NoSuchMeetup

28.10.2019

Ewolucja phishingu i socjotechniki oraz ich wpływ na sektor bankowy

Wiktor Szymański

kontakt@wiktorszymanski.pl

@wikszymans

Who am I?

Wiktor Szymański

DBE @ Alior Bank

kontakt@wiktorszymanski.pl

@wikszymans

@bezpiecznyblog

Bezpieczny.blog

Long time ago in a galaxy far, far away…

15 years

[redacted] ago [redacted]

- **Tylko 9mln obywateli Polski korzystało z internetu**
- **Nie było Iphone’a i Android’a**
- **Nie było w Polsce bankowych aplikacji mobilnych**
- **Około 3,5 mln użytkowników bankowości internetowej**
- **Nie było Alior Banku**
- **Był phishing…**

Nigerian prince scams

Hello Dear Respected One, Odebrane ×

Miss.Zalanda Mubarak <miszal1414@gmail.com> śr., 21 sie, 13:47

do Miss.Zalanda

Dear Respected One,

Nice To Meet You, I write briefly to ask for your partnership to assist me in the transfer and investment of my inheritance funds (USD 9.5M) Nine Million Five Hundred Thousand U.S Dollars from my late father who died mysteriously.

Am Miss.Zalanda Mubarak, I am 19 years old, I am the only child of my late parents Mr.and Mrs.Alhaji Bilal Mubarak. I got your contact email from international domain database and I decided to contact you for this offer, That is based on trust and your outstanding,

Please reply me back only if you are interested to asist me for more details.

Your urgent response will be appreciated.

Talk to you the more sincerely.

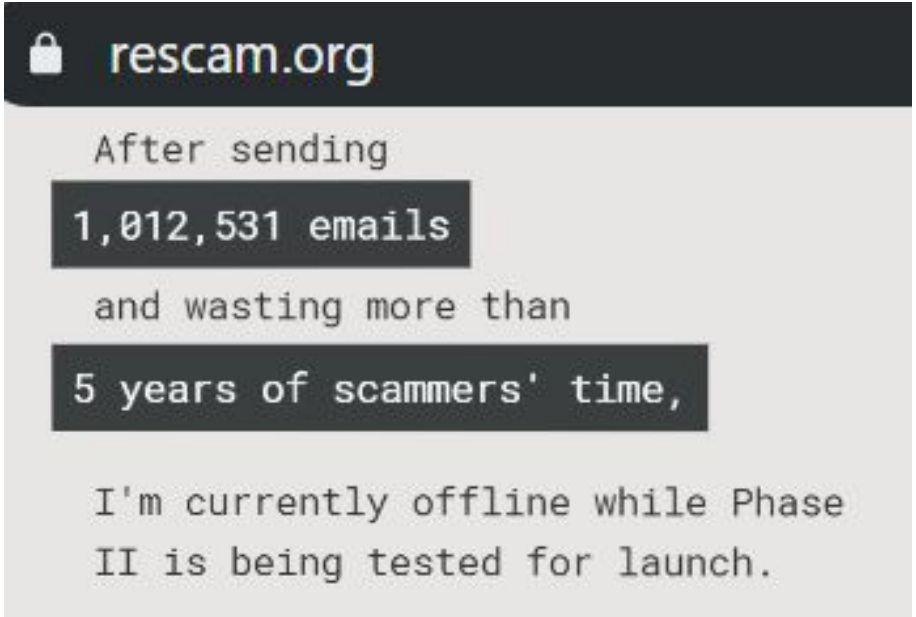
Regards Mis.Zalanda Mubarak

This is what happens when you reply to spam email | James Veitch

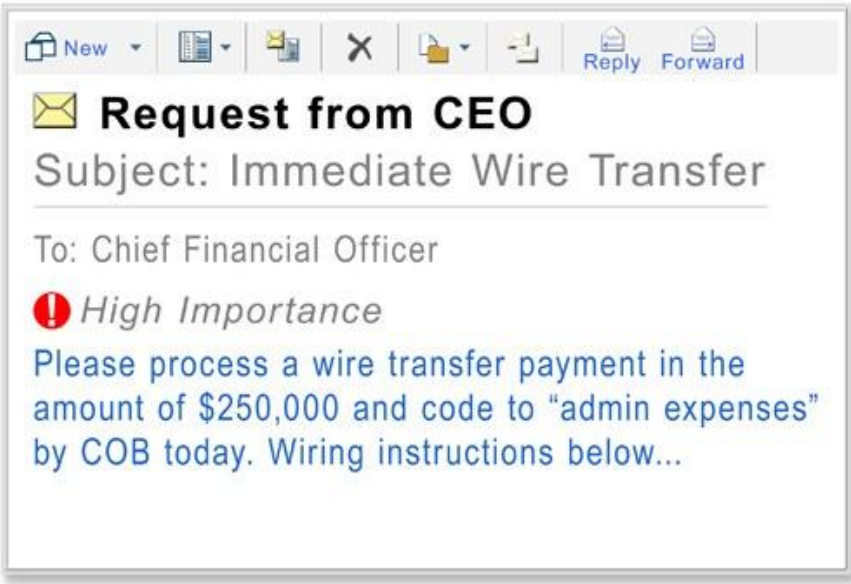
TED ✓ 43 mln wyświetleń • 3 lata temu

Suspicious emails: unclaimed insurance bonds, diamond-encrusted safe deposit boxes, close friends marooned in a foreign ...

