Wybrane problemy cyberbezpieczeństwa na przykładach scenariuszy ataków opartych na COVID-19

Dr inż. Agnieszka Gryszczyńska
Katedra Prawa Informatycznego
WPiA UKSW

Anty-Covid. Informatyka w zwalczaniu Covid-19, 22-23 czerwca 2020 r.
Inicjowanie i integrowanie działań zmierzających do przezwyciężania problemów związanych z Covid-19 metodami informatycznymi.

- Pandemia COVID -19 znacząco wpłynęła na metody pracy, nauki czy realizacji zadań publicznych.
- COVID-19 jest nie tylko poważnym problemem zdrowotnym, ale także niesie ryzyka dla cyberbezpieczeństwa.
- Przestępcy szybko skorzystali z rozprzestrzeniania się wirusa i nadużywają popytu na informacje i zasoby.
- Pandemia COVID – 19 dla cyberprzestępców stała się okazją do zwiększenia skuteczności ataków opartych na socjotechnice.

Jaka jest skala zagrożeń?

- Od 2018 do 2019 podwoiła się ilość incydentów zarejestrowanych przez zespół CERT Polska z 3739 incydentów w 2018 r. do 6 484 incydentów w 2019 r.
- W 2018 roku phishing stanowił 44 % wszystkich incydentów.
- Zgodnie z zapowiedzią raportu CERT Polska za 2019 na 6 484 przeanalizowane incydenty stwierdzono 3 516 przypadków phishingu.

Krajobraz bezpieczeństwa polskiego internetu, Raport roczny z działalności CERT Polska 2018, s. 13, https://www.cert.pl/wp-content/uploads/2019/05/Raport_CP_2018.pdf (dostęp 20.6.2020)

- Indeks zagrożenia w Polsce wg raportu Check Point wynosi 42,7 pkt, co daje Polsce 26 miejsce w Europie i 51. na świecie
- W maju 2020 polskie przedsiębiorstwa były atakowane średnio ponad 300 razy dziennie
- Ogólna ilość cyberataków wzrosła w maju o 16% w związku z ponownym otwieraniem gospodarki.

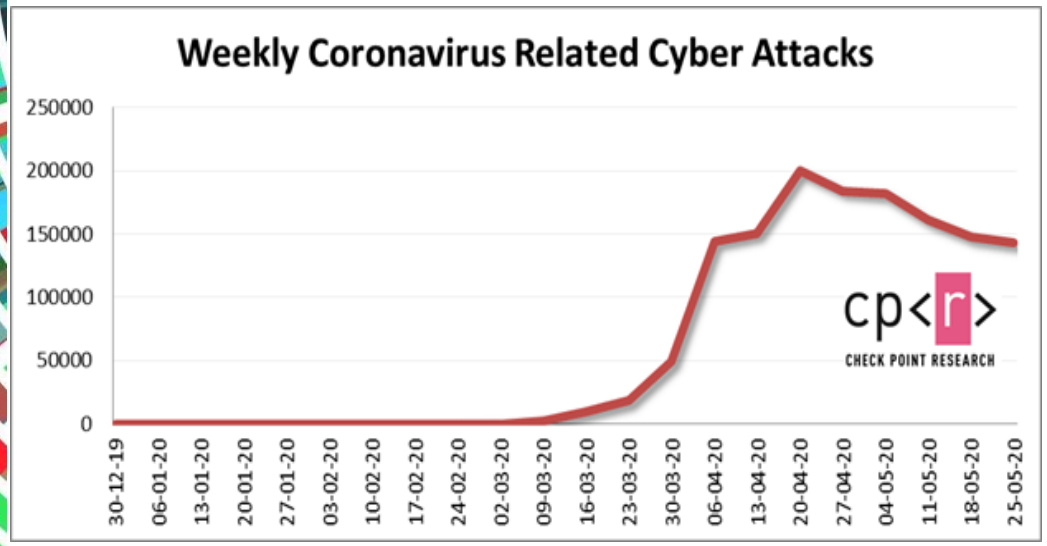
- https://www.rp.pl/CYFROWA-IT/306179901-Polska-cyberniebezpieczna-Druzgocacy-ranking.html (dostęp 20.6.2020)
- https://blog.checkpoint.com/2020/06/04/coronavirus-update-not-the-type-of-cv-youre-looking-for/(dostęp 20.6.2020)

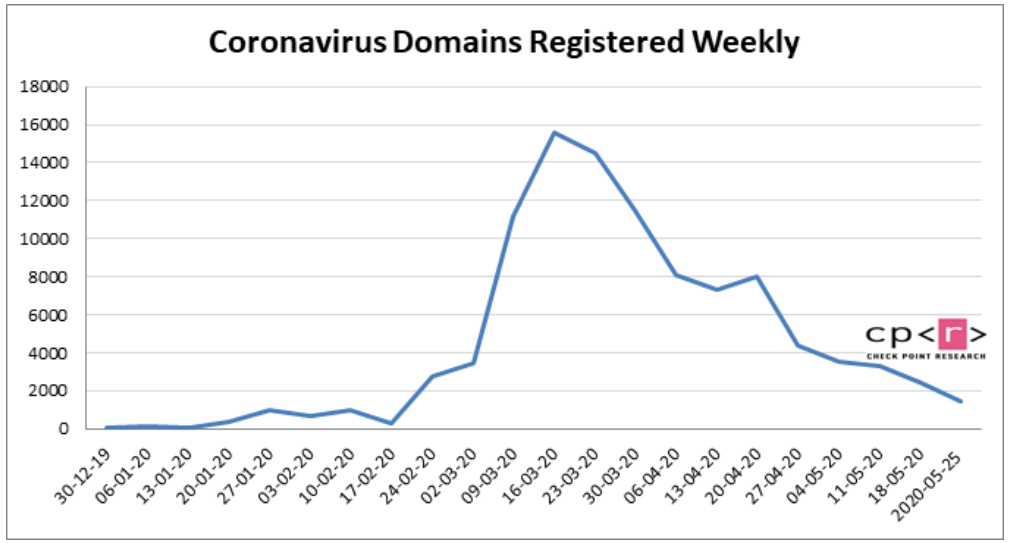
Jaka jest skala ataków związanych z COVID-19?

- W kwietniu Google zaobserwował 18 mln wiadomości phishingowych oraz złośliwego oprogramowania powiązanych z COVID-19 dziennie

https://www.theverge.com/2020/4/16/21223800/google-malware-phishing-covid-19-coronavirus-scams (dostęp 20.6.2020)

Uwagę zwraca również znaczący wzrost rejestracji domen wykorzystujących pandemię do infekowania użytkowników internetu, wyłudzania danych, środków finansowych, dezinformacji





https://blog.checkpoint.com/2020/06/04/coronavirus-update-not-the-type-of-cv-youre-looking-for/ (dostęp 20.6.2020)

Przykładowe incydenty

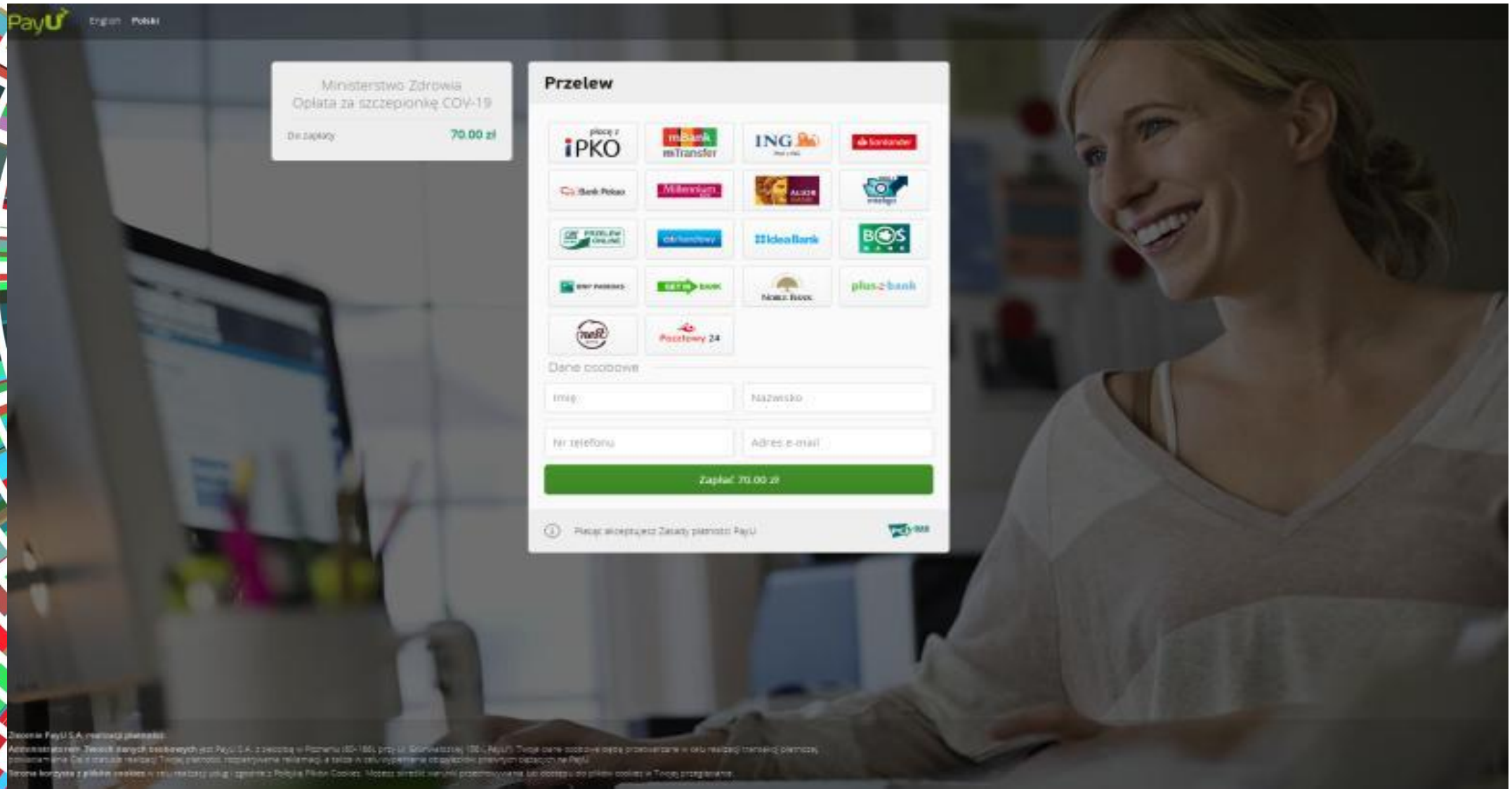
- Infekowanie złośliwym oprogramowaniem (głównie trojanami bankowymi) przy pomocy wiadomości e-mail zawierających złośliwe pliki imitujące CV, zwolnienia lekarskie lub dokumenty związane ze wsparciem finansowym podczas COVID-19
- Tworzenie stron fikcyjnych sklepów internetowych sprzedających środki ochronne
- Tzw. „oszustwa nigeryjskie” z wykorzystaniem w wiadomości e-mail scenariusza związanego ze wsparciem finansowym związanym z COVID-19
- Organizowanie fałszywych zbiórek pieniędzy na cele związane z ochroną zdrowia i wsparciem dla szpitali
- Tworzenie fałszywych stron agentów rozliczeniowych wyłudzających dane do logowania do bankowości elektronicznej
- Tworzenie fałszywych stron wyłudzających dane do logowania to portali społecznościowych
- Tworzenie fałszywych stron podszywających się pod WHO, Zoom, Microsoft, Google w celu wyłudzenia danych
- Infekowanie placówek ochrony zdrowia oprogramowaniem ransomware w celu wyłudzenia okupu (przykład Szpital Uniwersytecki w Brnie)

