# Ekonomiczny Uniwersytet Dziecięcy

## Bezpieczeństwo w sieci

Joanna Bienia - Fijas

**Politechnika Gdańska**
8 kwietnia 2021r



1

## Co nam grozi?

- Phishing
- Vhishing, czyli voice phishing
- Smishing

2

## Policja ostrzega!

Co się dzieje, gdy przestępca staje się Tobą?

Dlaczego amerykańskie żołnierki lubią Polaków, a jemeńscy lekarze Polki?

3

## Media społecznościowe - Jak się chronić?

- Sprawdź w ustawieniach, czy ktoś nie grzebał w Twoim Facebooku.
- Ustaw dwuskładnikowe uwierzytelnianie podczas logowania się.
- Zanim weźmiesz udział w promocji, głosowaniu, ankiecie sprawdź na oficjalnych stronach marki, czy organizują taką akcję.
- Reaguj na dziwne, podejrzane posty, wiadomości od Twoich znajomych.
- Znajomy ma do Ciebie niecodzienną prośbę – zadzwoń do niego.
- Miej bardzo! ograniczone zaufanie do znajomych z internetu.

4

## Policja ostrzega!

Które SMS-y są niebezpieczne?

5

## Smishing - Jak się chronić?

- Nie wchodź w żadne linki przesłane SMS-em!
- Oprogramowanie, aplikacje aktualizuj na smartfonie, nie przy pomocy linku
- Nie pobieraj aplikacji od nieznanych dostawców
- Zadzwoń do nadawcy sms-a (na policję, infolinię firmy kurierskiej ). Numer sprawdź na stronie.
- Zgłoś podejrzane sms-y.

6

## Policja ostrzega!

Kiedy **MUSISZ** zignorować maila z Urzędu Skarbowego?
I z ZUSu też.

7

## Podejrzane maile - Jak się chronić?

Zachowaj szczególną ostrożność jeśli wiadomość:

- pochodzi od nieznanego, podejrzanego nadawcy,
- została wysłany nieoficjalnej domeną firmy,
- zawiera załącznik w formacie .exe, .vbs, .rar, .zip, .tar, zaszyfrowany, z hasłem przesłanym w treści e-maila; pdf, .docx, .xslx (jeśli żąda włączenia makr)
- zawiera odnośniki prowadzące do nieznanych stron www,
- zawiera błędy językowe, literówki, jest nieskładny
- zawiera treść, której nie oczekiwałaś/eś (np. fakturę, awizo, dokumentację),
- zawiera prośbę o podanie danych wrażliwych (login, hasło, PESEL).

8

## Podejrzane maile - Co zrobić, gdy otworzyliśmy zawarte w nich linki?

- Nie korzystaj z tego urządzenia do logowania się do jakiegokolwiek systemu bankowości elektronicznej.
- Zmień hasła do wszystkich wykorzystywanych aplikacji i serwisów internetowych (systemów bankowości, poczty elektronicznej, portali społecznościowych itp.) - do zmiany haseł wykorzystaj inne urządzenie niż to, na którym otwarty był załącznik.
- Przeskanuj urządzenie programem antywirusowym. Po znalezieniu problemu, postępuj zgodnie z jego wskazówkami.
- Może być potrzebne ponowne zainstalowanie systemu. Zrób to.
- Poinformuj policję i rzekomego nadawcę.

9

## Policja ostrzega!

Jak **NIE STRACIĆ** majątku na sprzedaży drobiazgu?

10

## Sprzedaż na portalach - Jak się chronić?

- Propozycja zapłaty poprzez wiadomości mailowe, SMS-y i komunikatory, które zawierają linki, jest podejrzana.
- Nigdy nie podawaj numeru karty płatniczej po to aby otrzymać pieniądze.
- Nie ufaj żadnym zrzutom ekranu lub plikom PDF z potwierdzeniem nadania przelewu.
- Ustaw limity na karcie.
- Sprawdzaj adres strony.
- Czytaj DOKŁADNIE smsy z banku.
- Zwróć uwagę na sposób komunikacji.

11

## BANKI ostrzegają!

Jak **nie oddać KOMPUTERA** w ręce oszustów?