napisy



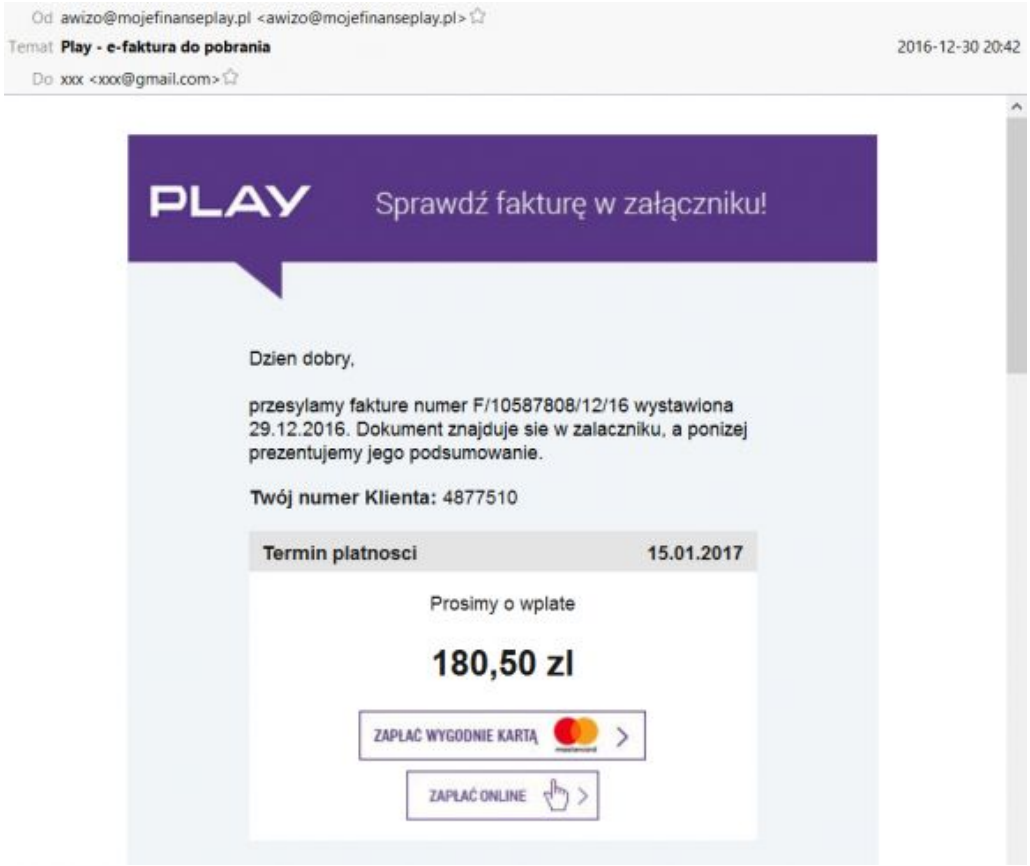
Business e-mail compromise (BEC)



source: https://www.fbi.gov/news/stories/business-e-mail-compromise

https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/business-email-compromise-bec-s

Casual Phishing



source: https://zaufanatrzeciastrona.pl/post/uwaga-na-faktury-od-playa-czyli-historia-nietypowego-konia-trojanskieg

Phishing e-mails z prawdziwymi danymi

Hello Tomasz Graszek,

I'm a hacker who broke your email as well as device a couple of weeks back.

You entered your password on one of the web sites you visited, and I intercepted that.

This is the security password of **tomasz.graszek@o2.pl** upon time of compromise: **1qaz@WSX**

Via your e-mail, I uploaded malware computer code to your Operation System.

Furthermore I set up a Virus on your system. You don't believe me?

Your email: **tomasz.graszek@o2.pl**,

Your phone number: **601123456**

Pesel: **74012000134**

You are not my only prey, I normally lock pcs and ask for a ransom.

source: https://sekurak.pl/dostales-swoje-prawdziwe-haslo-w-mailu-z-zadaniem-okupu-to-scam/

Jak to jest możliwe?

SECURITY BOULEVARD

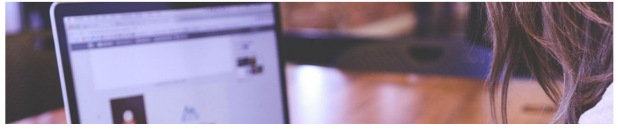
Home ▾ Security Bloggers Network ▾ Webinars ▾ Chat ▾ Library

ANALYTICS APPSEC CISO CLOUD DEVOPS GRC IDENTITY INCIDENT RESPONSE IOT / ICS THREATS / BREACHES

Home » Cybersecurity » Data Security » Data Breach at Stanford Exposes Student Records, Personal Info

Data Breach at Stanford Exposes Student Records, Personal Info

by Luana Pascu on February 20, 2019



Forbes Billionaires Innovation Leadership

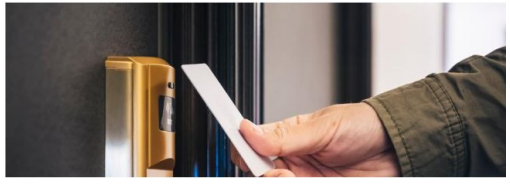
13,411 views | May 31, 2019, 07:49am

Security Systems Of Major Hotel Chains Exposed By Huge Data Breach

Davey Winder Senior Contributor

Cybersecurity

I report and analyse breaking cybersecurity and privacy stories



sekurak

SEKURAK EBOOK | AKTUALNOŚCI | TEKSTY | KONTAKT | AU

Wyciek zdjęć medycznych (400 milionów sztuk!) + danych osobowych z 52 krajów.