Przykładowe scenariusze ataków

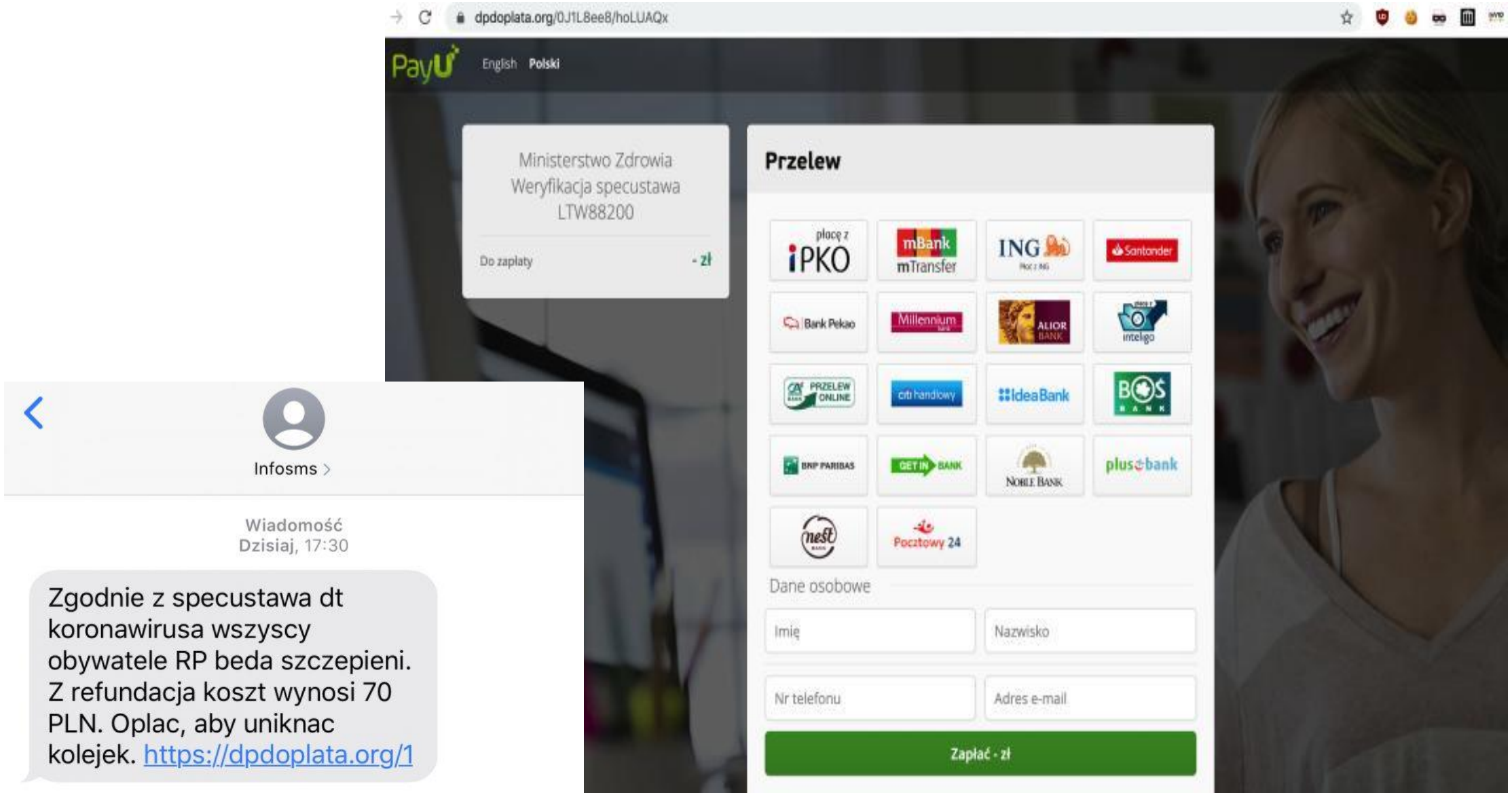
Fałszywe zbiórki:
Adres fałszywej strony:
https://pomoc[.]sie-pomaga[.]net/koronawirus?SS52

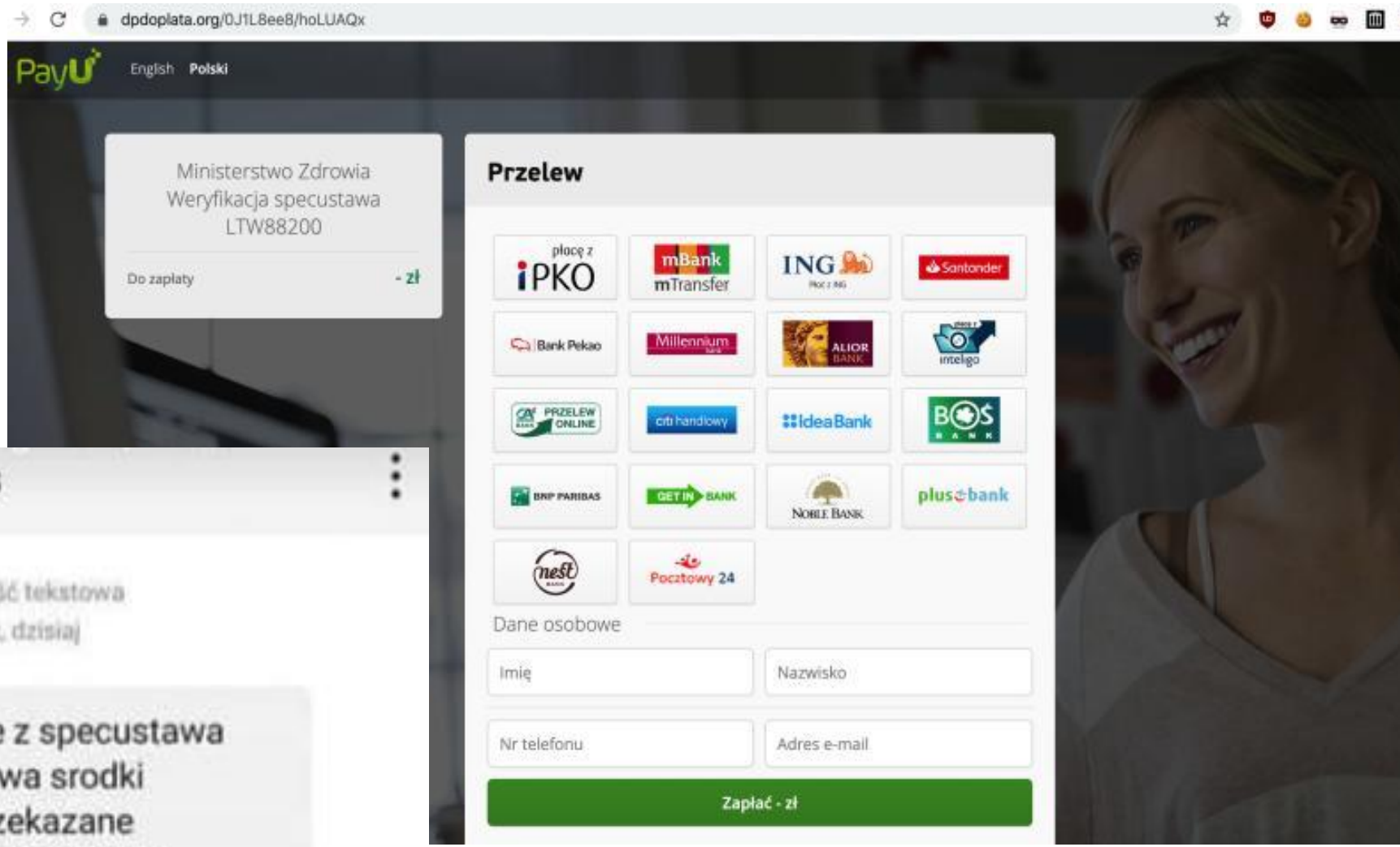
Ataki z wykorzystaniem fałszywych stron agentów rozliczeniowych i banków

