



Udostępnianie danych i ryzyko ich wykorzystania w przestępstwach finansowych

WYDZIAŁ PREWENCJI KWP ZS. W RADOMIU



Komputer z dostępem do Internetu jest jednym z najważniejszych narzędzi służących współczesnemu człowiekowi do pracy, nauki i rozrywki. Jak każde narzędzie może być wykorzystywane do różnych celów.



CYBERBEZPIECZEŃSTWO

90% Polaków czuje się bezpiecznie korzystając z bankowości elektronicznej (badanie ZBP i CPBiI, 2019)

59% Polaków postrzega banki jako liderów cyberbezpieczeństwa obok wojska i Policji oraz instytucji rządowych (badanie ZBP i CPBiI, 2019)

65% Polaków słabo ocenia swoją wiedzę z zakresu cyberbezpieczeństwa (poziom wiedzy finansowej Polaków 2019 Warszawski Instytut Bankowości)

39% Polaków aktualizuje hasło do bankowości mobilnej minimum raz w roku (badanie ZBP i CPBiI, 2019)

40% Polaków deklaruje, że jest słabo poinformowanych na temat ryzyka cyberprzestępstw w sieci (Komisja Europejska, 2019)



Phishing

Typ oszustwa internetowego, w którym sprawca podstępem
wyłudza od użytkownika jego osobiste dane.

Phishing obejmuje kradzież haseł, numerów kart kredytowych, danych kont bankowych i innych poufnych informacji

Podszywanie się pod bank poprzez:

strony www

wiadomości e-mail

portal
społecznościowy

sklepy internetowe

Phishing

Zagrożenia w Internecie

- fałszywe witryny,
- wiadomości e-mail, których celem jest wyłudzenie informacji,
- zagrożenie w trakcie korzystania z portali społecznościowych,
- cloud (Chmura) – dane w Sieci,
- fałszywe oprogramowania,
- wykradanie danych osobowych,
- skrócone adresy url, literówka w adresach www,
- nieaktualne oprogramowanie,
- fałszywe sklepy internetowe,
- hot-spot.





Phishing

Nie daj się nabrać, twój bank nigdy tego nie robi...

Nie wysyła informacji o blokadzie konta e-mailem;

Nie wysyła wiadomości e-mailem zawierającym link do serwisu bankowości internetowej;

Nie podaje linków do systemu transakcyjnego w e-mailach lub SMS-ach;

Nie dzwoni z prośbą o podanie hasła do konta lub numeru karty.

Phishing

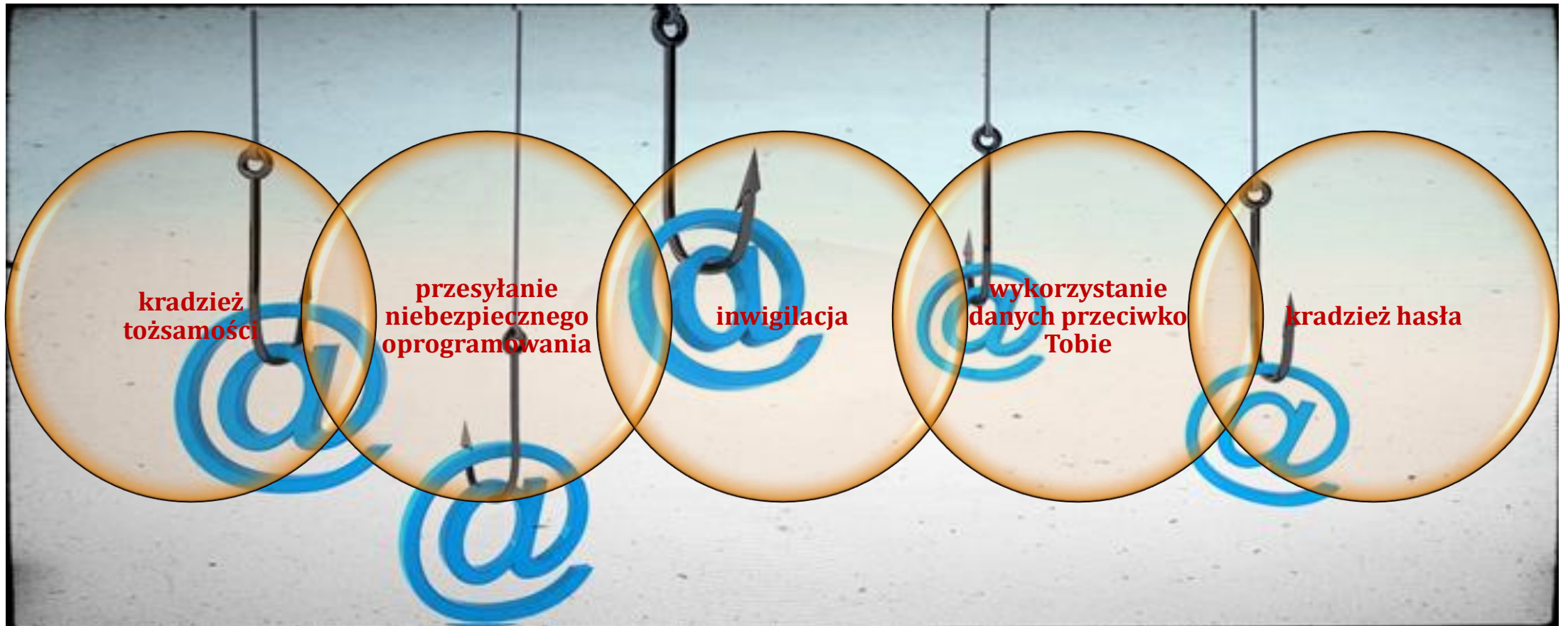
Uważaj na wiadomości e-mail...