17 WRZEŚNIA 2019, 18:32 | AKTUALNOŚCI | KOMENTARZY 5

TAGI: MEDYCYNA, PODATNOŚCI, RODO, WYCIEK

OFFLINE : zin o bezpieczeństwie - pobierz w pdf/epub/mobi.

Nikt wysokiej rozdzielczości zdjęć z badań nie będzie trzymał pod biurkiem. Raczej korzysta się z centralnych systemów, a centralne systemy dostępne są z Internetu (przecież jakoś trzeba te dane tam wgrać ;-). W tym badaniu pokazano podatne systemy PACS (Picture Archiving and Communication Systems) rozsiane po całym świecie. Wyniki są zatrważające:

Krypto Mobilne Prawo Prywatność Wpadki Włamania Złośniki SZKOLENIA

Zaufana Trzecia Strona

Baza danych 2,5 miliona klientów Morele.net wrzucona do sieci

Najlepsze w tyn

Jak bankowi złodzieje

zmian w logowaniu

vpnMentor Blog Best VPN Tools Coupons Search

vpnMentor. » Blog. » Report: Orvibo Smart Home Devices Leak Billions of User Records

Blog

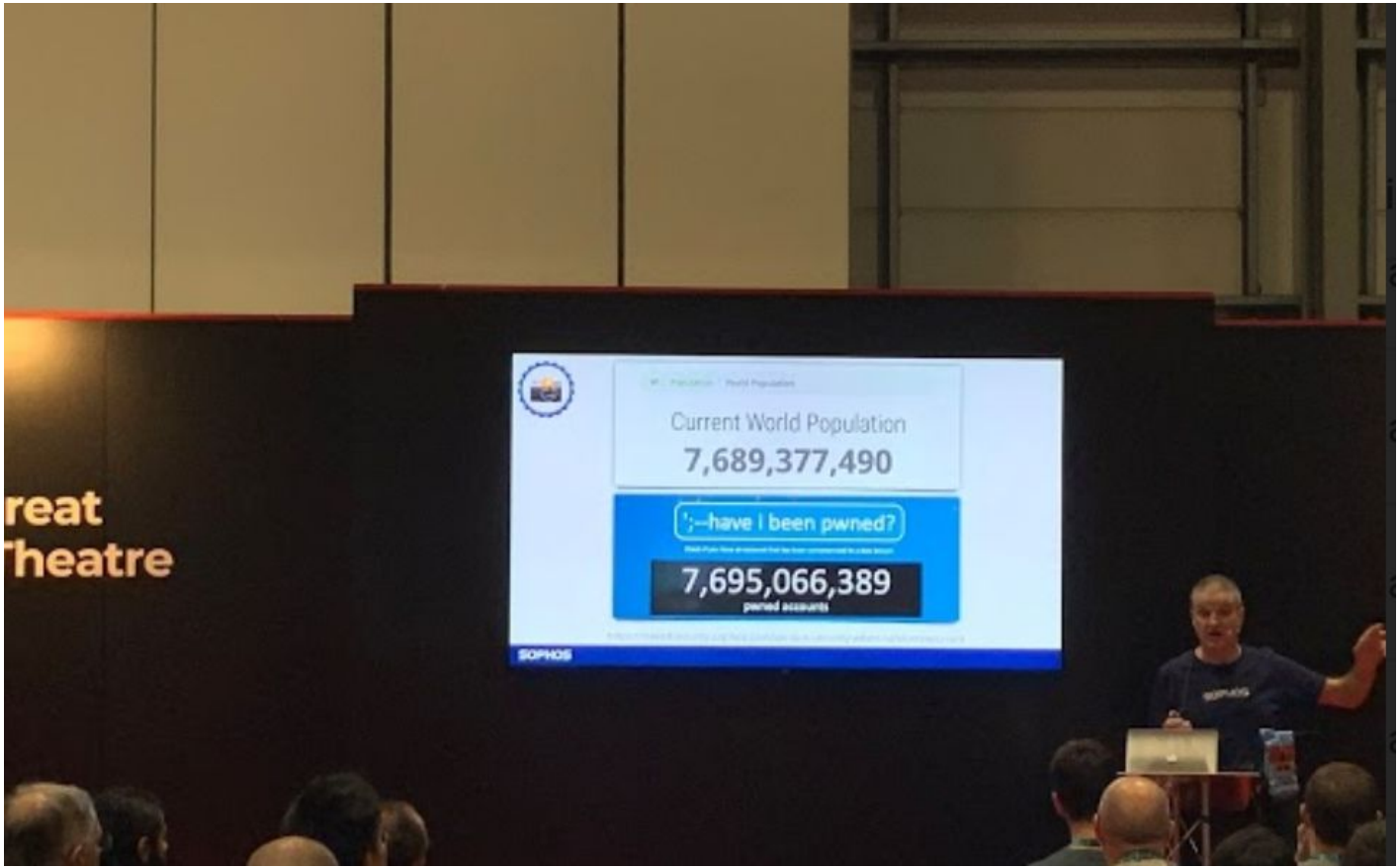
Views: 12,419,802

Posts: 1,280

Follow our experts

Report: Orvibo Smart Home Devices Leak Billions of User Records

Jak to jest możliwe?