Fałszywa strona PAYU (atak aktywy w dniu 13 marca 2020)



Fałszywa strona PAYU!




dpdoplata.org/0J1LBee8/hoLUAQx
PayU
English Polski
Ministerstwo Zdrowia
Weryfikacja specustawa
LTW88200
Do zapłaty - zł
Przelew
płacę z iPKO
mBank mTransfer
ING
Santander
Bank Pekao
Millennium
ALIOR BANK
inteligo
PRZELEW ONLINE
citi handlowy
IdeaBank
BOŚ BANK
BNP PARIBAS
GETIN BANK
NOBLE BANK
plus bank
nest
Pocztowy 24
Dane osobowe
Imię
Nazwisko
Nr telefonu
Adres e-mail
Zapłać - zł


Infosms
Wiadomość tekstowa
piątek, dzisiaj
Informujemy, iz zgodnie z specustawa dt. koronawirusa Panstwa srodki na rachunku zostaja przekazane do rezerw krajowych NBP. Zaloguj sie, aby zatrzymac 1000 PLN.
https://dpdoplata.org/0
23 minuty temu

mzgov.net

Ministerstwo Zdrowia | Serwis Rzeczypospolitej Polskiej

Login | Profil Zaufany

Wsparcie żywieniowe - Koronawirus

Zgodnie z rozporządzeniem Ministerstwa Zdrowia dla każdego obywatela przysługuje wsparcie żywieniowe w związku z epidemią Koronawirusa.

Na jedną osobę przysługuje:

- 20 l wody
- 3,5 kg zbóż, produktów zbożowych, chleba, ziemniaków, makaronu i ryżu.
- 2,5 kg owoców w puszkach lub słoikach i orzechów
- 4 kg suchych roślin strączkowych i warzyw w puszkach lub słoikach
- 2,6 kg mleka i produktów mlecznych
- 1,5 kg mięsa, ryb i jajek, ewentualnie jajek w proszku (świeże jajka mają trwałość kilka dni, proszek kilka lat)
- 0,4 kg tłuszczu i olejów

Ministerstwo Zdrowia | Serwis Rzeczypospolitej Polskiej

Login | Profil Zaufany

Wsparcie żywieniowe - Koronawirus

Zgodnie z rozporządzeniem Ministerstwa Zdrowia dla każdego obywatela przysługuje wsparcie żywieniowe w związku z epidemią Koronawirusa.

Na jedną osobę przysługuje:

- 20 l wody
- 3,5 kg zbóż, produktów zbożowych, chleba, ziemniaków, makaronu i ryżu.
- 2,5 kg owoców w puszkach lub słoikach i orzechów
- 4 kg suchych roślin strączkowych i warzyw w puszkach lub słoikach
- 2,6 kg mleka i produktów mlecznych
- 1,5 kg mięsa, ryb i jajek, ewentualnie jajek w proszku (świeże jajka mają trwałość kilka dni, proszek kilka lat)
- 0,4 kg tłuszczu i olejów

W celu otrzymania świadczenia prosimy o potwierdzenie danych osobowych poprzez profil zaufany.

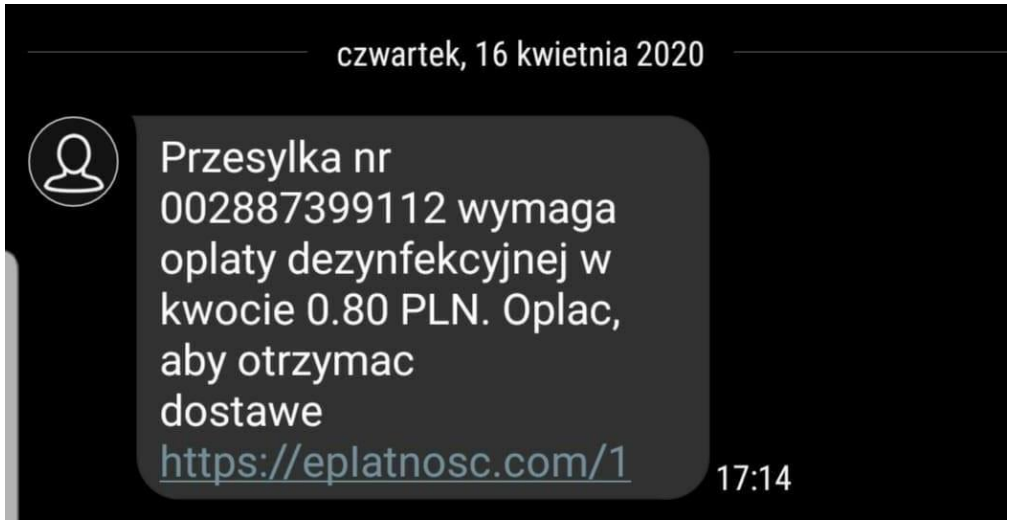
Zaloguj się przy pomocy banku

Bank Polski · mBank mTRANSFER · Santander Przelew24 · GETIN BANK · Millennium · ING · BNP PARIBAS · CA CREDIT AGRICOLE

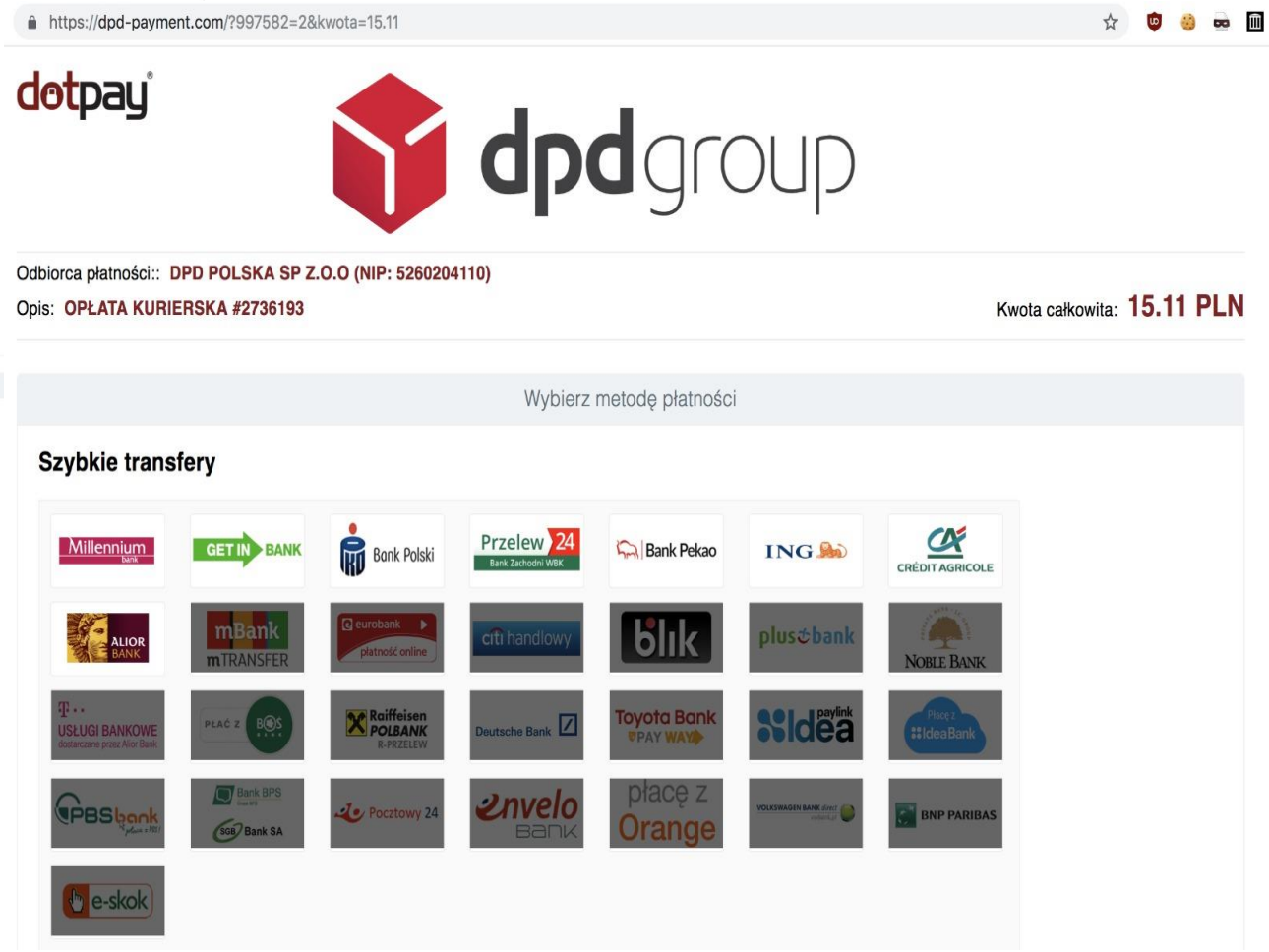
Przykładowe SMSy z linkami

RP informuje o obowiazkowych szczepieniach na koronawirusa. Szczepienia zaczna sie 20.03.2020. Koszt 10 zł, oplac aby uniknac kolejek https://nfz582.com/1259