- nieodebrana przesyłka pocztowa lub kurierska,
- egzekucja zajęcia konta bankowego,
- blokada konta bankowego,
- od firm, których nie znasz,
- fałszywe faktury,
- fałszywe rezerwacje np. hoteli,
- lokalizacja numerów telefonu,
- szansa otrzymania wyjątkowej nagrody.



Phishing.

Zagrożenia w trakcie korzystania z portali społecznościowych...





Włamania

Działania:

Włamanie do miejsca w Internecie strzeżonego hasłem lub innym zabezpieczeniem.

Formy:

Włamania na:

- ❖ konto e-mailowe, na bloga;
- ❖ profil w serwisie społecznościowym;
- ❖ inne miejsce strzeżone hasłem lub innym zabezpieczeniem w celu uzyskania jakichś informacji.

Włamanie (jak wyżej) oraz wprowadzanie zmian typu: zmiana hasła, dokonanie zmian w treści czy w wyglądzie strony/profilu, dodanie lub usunięcie zdjęć, niszczenie, uszkodzanie.



Włamania

Kodeks karny

Art. 267.

§ 1. Kto bez uprawnienia uzyskuje dostęp do informacji dla niego nieprzeznaczonej, otwierając zamknięte pismo, podłączając się do sieci telekomunikacyjnej lub przełamując albo omijając elektroniczne, magnetyczne, informatyczne lub inne szczególne jej zabezpieczenie, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2.

§ 2. Tej samej karze podlega, kto bez uprawnienia uzyskuje dostęp do całości lub części systemu informatycznego.

§ 3. Tej samej karze podlega, kto w celu uzyskania informacji, do której nie jest uprawniony, zakłada lub posługuje się urządzeniem podsłuchowym, wizualnym albo innym urządzeniem lub oprogramowaniem.

§ 4. Tej samej karze podlega, kto informację uzyskaną w sposób określony w § 1-3 ujawnia innej osobie.

§ 5. Ściganie przestępstwa określonego w § 1-4 następuje na wniosek pokrzywdzonego.

Art. 268a.

§ 1. Kto, nie będąc do tego uprawnionym, niszczy, uszkadza, usuwa, zmienia lub utrudnia dostęp do danych informatycznych albo w istotnym stopniu zakłóca lub uniemożliwia automatyczne przetwarzanie, gromadzenie lub przekazywanie takich danych, podlega karze pozbawienia wolności do lat 3.

§ 2. Kto, dopuszczając się czynu określonego w § 1, wyrządza znaczną szkodę majątkową, podlega karze pozbawienia wolności od 3 miesięcy do lat 5.

§ 3. Ściganie przestępstwa określonego w § 1 lub 2 następuje na wniosek pokrzywdzonego.



Co więc mamy jeszcze...



KODEKS KARNY

- **Zniesławienie** – art. 212
- **Znieważenie** – art. 216
- **Włamanie na konto internetowe** – art. 267, 268a
- **Groźby** – art. 190, 191
- **Rozpowszechnianie pornografii** – art. 202



KODEKS CYWILNY

- **Naruszenie wizerunku** – art. 23 i 24



KODEKS WYKROCZEŃ

- **Złośliwe niepokojenie** – art. 107
- **Wulgaryzmy** – art. 141

Akty prawne



kradzież / zagubienie

W przypadku utraty karty niezwłocznie zgłoś ten fakt
w **PLACÓWCE BANKU** lub pod ogólnopolskim numerem telefonu

+48 828 828 828



Dowód osobisty – czemu jest tak ważny?

**Jest to dokument, który potwierdza tożsamość,
każda osoba pełnoletnia ma obowiązek posiadać dowód.**

W przypadku utracenia dowodu osobistego jak najszybciej zastrzeż go w placówce bankowej oraz powiadom Policję w przypadku jego kradzieży.