12

## Kradzież na zdalny pulpit - Jak się chronić?

- NIGDY NIKOMU nie udostępniaj swojego konta bankowego i danych logowania
- „konsultant”, który proponuje zainstalowanie oprogramowania typu Any Desk, to ZŁODZIEJ
- jeśli osoba podająca się za pracownika banku żąda zweryfikowania Twoich danych i danych konta lub zainstalowania jakiegokolwiek oprogramowania rozłącz się i zadzwoń do banku

13

## Co na to bank? - Chroń swoje dane!

- dane do logowania
- kody autoryzacyjne i kody PIN
- dane osobowe

14

## Co na to bank? - Jak się chronić?

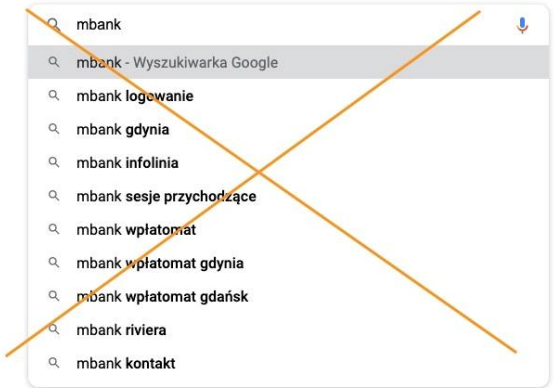
- Bank nie wysyła odnośników do strony logowania w wiadomościach SMS ani w e-mailach.
- Nie loguj się do banku, lub innych serwisów poprzez linki zawarte w wiadomościach e-mail lub SMS.
- Nie instaluj aplikacji z linków nadesłanych SMS-em, komunikatorem, pocztą elektroniczną.
- Ustaw hasło zwrotne.
- Nie wpisuj kodu z smsa, którego **dokładnie** nie sprawdzisz.
- Podejrzane rozmowy, smsy, maile zgłoś do banku.

15

## Jak się prawidłowo logować?


16

## Jak się NIE logować?



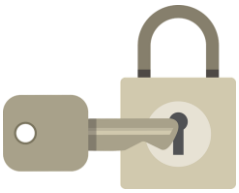

17

## Jak się prawidłowo logować?

- Nie dodawaj strony banku do zakładek.
- Loguj się **tylko** ze strony głównej banku.
- Z bankowości internetowej korzystaj **tylko** na swoim komputerze/smartfonie.
- Zawsze się wyloguj.
- Sprawdź numer rachunku odbiorcy – **nie tylko,** jeżeli go kopiujesz.
- Czytaj otrzymanego SMSa z kodem do operacji.
- Miej **bezpieczne hasła.**

18

## Jakie hasło jest bezpieczne?



- Unikalne
- Silne – stosuj zasadę 8-4
- Hasło musi być inne niż login.
- Nie używaj:

  - istniejących wyrazów (w żadnym języku)
  - dat i numerów związanych z Twoim z życiem

- Przechowuj hasła w bezpiecznym miejscu
- Sprawdź, czy Twoje dane nie wyciekły np. na stronie Identity Leak Checker

19

## Bezpieczne aplikacje, czyli jakie?

- Tylko z zaufanych sklepów, ale i tak **UWAŻAJ!**
- Sprawdź uprawnienia aplikacji.
- Usuń aplikację, gdy masz najmniejsze podejrzenia.
- Weryfikuj listę zainstalowanych aplikacji.
- Włącz funkcję Play Protect.

20

## Policja ostrzega!

Jak **NIE PRZESTAĆ BYĆ**
właścicielem swojego telefonu?

21

## Wyłudzenia karty SIM – Jak się chronić?

- Jeżeli Twój numer jest publiczny **NIE** podpinaj go do konta.
- Ogranicz udostępnianie danych o sobie.
- Jeśli Twój telefon nagle traci zasięg bez wyraźnego powodu, skontaktuj się z operatorem i ustal, czy ktoś nie wyłudził Twojej karty SIM.

22

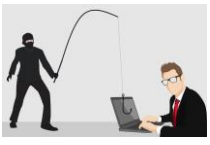
## Policja ostrzega!

Kiedy **ZAKUPY** są niebezpieczne?

23

## Zakupy internetowe – Jak się chronić?

- Sprawdź sklep:
  - dane sprzedawcy
  - zabezpieczenie sklepu certyfikatem SSL
  - opinię i historię strony
- Porównaj ceny. **SUPER** promocje są podejrzane!
- Wybierz bezpieczną płatność



24

## Bezpieczna płatność, czyli…

- Unikaj:
  - przelewów ekspresowych
  - przelewania pieniędzy na prywatne konta sprzedającego
- Korzystaj z bramek płatności.