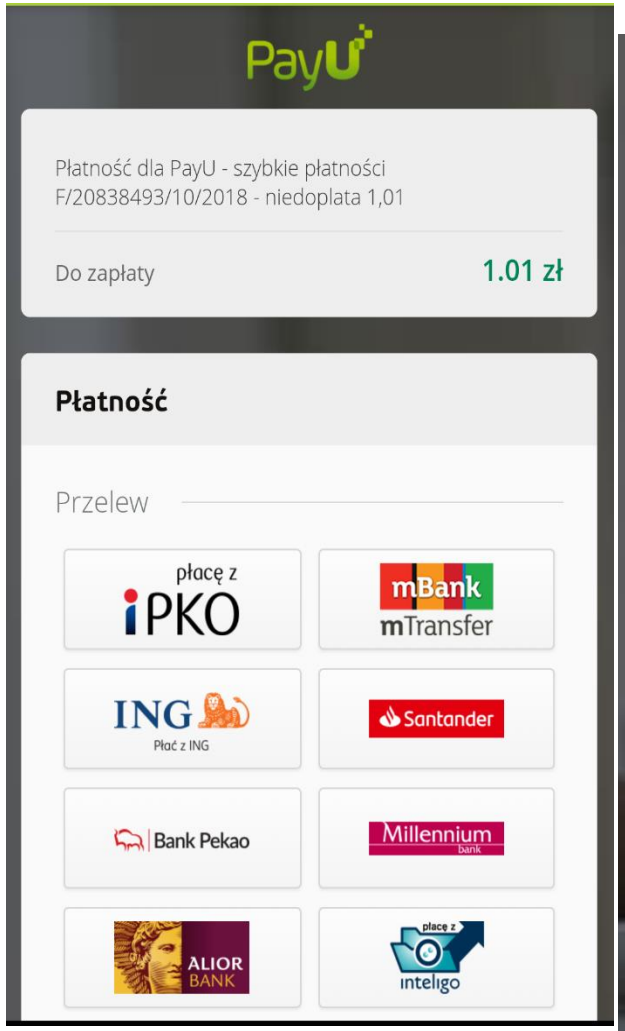
Paczka nr 00772990012 wymaga dezynfekcji. Oplata dodatkowa wynosi 1.70 PLN. Oplac, aby otrzymac przesylke. https://paczkadpd.com/1

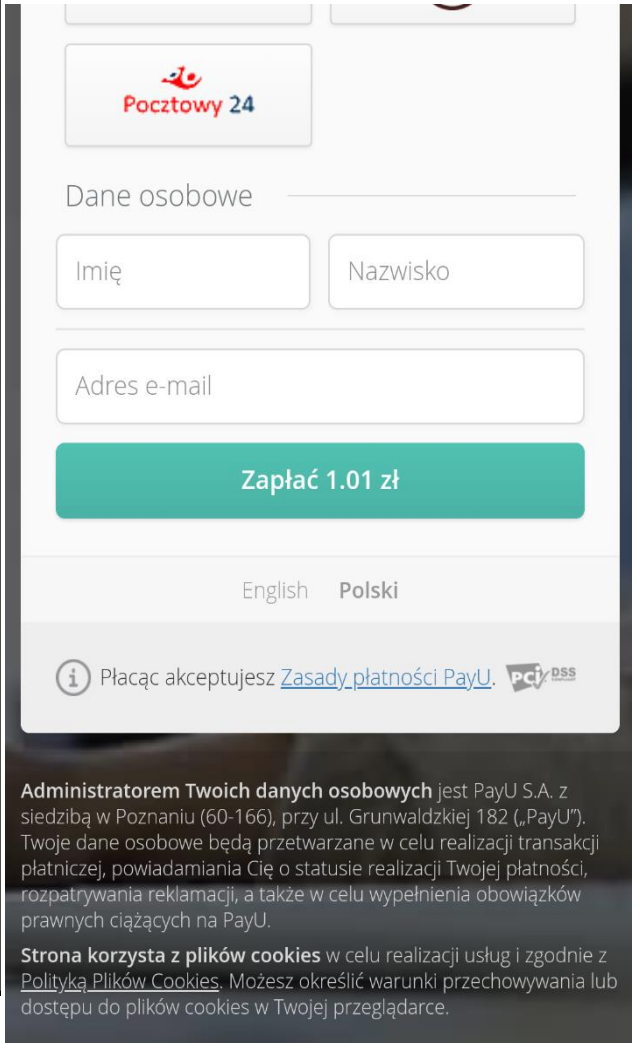


Przykładowe fałszywe strony pośredników płatności

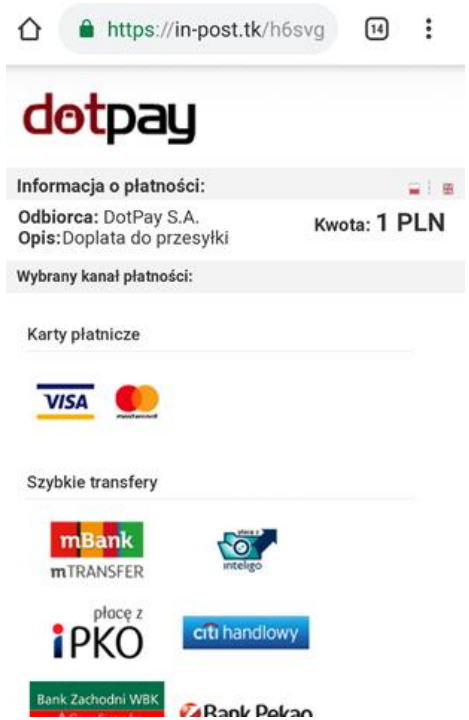


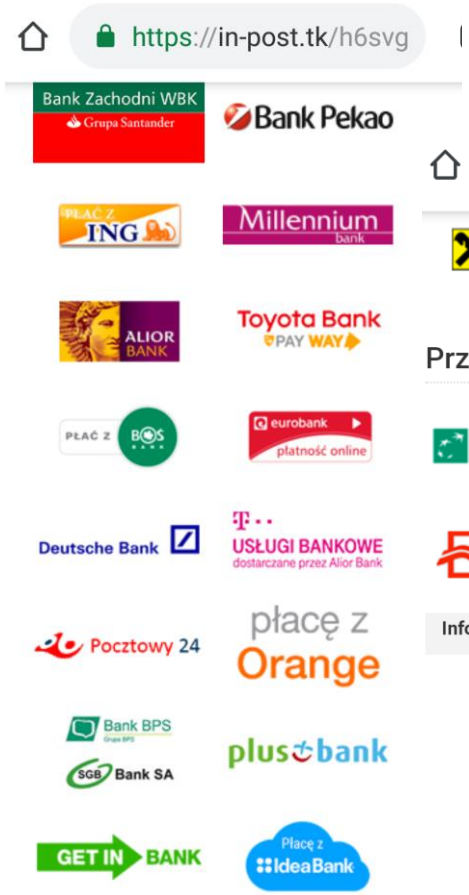
Przykładowe fałszywe strony pośredników płatności

