Szybuj bezpiecznie w internetowej chmurze 2019

82% Polaków zagląda do internetu codziennie

13% Polaków zagląda do internetu raz w tygodniu

5% Polaków zagląda do internetu raz w miesiącu

Polak w internecie spędza średnio

5 godzin

i 55 minut,

z czego:

ponad
3 godziny
poświęca na oglądanie filmów i różnych relacji on-line

1 godzinę
i 42 minuty
zajmuje przeglądanie portali społecznościowych

ponad
40 minut
to słuchanie muzyki

Polski Instytut Cyberbezpieczeństwa szacuje ponadto, że:

Polacy wysyłają
250 mln
SMS-ów
dziennie

oraz

poświęcają swojemu smartfonowi
3 godziny
każdej doby.

SKALA CYBERPRZESTĘPCZOŚCI

556 MILIONÓW OFIAR ROCZNIE

TO WIĘCEJ NIŻ CAŁA POPULACJA UNII EUROPEJSKIEJ

7,2 MILIONA OFIAR ROCZNIE W POLSCE

1.5+ MILIONA
OFIAR DZIENNIE

18 OFIAR NA SEKUNDĘ

GLOBALNE KOSZTY SPOWODOWANE CYBERPRZESTĘPCZOŚCIĄ

$110 MLD

85% KOSZTÓW BEZPOŚREDNICH TO EFEKT OSZUSTW, KRADZIEŻY I STRAT ORAZ NIEZBĘDNYCH NAPRAW

ŚREDNI KOSZT W PRZELICZENIU NA 1 OFIARĘ **197 USD**

STRATY W POLSCE SPOWODOWANE CYBERPRZESTĘPCZOŚCIĄ

4,8 MLD ZŁ

ŚREDNI KOSZT W PRZELICZENIU NA 1 OFIARĘ

672 ZŁ

Cyberprzestępczość - definicja

- w polskim prawie brak jest jednolitej definicji cyberprzestępstwa;
- ogólnie jest to szereg przestępstw określonych w Kodeksie Karnym, do których popełnienia doszło przy użyciu komputerów lub Internetu;
- komputer/Internet mogą służyć do popełnienia przestępstwa:
  - jako narzędzie przestępstwa
  - jako cel ataku
  - jako urządzenie związane z popełnieniem przestępstwa

Cyberprzestępczość - problematyka

W celu dokonania cyberprzestępstwa sprawcy stosują różne metody i narzędzia, takie jak np.:

- wyłudzanie danych (phishing),
- wirusy, oprogramowanie typu spyware lub ransomware,
- socjotechnika

Co to jest Phishing ?

Phishing to oszustwo stosowane przez internetowych przestępców w celu uzyskania cennych informacji, takich jak:

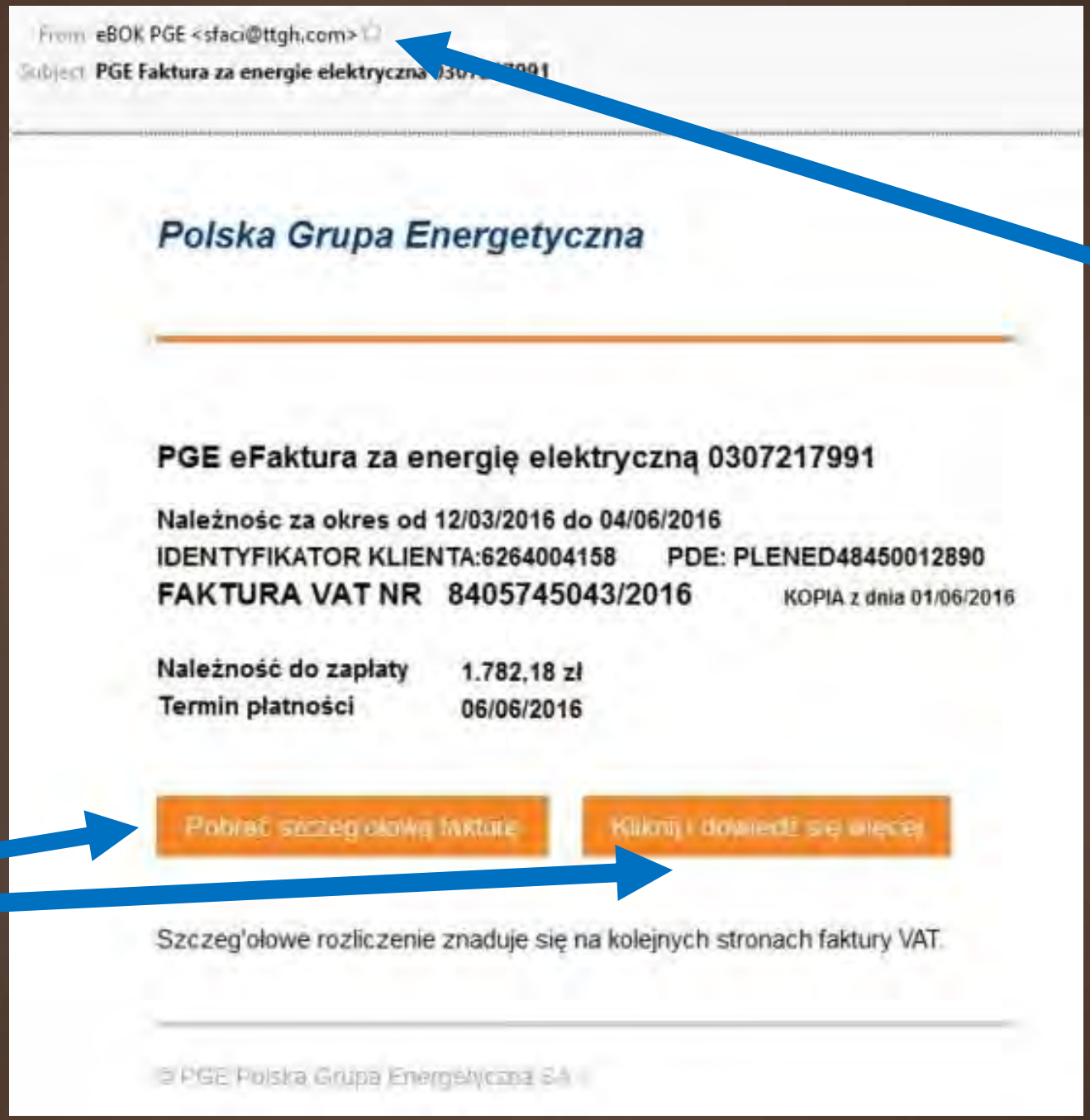
- loginy,
- hasła,
- numery kart kredytowych