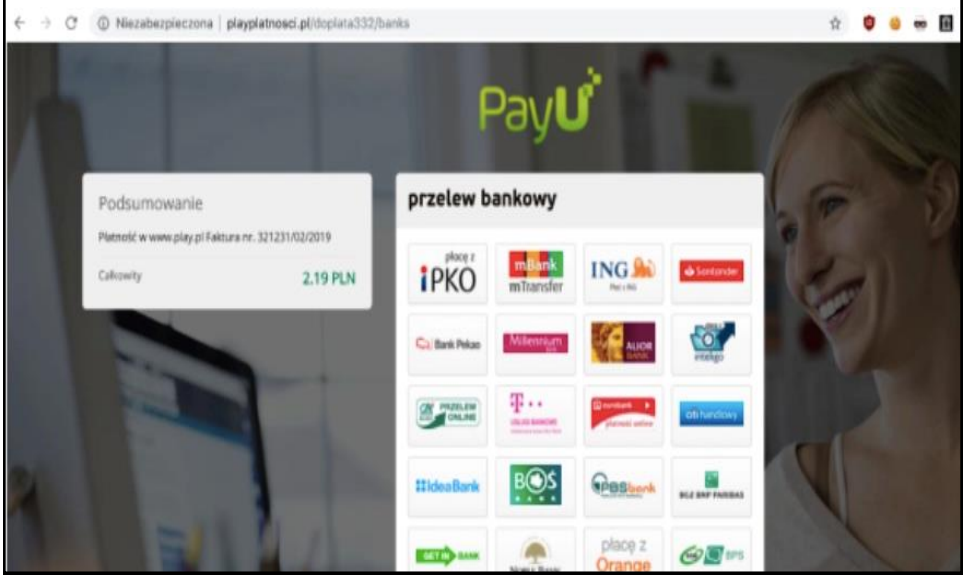
25

## Bezpieczna bramka płatności, czyli…

- Sprawdź:
  - czy jest kłódka, https
  - **DOKŁADNIE** adres bramki

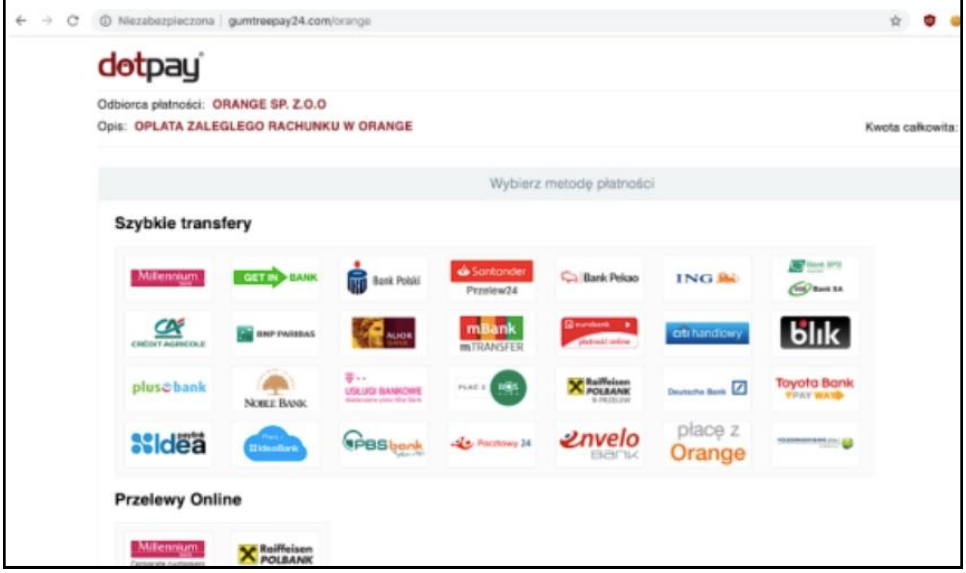
26

## Bezpieczna bramka płatności, czyli…




27

## Bezpieczna bramka płatności, czyli…




28

## Gdy musisz zastrzec kartę…


29

## Policja ostrzega!

Na co warto jeszcze zwrócić uwagę na **ZAKUPACH?**

30

## Przydatne linki

PRZYDATNE INFORMACJE
- ✔ NASK CERT.PL
- ✔ niebezpiecznik.pl

ZGŁOŚ INCYDENT
- ✔ CERT.PL – Zgłoś incydent
- ✔ Zawsze informuj bank, operatora sieci, platformę zakupową o próbie oszustwa

31

## Ekonomiczny Uniwersytet Dziecięcy

**Dziękuję za uwagę!**

**Politechnika Gdańska**
Data: 08 kwietnia 2021r



32