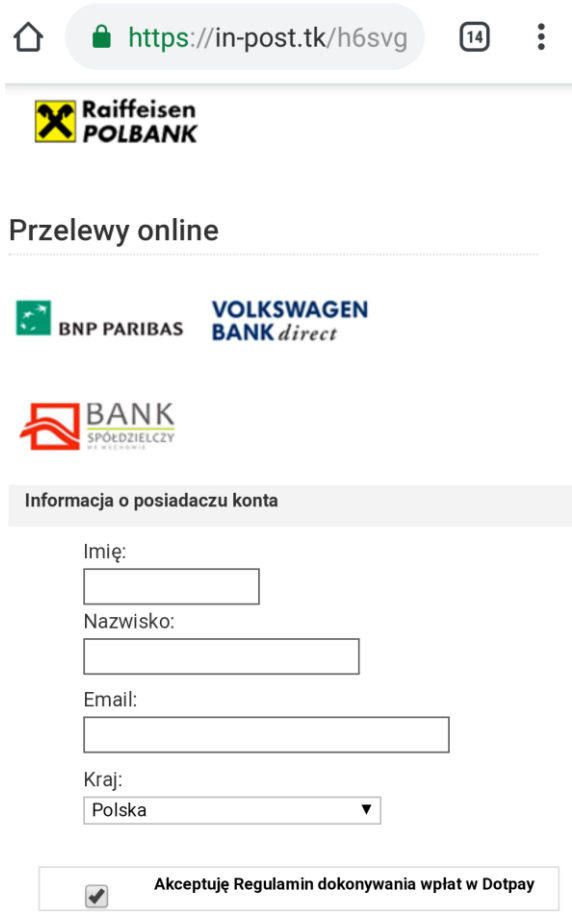


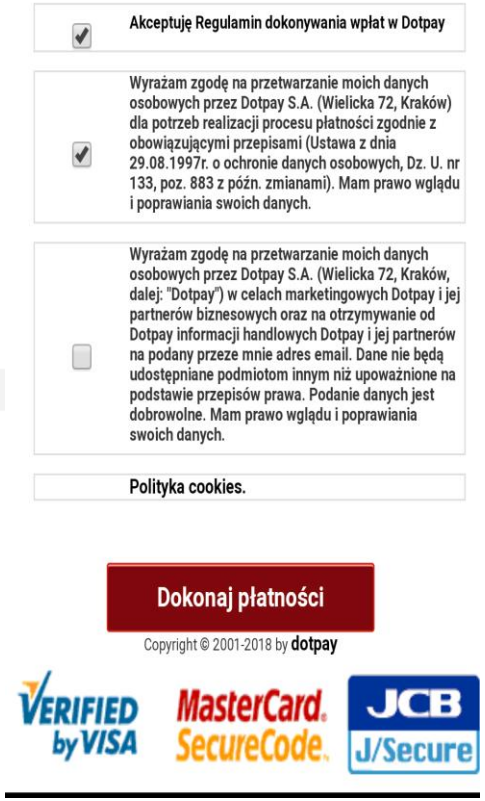


Przykładowe fałszywe strony pośredników płatności

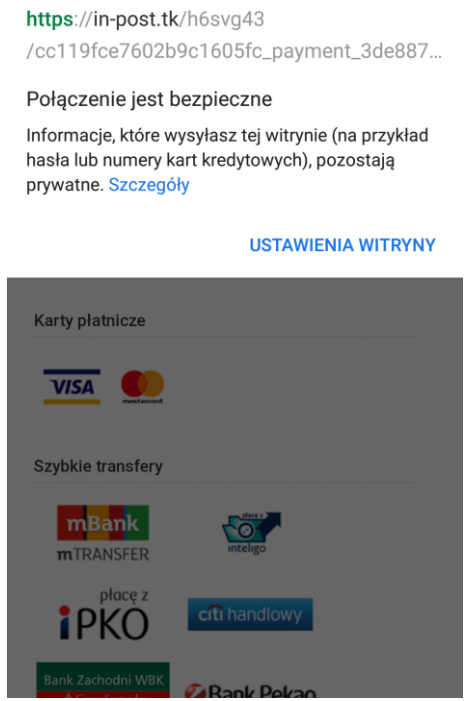


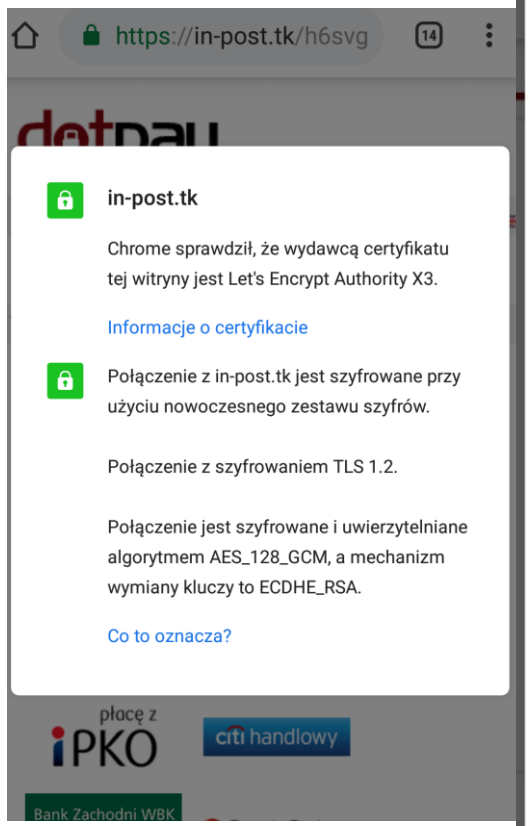


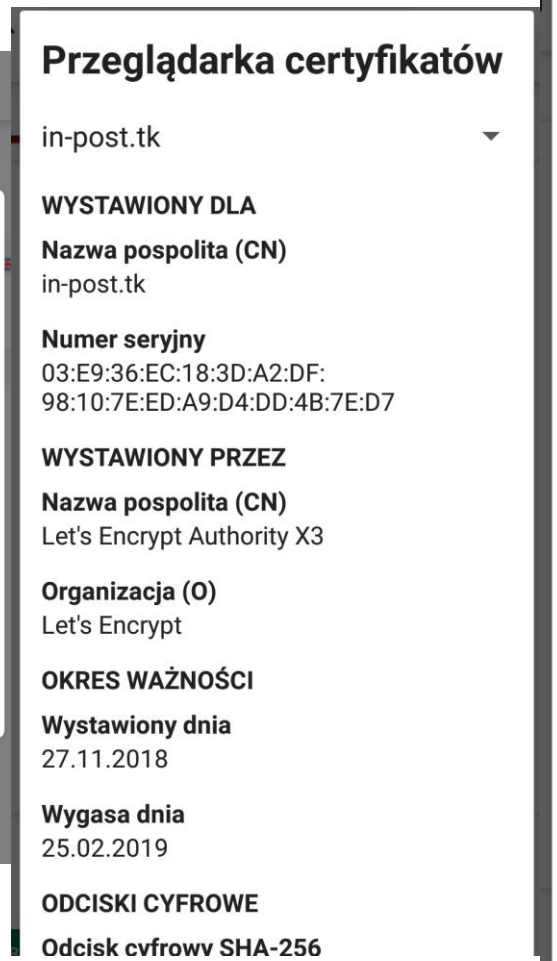


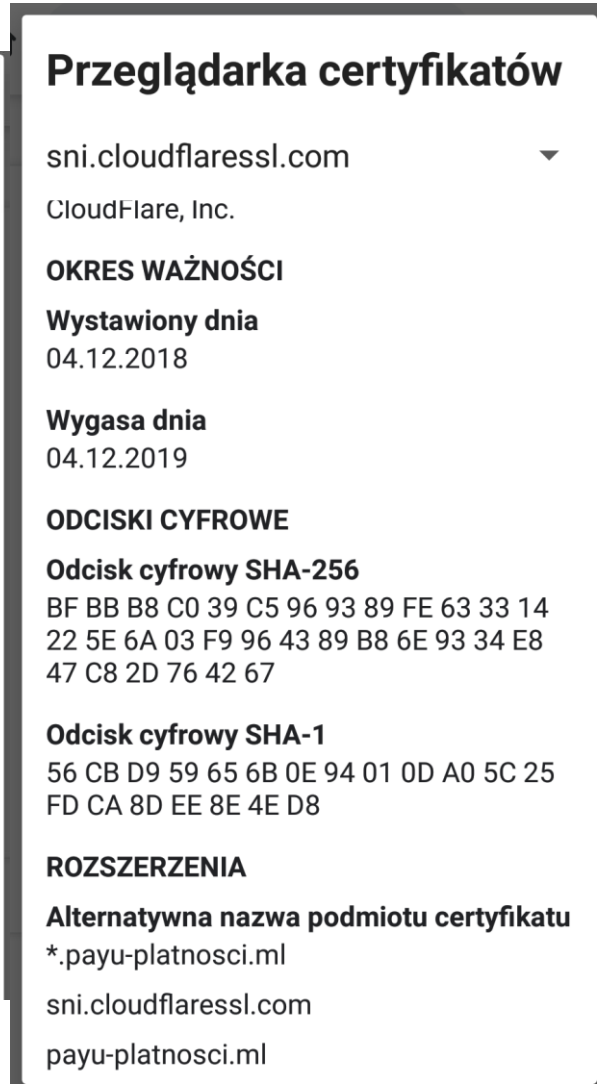


Przykładowe fałszywe strony pośredników płatności

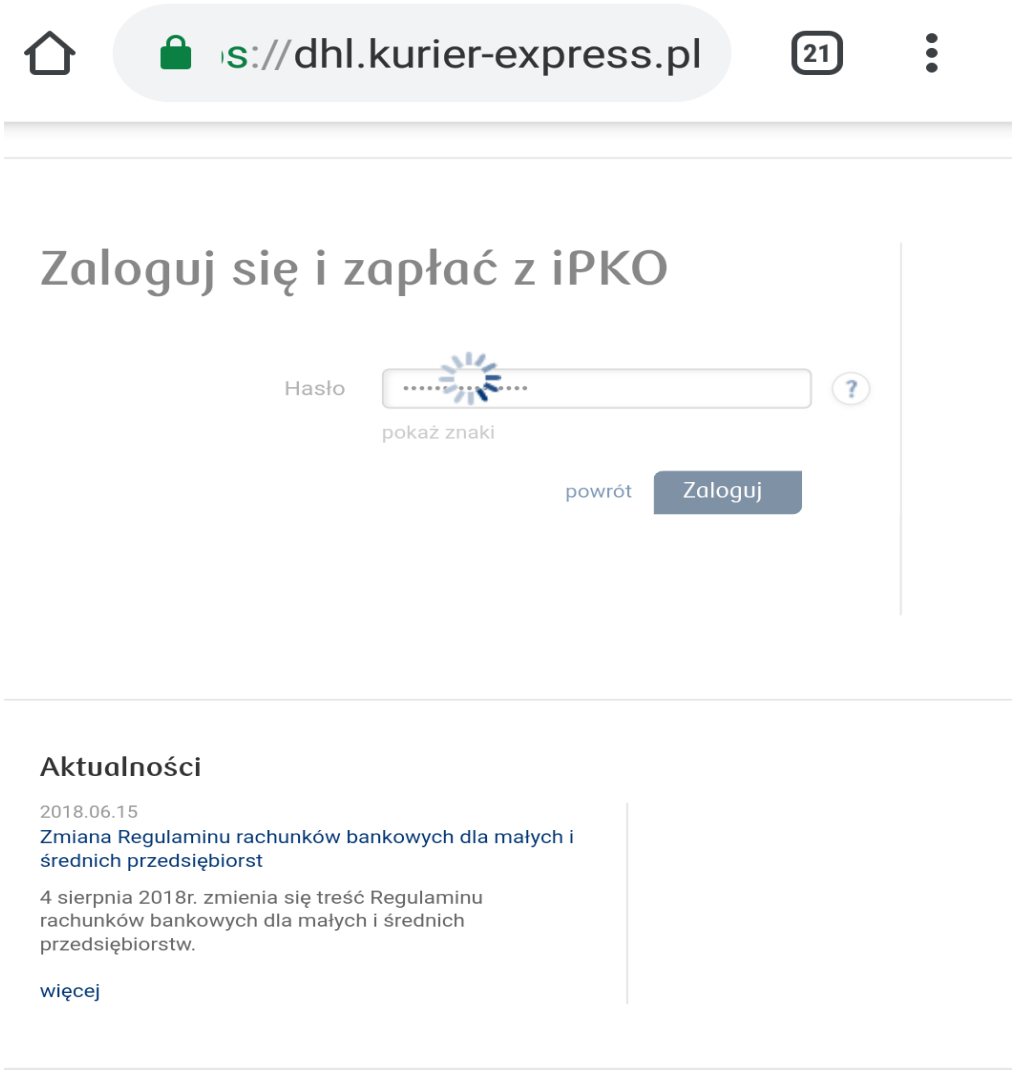


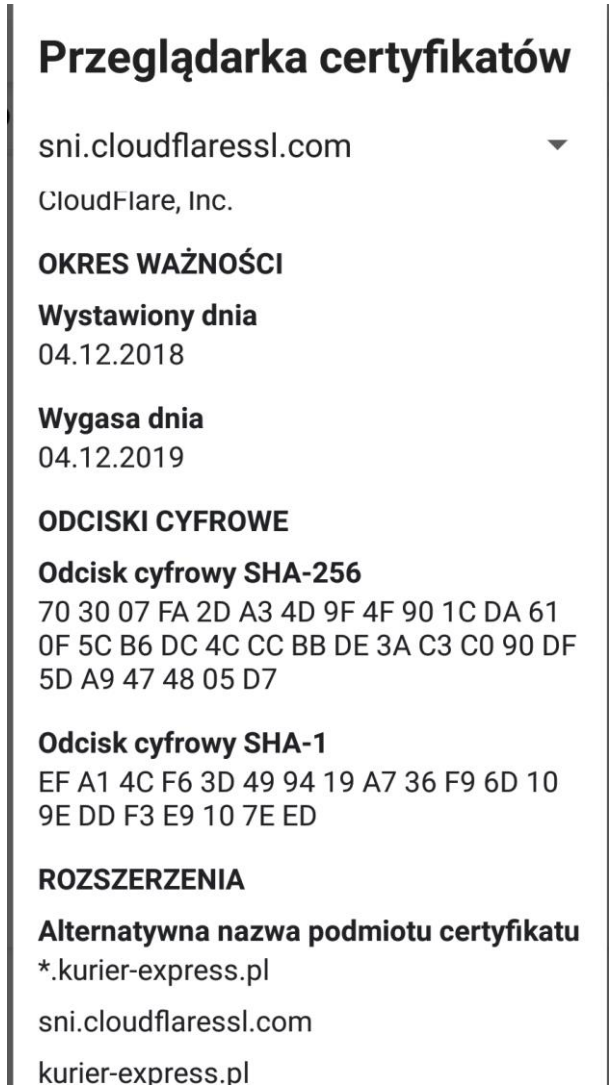


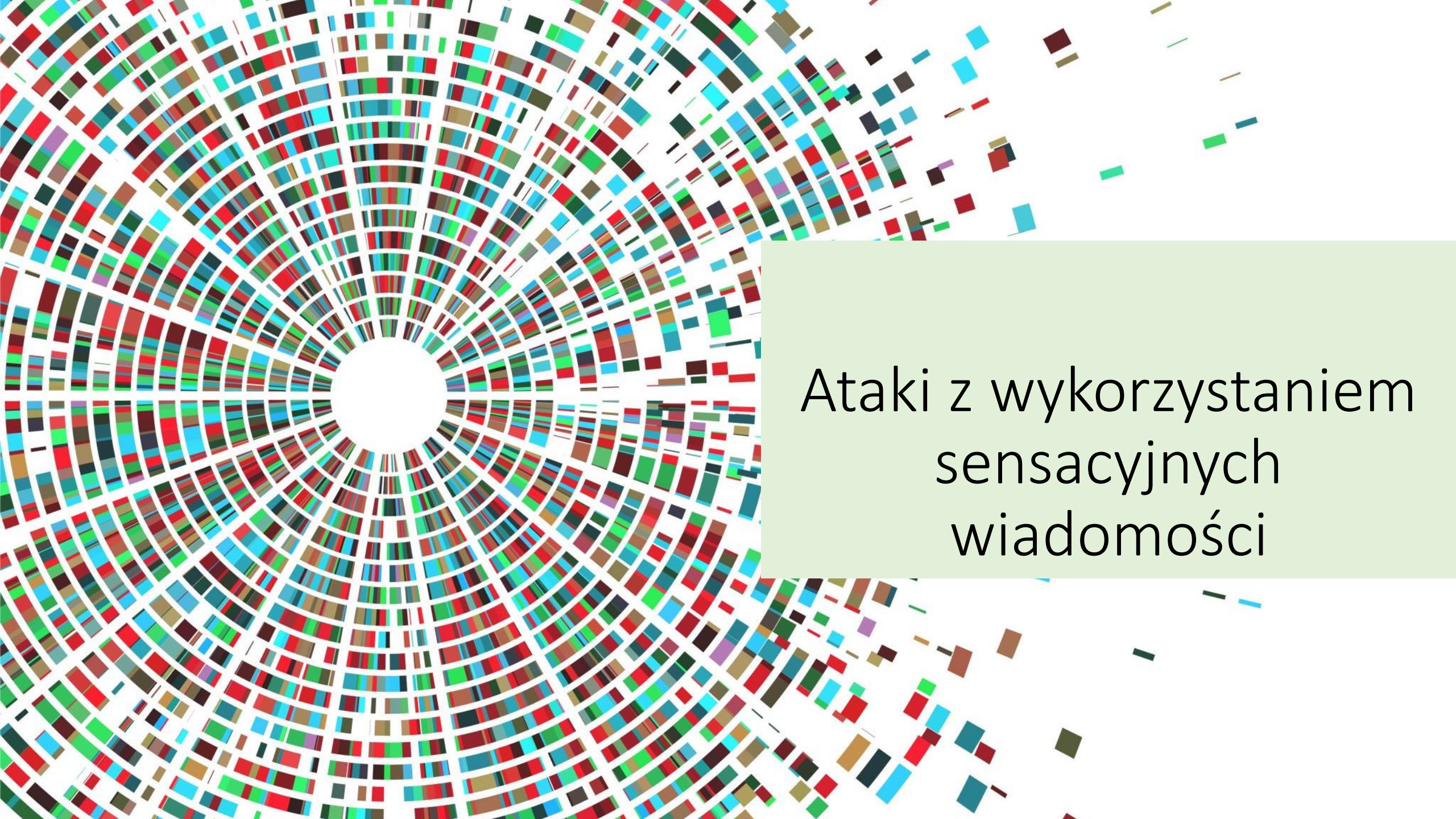




Przykładowe fałszywe strony banków

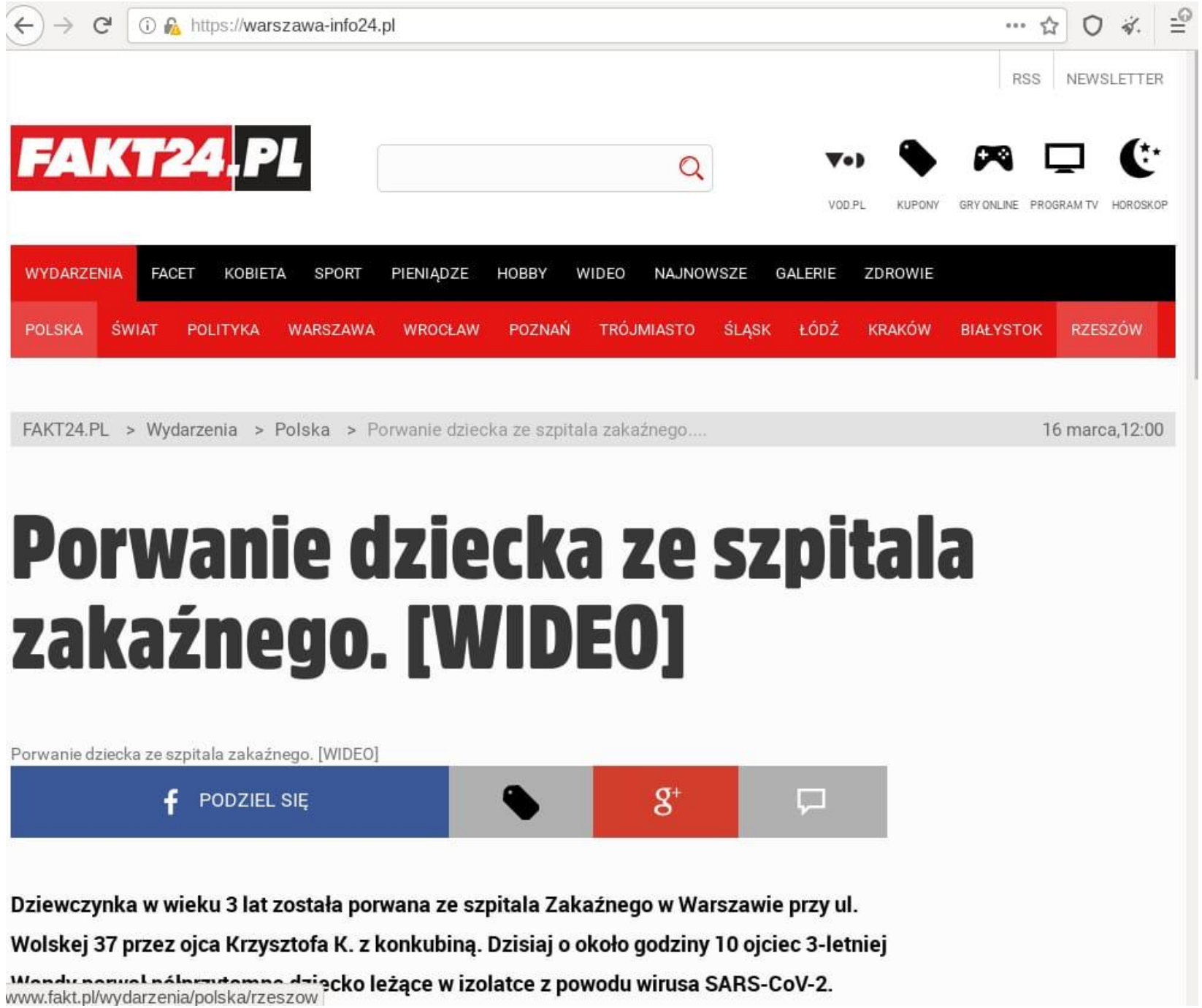




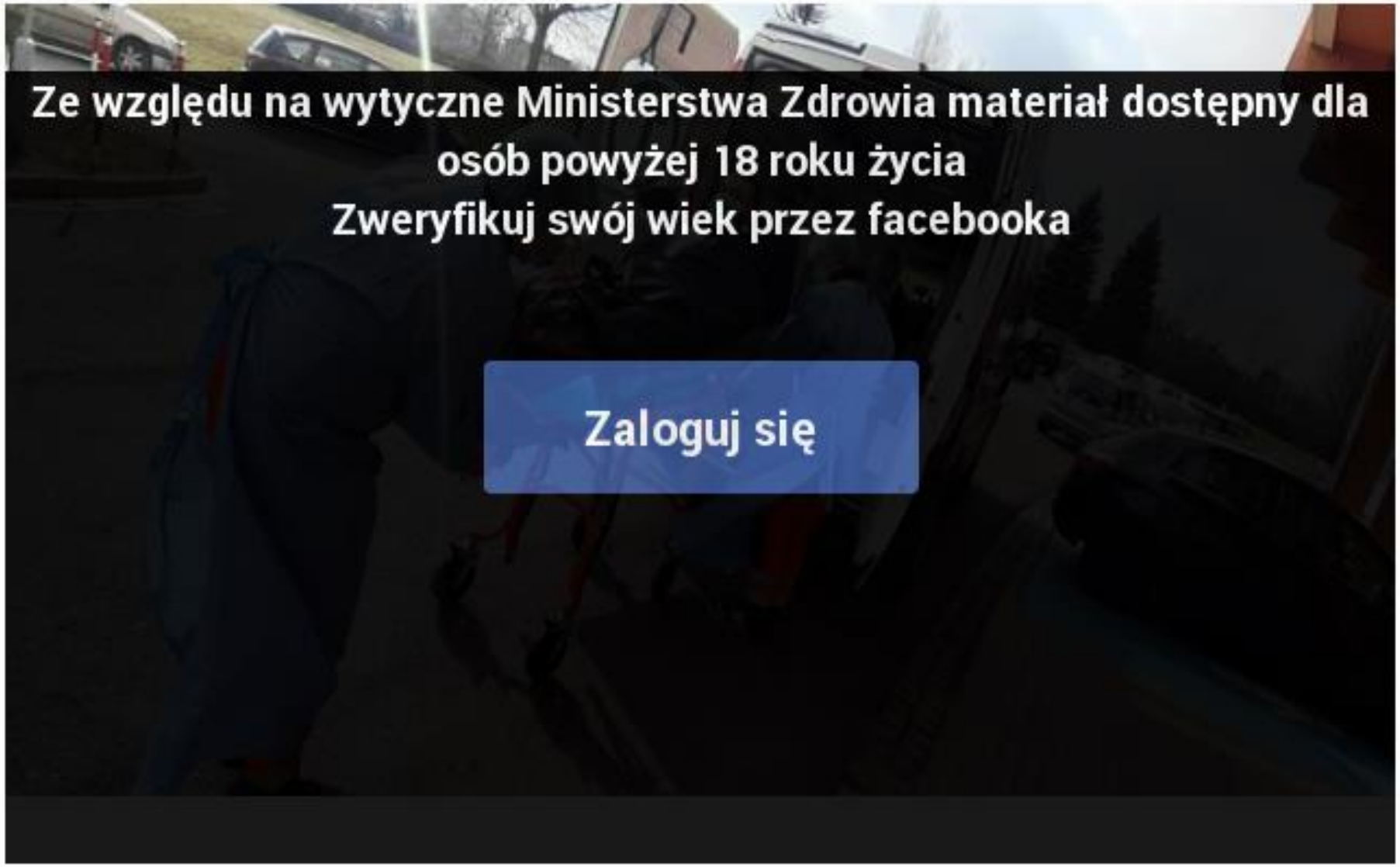


Ataki z wykorzystaniem sensacyjnych wiadomości

Przykładowe phishingowe nazwy domenowe: koronawirusnews[.]com[.]pl koronawirusnews[.]net[.]pl ikoronawirusnews[.]pl e-koronawirusnews[.]pl


https://warszawa-info24.pl
RSS
NEWSLETTER
FAKT24.PL
VOD.PL
KUPONY
GRY ONLINE
PROGRAM TV
HOROSKOP
WYDARZENIA
FACET
KOBIETA
SPORT
PIENIĄDZE
HOBBY
WIDEO
NAJNOWSZE
GALERIE
ZDROWIE