Wektory ataku

Direct contact

Text messages

Phone call

Socialmedia

Traditional mail

E-mail

Online services

BUCKINGHAM PALACE

From: Mr. Edward Young,
Private Secretary to HM the Queen Elizabeth II

Private and Confidential 16 September, 2019

Dear Mr. Ridden,

For the second time in the last 30 yrs, Her majesty the Queen Elizabeth II appeals to a certain number of people to save Great Britain's economy. As you know, the Brexit will happen quite quickly, and we have not reached a bilateral agreement with the European Union.
To save and sustain the UK's economy after Brexit, we must pay to the European Union £19 billions. We currently have more than 82% of money available, and we need to rise the rest until Oct 19th 2019.

With indulgence we appeal to you if you can borrow the Royal House with amounts between £450,000 - £2,000,000
We will offer **30%** interest for a period of 3 months and a posibility to become a Member of the Royal Warrant Holders Assiciation.

By paying this amount to the European Union, we will be able to keep the economy and inflation exactly as it is for a minimum period of 10 years and the future changes will not affect imports from EU countries.

We want this letter to remain anonymous as we do not wish the subject to go viral.
This could affect the agreements we have in order to obtain the bilateral agreement.

In order to be able to help us financially,please transfer the money to the **Bitcoin** address that was attached to your letter. Once we receive the funds, we wil send you another letter with the contract.

The Queen's warm good wishes to you all for your continuing success in the future.

BTC WALLET: 1sycBKECFgPBD3EiaTCcD2VCeobr8DrpD

THE ROYAL WARRANT HOLDERS ASSOCIATION BY AUTHORITY

Your sincerly,

Edward Young
Private Secretary to HM the Queen Elizabeth II

Mr. Ridden

Standard Chartered

Date: September 5th, 2019

Dear: [redacted]

Hello, this letter may come to you as a surprise as we have not met before or handled any business deal in the past. Nevertheless, I have contacted you with genuine intentions and I hope I can trust you with this Inheritance opportunity which I explain below.

My name is Mr. Peter Pfizer, an account manager with Standard Chartered Bank, London United Kingdom. I retrieved your contact address in my search for the next of kin to a deceased customer of our bank MR. VAN COBB, a citizen of your country, who lived and died in London from Cardiac Arrest in the year 2009. Unfortunately, this customer died intestate leaving his bank account with an open beneficiary status. All efforts made by our bank to locate his relatives have been unsuccessful so I decided to write you as I have monitored this account in the bank for almost 10 years now and no one has come forth with any claim. I would like to present you to our bank as his next of kin to claim this dormant account worth $11.6 Million USD (Eleven Million Six Hundred Thousand US Dollars).

While I work from the inside to make sure all needed information and evidences are provided to you to back up your claim. You will apply to the bank as an extended relative to the deceased customer, the account has an open beneficiary status, which is why I have contacted you to come forth and claim the funds as the next of kin and beneficiary. Since he is from your country and you both share the same last name, it easy for you to become his official next of kin. If we do not make claim to the funds now, the funds would be reverted back to the system as unclaimed estate at the expiration of a 10-year dormancy period.

It requires all confidentiality at this stage and I believe that you are ready to keep this absolutely discreet until you are able to claim the funds from the bank. I also assure you that this transaction would be handled under due inheritance procedures and every necessary legitimate arrangement will be put in place to make you the real beneficiary of the inheritance funds. Once the funds are released to you, it will be shared between the two of us.

Please send your response to my personal email: dexyan54321@yandex.com indicating readiness to proceed with this transaction. Then I will give you more details and we shall have in-depth discussion regarding a successful completion of this transaction.

I await your response

Sincerely

Socjotechnika

czyli hakujemy człowieka, a nie komputer...

- Fałszywy sklep
- Fałszywy sklep + fałszywa strona z opiniami
- Fałszywy sklep + prawdziwa strona z opiniami
- Fałszywy sklepy + prawdziwe płatności
- Prawdziwe usługi + fałszywe smsy
- Vishing
- Konto w portalu ogłoszeniowym
- Konto w serwisie aukcyjnym
- Konto w serwisie społecznościowym
- …

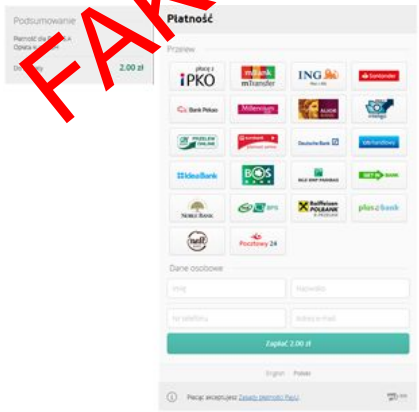
Socjotechnika

czyli hakujemy człowieka, a nie komputer...

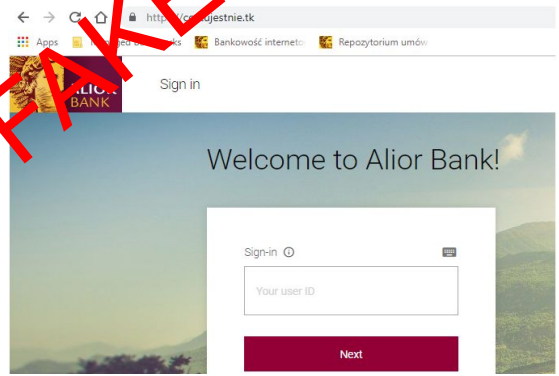
1.

Fałszywa strona
Prawdziwa strona
E-mail
SMS
Socialmedia

2.