Nazwa budzi dźwiękowe skojarzenia z "fishingiem" – czyli łowieniem ryb. Przestępcy, podobnie jak wędkarze, stosują bowiem odpowiednio przygotowaną „przynętę". W tej roli wykorzystują najczęściej sfałszowane e-maile i SMS-y. Coraz częściej oszuści działają także za pośrednictwem komunikatorów i portali społeczności.

Przykłady phishingu – jak to działa?

UWAGA!
PO KLIKNIĘCIU ZAINSTALUJE SIĘ ZŁOŚLIWE
OPROGRAMOWANIE

UWAGA!
FAŁSZYWY
ADRES E-MAIL


From eBOK PGE <sfaci@ttgh.com>
Subject PGE Faktura za energie elektryczna
Polska Grupa Energetyczna
PGE eFaktura za energię elektryczną 0307217991
Należnośc za okres od 12/03/2016 do 04/06/2016
IDENTYFIKATOR KLIENTA:6264004158 PDE: PLENED48450012890
FAKTURA VAT NR 8405745043/2016 KOPIA z dnia 01/06/2016
Należność do zapłaty 1.782,18 zł
Termin płatności 06/06/2016
Pobrać szczegółową faktur
Kliknij i dowiedz się więcej
Szczegółowe rozliczenie znaduje się na kolejnych stronach faktury VAT.
© PGE Polska Grupa Energetyczna SA

UWAGA!

UWAGA!

Od: "ING" <mail@imdetective.net>
Data: 1 grudnia 2018 17:14:58 CET
Do: [redacted]
Temat: **Blokoda konta ING**
Odpowiedz-do: "ING" <maillist@mailserver.com>

ING

ING BANK ŚLĄSKI

fot.-niebezpiecznik.pl

Blokada konta ING Bank Śląski

W trosce o bezpieczeństwo naszych odbiorców zablokowaliśmy konto w ING Bank Śląski, powodem jest włamanie do konta.

W celu odblokowania dostępu prosimy o weryfikację właściciela konta, logując się na:

Zaloguj aby odblokowac

Zespół ING BANK ŚLĄSKI

Więcej informacji można uzyskać dzwoniąc na infolinię pod numer: 801 222 222.

Prosimy, nie odpowiadaj na tą wiadomość - została wysłana automatycznie.

[redacted]

www.ingbank.pl INGMobile oddział banku 801 22 22 22

UWAGA!

UWAGA!

Jak się bronić przed phishingiem?