POLSKA
ŚWIAT
POLITYKA
WARSZAWA
WROCŁAW
POZNAŃ
TRÓJMIASTO
ŚLĄSK
ŁÓDŹ
KRAKÓW
BIAŁYSTOK
RZESZÓW
FAKT24.PL > Wydarzenia > Polska > Porwanie dziecka ze szpitala zakaźnego.... 16 marca,12:00
Porwanie dziecka ze szpitala zakaźnego. [WIDEO]
Porwanie dziecka ze szpitala zakaźnego. [WIDEO]
PODZIEL SIĘ
Dziewczynka w wieku 3 lat została porwana ze szpitala Zakaźnego w Warszawie przy ul. Wolskej 37 przez ojca Krzysztofa K. z konkubiną. Dzisiaj o około godziny 10 ojciec 3-letniej
ecko leżące w izolatce z powodu wirusa SARS-CoV-2.
www.fakt.pl/wydarzenia/polska/rzeszow

WYPOWIEDŹ DOKTORA Z JEDNEGO Z WARSZAWSKICH SZPITALI NA TEMAT NAMNAŻAJĄCEJ SIĘ LICZBY ZARAŻONYCH W POLSCE.



Co ułatwia sprawcom ataki i utrudnia ustalenie ich tożsamości?

- Możliwość anonimowego korzystanie z usług świadczonych drogą elektroniczną
- Wykorzystanie tożsamości innych osób (z uwagi na brak weryfikacji tożsamości przy korzystaniu z e-usług)
- Ograniczenie zakresu danych publikowanych w bazach WHOIS – utrudniające m.in. atrybucje ataku oraz prowadzenie postępowań karnych
- Obrót zarejestrowanymi na dane innych osób kartami SIM
- Brak przepisów regulujących gromadzenie logów, ich struktury oraz ustalenia okresu ich przechowywania
- Brak retencji danych „internetowych” – w szczególności w zakresie logów oraz danych abonentów usług
- Stosowanie NAT w sieciach (przy jednoczesnym niegromadzeniu przez większość podmiotów -w tym banki numerów portów)
- Łatwość pozyskania rachunków bankowych do prania pieniędzy pochodzących z przestępstwa
- Dostępność anonimowych usług płatniczych (płatności w kryptowalucie, płatności przy pomocy SMS Premium)
- Brak ogólnych regulacji dotyczących blokowania domen podszywających się pod inne podmioty lub służących do popełnienia przestępstwa
- Wadliwa regulacja karnoprawnych znamion kradzieży tożsamości
- Bardzo niskie zagrożenie karne przestępstwa „hackingu”

Czy i jak zablokować dostęp do stron internetowych wyłudzających dane?