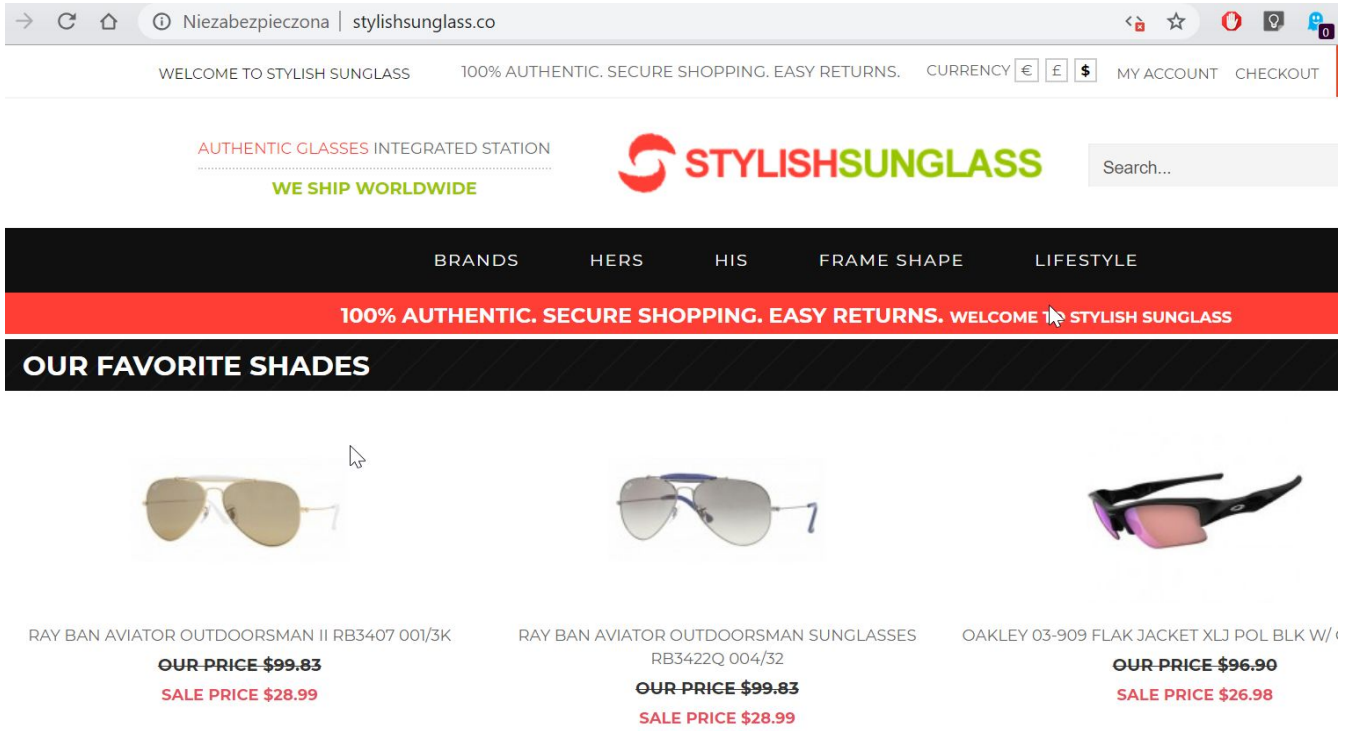


3.



