesz również potwierdzić, logując się do swojego konta BZ WBK 24 pod adresem <https://www.centrum24.pl/bzwbk24.html>.

Dziękujemy za korzystanie z systemu BZ WBK 24!
Zespół BZ WBK 24.

Bank Zachodni WBK S.A.

Masz pytanie zadzwoń - 0-801-666-444

Bezpieczeństwo w sieci



5 ZASAD BEZPIECZEŃSTWA W SIECI

1. 

CHROŃ SWOJE HASŁA
używaj różnych haseł
do różnych usług

2. 

OSTROŻNIE KORZYSTAJ
z niezabezpieczonych
sieci wi-fi

3. 

PAMIĘTAJ AKTUALIZOWAĆ
oprogramowanie
antywirusowe

4. 

CZYTAJ REGULAMINY
i polityki prywatności

5. 

ZAINSTALUJ W PRZEGLĄDARCE
wtyczki pozwalające uniknąć śledzenia
Twoich zachowań w internecie

Aktualizacje



- Regularne aktualizacje pozwalają chronić komputer przed niebezpieczeństwami takimi jak włamania, wirusy itp.
- Dlaczego zatem wyłączamy aktualizacje?
 - Bo często trwają wiele godzin
 - Podczas instalowania komputer działa wolniej
 - Czasem zmuszają nas do niechcianych zmian
 - Zdarza się, że zamiast pomagać szkodzą
 - Mamy nielegalny system więc nie aktualizujemy
 - Mamy stary system, który już nie jest wspierany



Przeglądarka



- Dobrze jest zainstalować program do blokowania reklam i skryptów śledzących taki jak np. uBlock Origin.
 - Dla Chrome – [Pobierz](#)
 - Dla Firefox – [Pobierz](#)



Rozważne logowanie



- Podczas logowania się do poczty czy banku zwróćmy uwagę na to, czy połączenie jest bezpieczne i zaszyfrowane.



<https://www.formsite.com/yourform/>

Transakcje finansowe



Ćwiczenia na przykładzie banku



- Wejdźmy na www.pekao24.pl



Dziękuję za uwagę ;)



DO NASTĘPNEGO SPOTKANIA!