- Pamiętaj o tym, że w sieci należy stosować **zasadę** ograniczonego zaufania. Odruchowe klikanie w linki i pobieranie plików z nieznanych źródeł jest bardzo ryzykownym zachowaniem – zanim otworzysz wiadomość od „firmy kurierskiej", zastanów się, czy faktycznie czekasz na jakąś przesyłkę

- Zanim otworzysz załącznik, dokładnie przeczytaj treść e-maila. Fałszywe wiadomość bardzo często (choć nie zawsze) zawierają **błędy ortograficzne, gramatyczne i** interpunkcyjne

- Jeżeli masz wątpliwości, czy wiadomość faktycznie pochodzi od danej firmy czy instytucji, skontaktuj się z jej przedstawicielem

- Zwróć uwagę na dane nadawcy wiadomości. Adresy mailowe, którymi posługują się oszuści, mogą się różnić od tych autentycznych łatwymi do przeoczenia szczegółami, np. literówką w nazwie domeny – zamiast kontakt@bank.pl – kontakt@bank.ppl. Adresy mogą również zawierać **przekręconą lub niepełną nazwę firmy** czy instytucji

- Przed kliknięciem w link dokładnie się mu przyjrzyj. Oszuści często wykorzystują pozornie banalne, ale trudne do wykrycia sztuczki – np. zastępują literę „l" cyfrą „1", a literę „O" – cyfrą „0". Jeżeli chcesz zalogować się do serwisu transakcyjnego banku, najbezpieczniej będzie, jeżeli **własnoręcznie wprowadzisz jego adres www**

Co to jest socjotechnika?

Najsłabszymi ogniwami w dowolnym łańcuchu bezpieczeństwa są ludzie. Socjotechnika stara się wykorzystać te słabe ogniwa przez odwołanie się do próżności, chciwości, ciekawości i altruizmu ludzi lub do ich poszanowania lub strachu przed władzą w celu nakłonienia ich do ujawnienia pewnych informacji lub przejęcia dostępu do systemu informatycznego

Przykłady socjotechniki – jak to działa ?

Oszustwo „nigeryjskie” – na amerykańskiego żołnierza

Osoba podająca się za amerykańskiego żołnierza ze zdjęcia

Oszustwo internetowe – atrakcyjna cena / okazja !!!

Audi Q5 (7639851667)

Kategoria: 8R (2008-2016)
Lokalizacja: Zapałów

ZOBACZ AKTUALNE OFERTY

AKTUALNE PRZEDMIOTY SPRZEDAJĄCEGO

zgłoś naruszenie zasad

Przykład kradzieży tożsamości „na ofertę pracy”

- Sprawca zamieszcza na portalu ogłoszeniowym ofertę pracy
- Po nawiązaniu kontaktu przez osobę zainteresowaną ogłoszeniem, sprawca prosi o przesłanie CV, skanów dowodu osobistego, prawo jazdy, itp.
- Sprawca przysyła ofierze fikcyjną umowę o pracę
- W międzyczasie sprawca zakłada rachunek bankowy na dane ofiary, które pozyskał ze skanów dokumentów oraz CV
- Sprawca prosi ofiarę o przelew w kwocie 1 zł/ 1 gr na założony uprzednio rachunek na dane ofiary celem potwierdzenia danych dla banku
- Na założony na dane ofiary rachunek sprawca zaciąga tzw. chwilówki

Aby bezpiecznie korzystać z Internetu, wykorzystuj następujące metody:

- Bądź anonimowy. Jeśli nie musisz podawać swoich danych prywatnych — nie rób tego. Im mniej informacji o tobie jest w sieci, tym jesteś bezpieczniejszy.

- Ustaw „silne” hasła. Ważne, aby twoje hasła były jak najdłuższe. Miej wiele haseł i czesto je zmieniaj.

Najpopularniejsze hasła 2018 roku

1. 123456
2. password
3. 123456789
4. 12345678
5. 12345
6. 111111
7. 1234567
8. sunshine
9. qwerty
10. iloveyou

- Sprawdzaj, czy łączysz się bezpiecznie (przez połączenie https://). Bezpieczne połączenia oznacza się za pomocą zielonego zaznaczenia lub kłódeczki koło paska adresu. Czasem występuje problem z bezpieczeństwem połączenia i pojawiają się ostrzeżenia o błędach certyfikatu. Nie ignoruj ich, zwłaszcza jeśli witryna nie jest godna zaufania lub wcześniej nie pojawiał się na niej błąd.

- Zainstaluj program taki jak np.: Adblock, NoScript, Flashblock, Cookie Monster. Te programy blokują niepożądane elementy stron

- Wyloguj się po pracy. Nie można o tym zapomnieć!

DZIĘKUJĘ ZA UWAGĘ

podkom. Łukasz Pietrzyk
Wydział dw. z Cyberprzestępczością
KWP w Kielcach
e-mail: lukasz.pietrzyk@ki.policja.gov.pl
tel: 41 349 15 23, 607269836