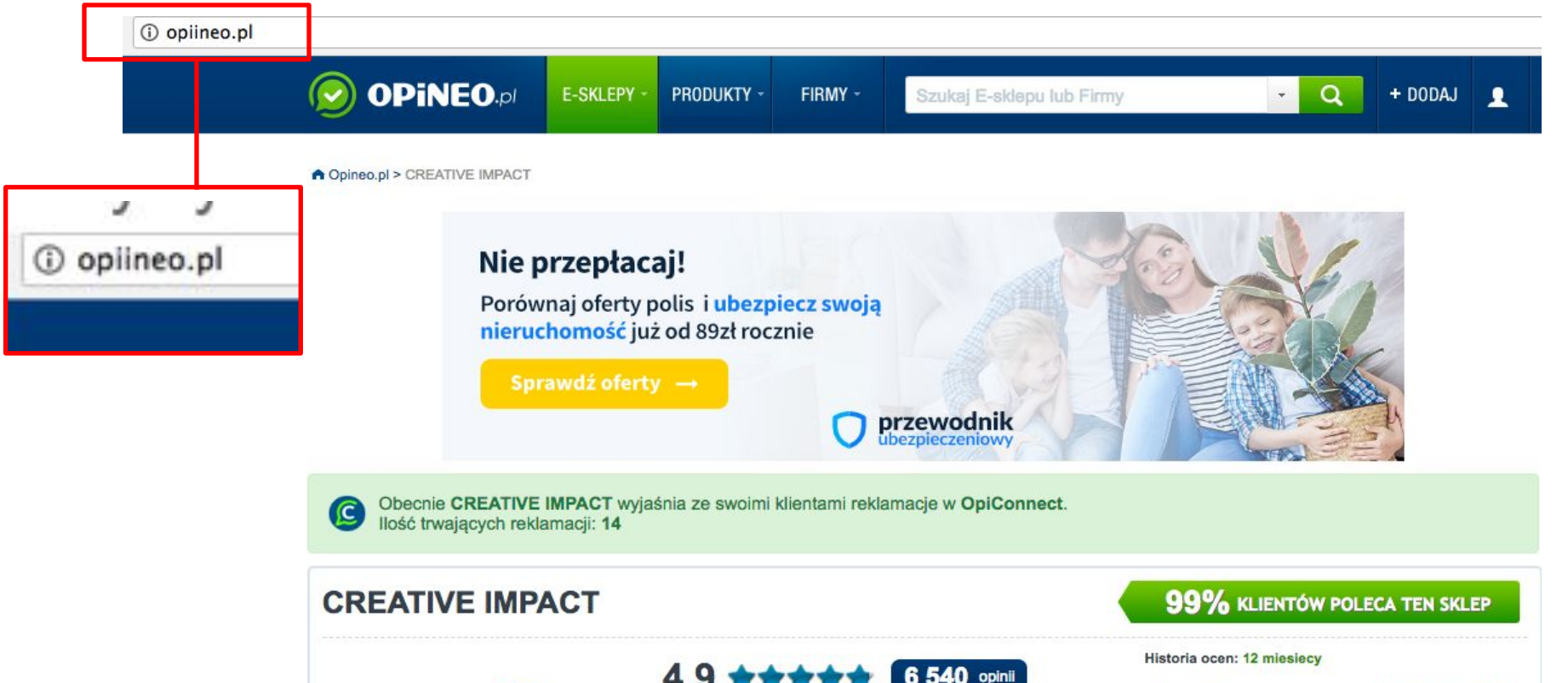
Socjotechnika

Fałszywy sklep



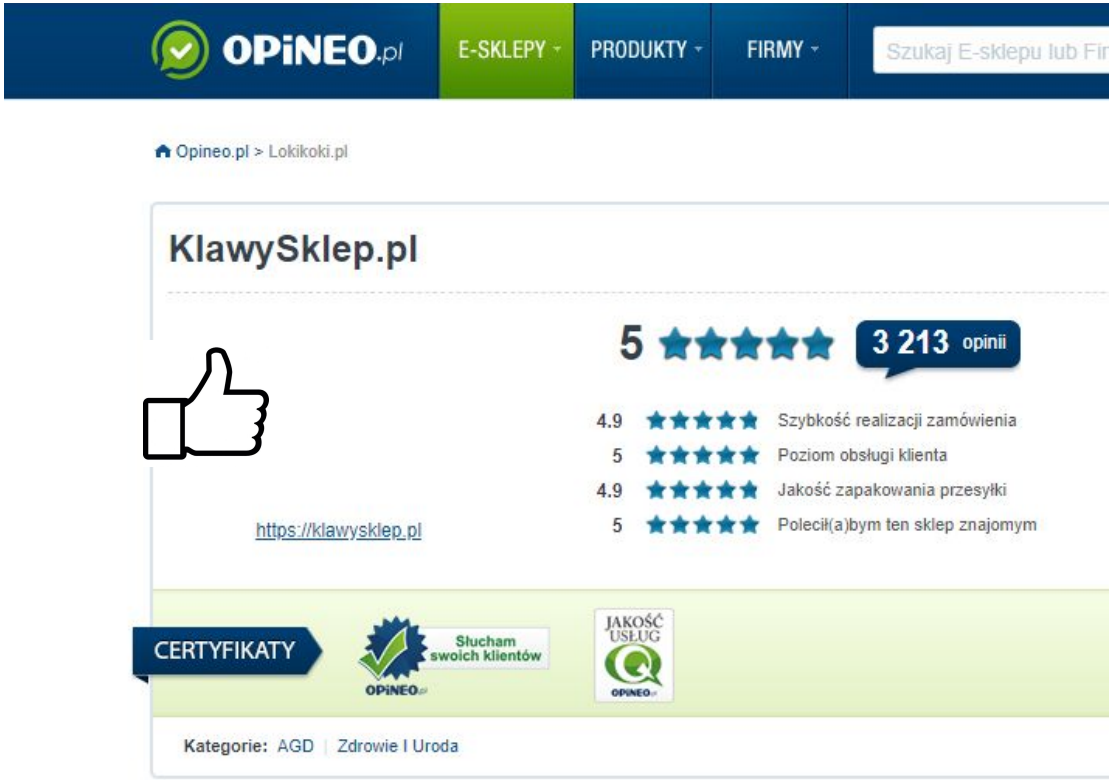
Socjotechnika

Fałszywy sklep + fałszywa strona z opiniami