Im szybciej to zrobisz, tym większa masz pewność, że nie zostanie on wykorzystany przez przestępców, w celu wyłudzenia pieniędzy (kredytu).

Osoba, która znalazła dowód osobisty innej osoby, jest obowiązana niezwłocznie przekazać ten dokument najbliższemu organowi gminy, Policji lub innemu organowi administracji publicznej. A urzędy te przekazują niezwłocznie dokument organowi, który go wydał, w celu unieważnienia go.

Osoba, która znalazła dowód osobisty innej osoby, może, bez zbędnej zwłoki, przekazać ten dokument posiadaczowi dowodu osobistego.

Sytuacje, gdy ktoś się posługuje cudzym dowodem osobistym, żeby wyłudzić kredyt, towar czy usługi nie należą do rzadkości . Banki co roku odnotowują kilka tysięcy prób wyłudzeń pieniędzy na skradziony dokument tożsamości.



Jak być bezpiecznym w Internecie?

Zasady bezpieczeństwa!

1. Zanim dołączysz

Kontakty z ludźmi na portalach społecznościowych, podobnie jak kontakty z ludźmi w świecie rzeczywistym, rządzą się pewnymi zasadami. Zastanów się w jaki sposób działa portal zanim utworzysz na nim swój profil. Przede wszystkim zainteresuj się jaki poziom prywatności gwarantuje Ci dany portal. Informacji tego typu szukaj w regulaminie, który powinien jasno określać zasady twojego uczestnictwa w serwisie.

2. Prywatność

Kontroluj dostęp do Twoich danych i innych informacji, które umieszczasz w swoim profilu. Bezpieczny portal społecznościowy powinien pozwolić Ci nadać sobie taki status prywatności, który zagwarantuje, że informacje o Tobie będą dostępne tylko dla znajomych, których świadomie dodałeś/aś do swojej listy. Pamiętaj też, że Twoje hasło to Twój sekret.



Zasady bezpieczeństwa!

3. Informacje o mnie

Zamieszczając informacje o sobie pamiętaj, że potencjalnie każdy może je zobaczyć. Dbaj o to, żeby nie ujawniać swoich danych osobowych. Stwórz bezpieczny Nick, który nie zdradzi Twojej prawdziwej tożsamości. Sieć daje nam możliwość bycia kimś innymi niż w codziennym życiu.

Znaj jednak swoje granice tej zabawy - myśl jak się prezentujesz.

4. Zdjęcia

Zastanów się dobrze zanim zamieścisz w Sieci swoje zdjęcia, które mogą być użyte, przez innych użytkowników Sieci, w sposób jakiego byś sobie nie życzył/a lub skopiowane do miejsca, w którym byś ich nie zamieścił/a. Jeżeli już na pewno chcesz zamieścić swoje zdjęcia w Internecie ustaw taki status prywatności, który zagwarantuje Ci bezpieczeństwo.



Zasady bezpieczeństwa!

5. Zagrożenia

Uważaj na e-maile od nieznanych Ci osób. Nigdy nie otwieraj podejrzanych załączników i nie korzystaj z linków przesłanych przez obcą osobę! Mogą na przykład zawierać wirusy. Najlepiej od razu kasuj maile od nieznanomych.

6. Dane osobowe

Jeżeli prowadzisz w Internecie stronę lub bloga, pamiętaj, że mają do niej dostęp osoby o różnych zamiarach. Nigdy nie podawaj na swojej stronie adresu domowego, numeru telefonu, informacji o rodzicach, itp. Bez zgody nie publikuj też na niej zdjęć swoich, rodziny ani nikogo innego, kto nie wyrazi na to zgody. Zadbaj o ukrycie przed obcymi swoich prawdziwych danych. Nie używaj także w adresie poczty elektronicznej swojego imienia i nazwiska.



CO MY ROBIMY JAKO POLICJA

DZIAŁANIA PROFILAKTYCZNE I KAMPANIE INFORMACYJNE

- rozmowy;
- pogadanki w szkołach;
- projekty profilaktyczne;
- spoty profilaktyczne;
- materiały profilaktyczne.

**Wszystko dostosowane do
grupy odbiorców**

DZIAŁANIA PREWENCYJNE:

- filtry, kontrola przeglądanych stron, właściwa reakcja na niepożądane zachowania dzieci i młodzieży;

SYSTEM ZAPOBIEGANIA CYBERPRZEMOCY W SZKOLE:

- opracowanie procedur reagowania na cyberprzemoc,
- podejmowanie interwencji w każdym przypadku ujawnienia lub podejrzenia cyberprzemocy,
- sankcje regulaminowe szkoły,
- kontrakt z rodzicami.

Dziękuję za uwagę