POROZUMIENIE z dnia 23 marca 2020 o współpracy w zakresie ochrony użytkowników internetu przed stronami wyłudzającymi dane, w tym dane osobowe oraz doprowadzających użytkowników internetu do niekorzystnego rozporządzenia ich środkami finansowymi w okresie stanów nadzwyczajnych, stanu epidemii lub stanu zagrożenia epidemicznego w Rzeczypospolitej Polskiej

pomiędzy
Orange Polska S.A.
Polkomtel Sp. z o.o.
P4 Sp. z o.o.
T-Mobile Polska S.A.
a
Ministrem Cyfryzacji oraz Prezesem Urzędu Komunikacji Elektronicznej (zwanymi dalej „Stroną rządową")

a także

Naukową i Akademicką Siecią Komputerową – Państwowym Instytutem Badawczym

- W okresach stanów nadzwyczajnych, stanu epidemii lub stanu zagrożenia epidemicznego w Rzeczypospolitej Polskiej, NASK-PIB będzie opracowywał, prowadził i utrzymywał jawną listę ostrzeżeń dotyczących domen internetowych, które służą do wyłudzeń danych i środków finansowych użytkowników internetu (dalej „Lista Ostrzeżeń"). Lista Ostrzeżeń jest prowadzona w formie publikacji na stronie internetowej www.cert.pl/ostrzezenia_phishing.
- Na Listę Ostrzeżeń wpisywane są domeny internetowe, które za podstawowy cel swojego działania mają wprowadzenie w błąd użytkowników internetu i w ten sposób doprowadzenie ich do niekorzystnego rozporządzenia środkami finansowymi albo do wyłudzenia ich danych osobowych
- Każdy może zgłosić domenę internetową służącą do wyłudzeń danych i środków finansowych do NASK-PIB. Zgłoszenia powinny zawierać uzasadnienie dotyczące każdej zgłoszonej domeny
- Zgłoszeń domen internetowych, o których mowa w niniejszym Porozumieniu, dokonuje się na stronie https://incydent.cert.pl/phishing lub emailem na adres: cert@cert.pl.
- Każde zgłoszenie jest weryfikowane przez NASK-PIB. NASK-PIB dołoży najwyższej staranności, aby weryfikacja zgłoszenia trwała najkrócej jak to możliwe w celu zapewniania realizacji celów niniejszego Porozumienia. Po dokonaniu weryfikacji NASK-PIB niezwłocznie wpisuje na Listę Ostrzeżeń domeny, które pozytywnie przeszły weryfikację

Techniczna implementacja blokowania na podstawie porozumienia

Operatorzy oświadczają, że od dnia udostępnienia Listy Ostrzeżeń przez NASK-PIB dołożą należytej staranności, by:

- a) uniemożliwić dostęp do stron internetowych wykorzystujących nazwy domen internetowych opublikowanych na Liście Ostrzeżeń **poprzez ich usunięcie ze swoich systemów teleinformatycznych służących do zamiany nazw domen internetowych na adresy IP,** w najkrótszym możliwym czasie od otrzymania informacji o wpisaniu nowej domeny internetowej na Listę Ostrzeżeń,

- b) **przekierować połączenia odwołujące się do nazw domen internetowych opublikowanych na Liście Ostrzeżeń do strony internetowej prowadzonej przez NASK-PIB zawierającej komunikat** skierowany do użytkowników internetu lub do innej strony o analogicznym komunikacie z wykorzystaniem narzędzi dostępnych po stronie Operatorów, obejmujący w szczególności informacje o lokalizacji Listy Ostrzeżeń, wpisaniu szukanej nazwy domeny internetowej na Listę Ostrzeżeń oraz o możliwej próbie wyłudzenia danych lub środków finansowych. W przypadku przekierowania do strony Operatora, Operator przekazuje NASK dane statystyczne dotyczące liczby wywołań danej domeny od momentu jej zablokowania

W dniu 20.6.2020 na liście znajdowało się **2 357** nazw domenowych https://hole.cert.pl/domains/domains.txt

Wybrane statystyki Listy Ostrzeżeń:

- Dla scenariusza, w którym sprawcy tworzą strony podszywające się pod agentów rozliczeniowych i banki, rejestrują nazwy domenowe podszywające się pod pocztę, podmioty świadczące usługi transportowe, rozliczeniowe i banki, na Liście Ostrzeżeń znajdują się m.in. nazwy domenowe zawierające następujące ciągi znaków:
  - „poczta” (148)
  - „pay” (113)
  - „kurier” (85)
  - „dotpay” (75)
  - „paczka” (63)
  - „allegro” (43)
  - „pocztex” (35)
  - „dhl” (28)
  - „inpost” (28)
  - „platnosc” (20)
  - „payu” (19)
  - „bank” (18)
  - „dpd” (18)
  - „paczki” (13)
  - „dostawa” (13)
  - „ssl” (9)
- Dla scenariusza, w którym sprawcy tworzą strony podszywające się pod portale informacyjne i wyłudzają dane do logowania do portali społecznościowych (zwykle kolejnym etapem jest podszywanie się pod osoby, których dane do logowania pozyskano i wysłanie próśb o pożyczenie pieniędzy poprzez wysłanie kodu BLIK), rejestrowane są głównie nazwy domenowe zawierające następujące ciągi znaków”
  - „fakt” (261)
  - „porwan” (203)
  - „gwałt” (156)
  - „poszukiwan” (60)
  - „news” (59)
  - „dziennik” (40)
  - „korona” (10)

Postulaty *de lege ferenda*

- Celowe jest wprowadzenie obowiązków związanych z przechowywaniem logów dostępowych oraz danych abonentów usług świadczonych drogą elektroniczną przez okres 12 miesięcy (retencja danych).
- Dla podniesienia poziomu bezpieczeństwa i przeciwdziałania zjawisku kradzieży tożsamości celowe jest wprowadzenie obowiązków dotyczących lepszej weryfikacji tożsamości podmiotów korzystających z usług podmiotów świadczących usługi drogą elektroniczną.
- Z uwagi na to, że w części z omówionych powyżej ataków wykorzystano nazwy domenowe z domeny *.pl lub domeny gdzie rejestratorami (pośrednikami) są podmioty mające siedzibę na terytorium Polski należy dokonać zmian w procesie pośrednictwa w rejestracji domen i nałożyć na rejestratorów obowiązki związane z weryfikacją tożsamości podmiotów rejestrujących domeny (abonentów).
- Jawny rejestr domeny .pl powinien zawierać dane kontaktowe do abonenta domeny (co najmniej adres e-mail). Aktualnie w bazie WHOIS nie są publikowane dane abonentów będących osobami fizycznymi. Dla porównania należy wskazać, że dla domeny *.eu baza WHOIS zawiera dane w postaci adresu mailowego abonenta.
- Celowe jest wprowadzenie w sytuacji nabycia karty przedpłaconej (SIM) od innego podmiotu obowiązku ponownej rejestracji takiej karty pod rygorem dezaktywacji usługi. Aktualna regulacja w zestawieniu z praktyką pokazuje, że cel wprowadzenia rejestracji abonentów usług przedpłaconych ustawą o działaniach antyterrorystycznych nie został osiągnięty, a zarejestrowane na dane innych osób karty SIM można kupić na powszechnie dostępnych portalach ogłoszeniowych oraz na forach w sieci TOR.
- Celowe jest dalsze prowadzenie Listy Ostrzeżeń, należy jednak jej dalsze prowadzenie oprzeć o przepisy prawa powszechnie obowiązującego i wprowadzić procedurę odwoławczą.

Postulaty *de lege ferenda*

- W związku z narastającym negatywnym zjawiskiem kradzieży tożsamości i wykorzystywaniem tożsamości innych osób przez cyberprzestępców celowe jest rozszerzenie odpowiedzialności karnej za czyn z art. 190 a § 2 KK.
- Aktualnie z uwagi na wąsko określony w art. 190a § 2 KK cel działania sprawcy, poza zakresem penalizacji pozostaje sytuacja, w której sprawca działa w celu ukrycia własnej tożsamości lub wyrządzenia szkody innej osobie niż ta, której danymi się posługuje.
- *De lege ferenda* można postulować zmianę art. 190a § 2 KK poprzez użycie zamiast wyrażenia "w celu" sformułowania "w zamiarze". Analiza *sposobów działania* sprawców wskazuje również na zasadność odstąpienia od zasady tożsamości podmiotu, pod który sprawcy się podszywają i któremu chcą wyrządzić szkodę.

- Mając na względzie skalę oraz skutki ataków niezbędne jest również podniesienie górnej granicy odpowiedzialności karnej za czyn z art. 267 § 1 kk. Aktualne zagrożenie karne wynosi do 2 lat pozbawienia wolności.

Dziękuję za uwagę!

Kontakt:
a.gryszczynska@uksw.edu.pl