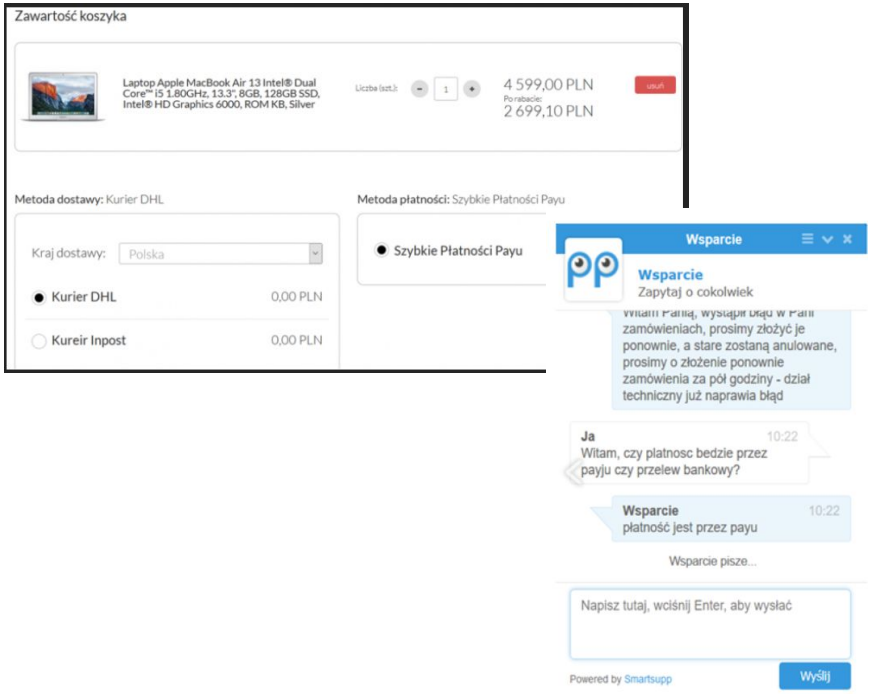
Socjotechnika

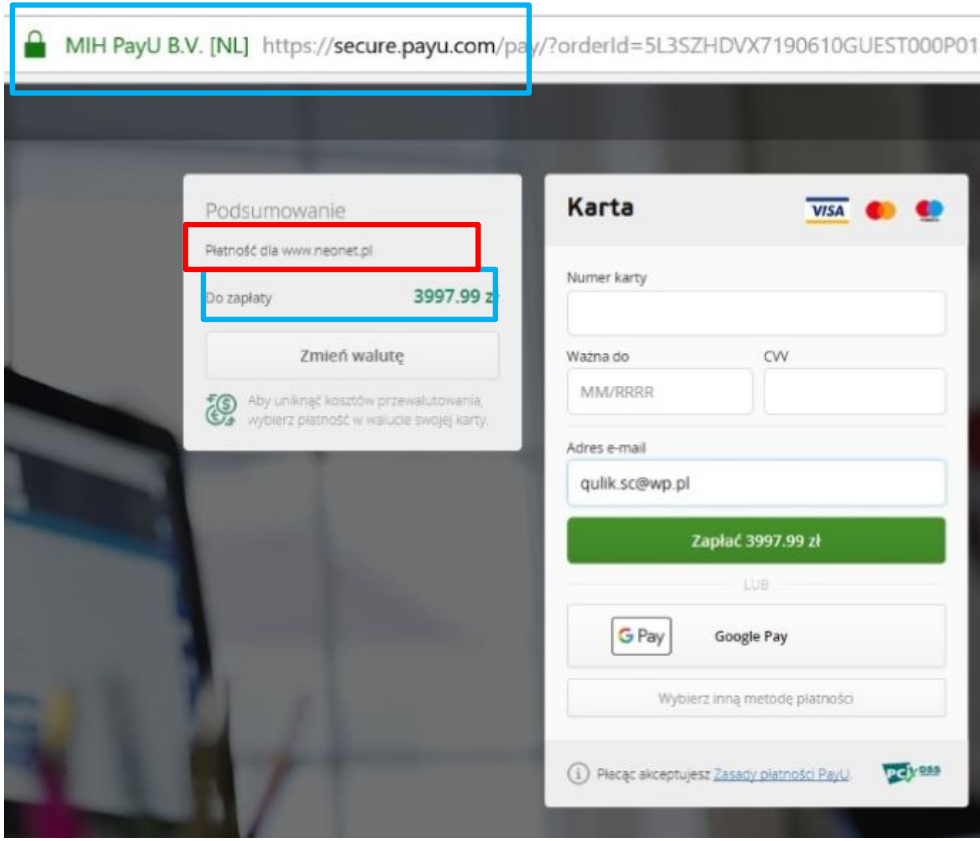
Fałszywy sklep + prawdziwa strona z opiniami



Socjotechnika

Fałszywy sklepy + prawdziwe płatności

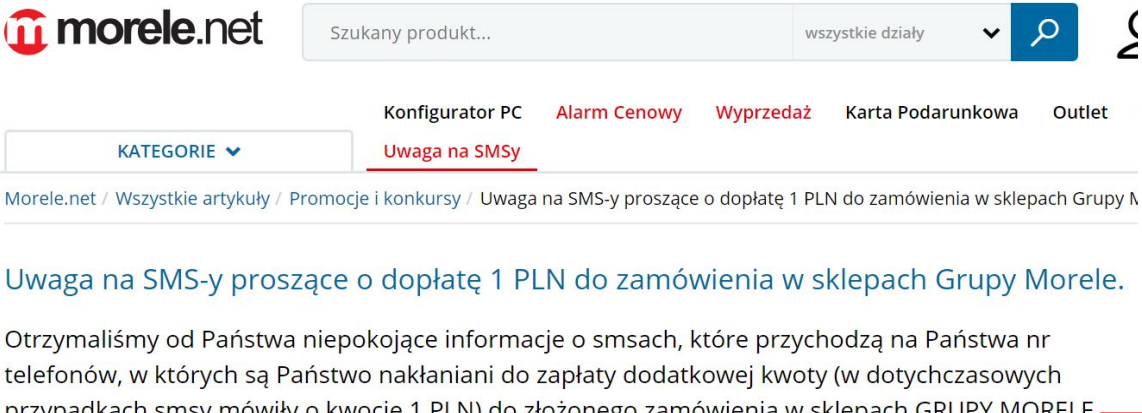


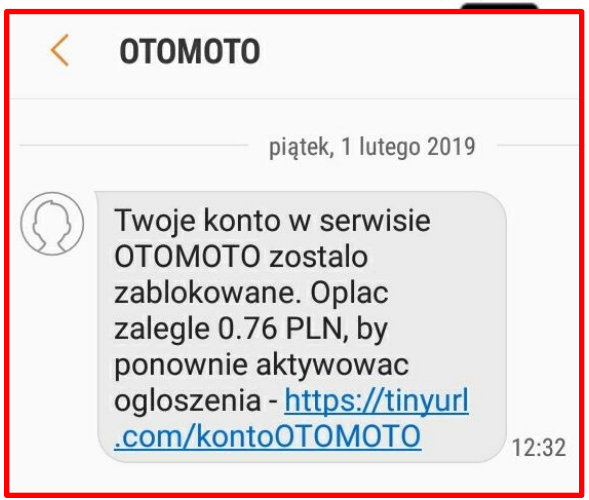


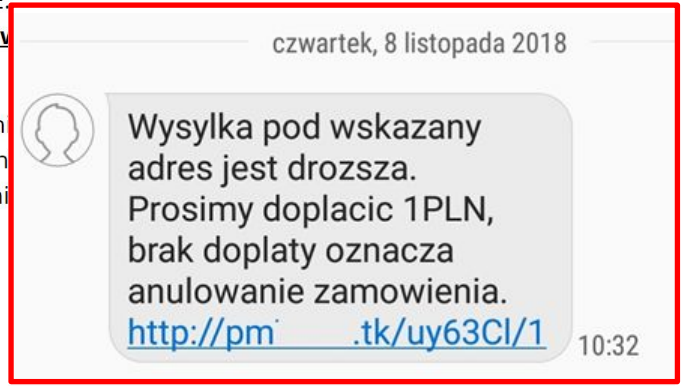
źródło: https://zaufanatrzeciastrona.pl

Socjotechnika

Prawdziwe usługi + fałszywe smsy







Socjotechnika

Vishing

Idea Bank Usługi Finansowanie dla firm Konta Oszczędności 3 Kontakt Zaloguj

Ostrzeżenie przed nowym rodzajem cyberataków na klientów!

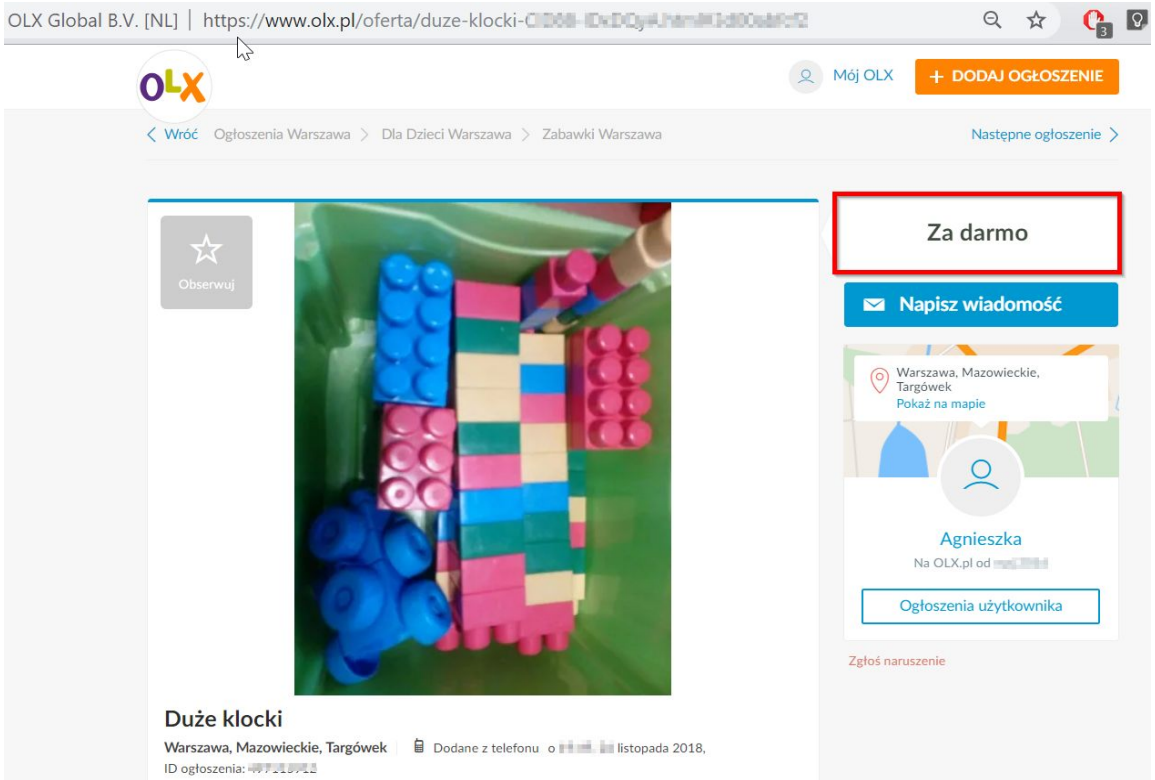
Bank zidentyfikował nowy sposób działania przestępców próbujących wykradać środki Klientów. Przestępcy, podszywając się pod numery infolinii, dzwonią do Klientów z prośbą o podanie kodów jednorazowych otrzymanych SMS-em.

Jak bronić się przed przestępcami:

1. Pamiętaj, NIE PODAWAJ NIKOMU haseł do bankowości ani kodów jednorazowych, które otrzymujesz w momencie dokonywania transakcji w bankowości.
2. Bank NIGDY nie prosi o podanie haseł jednorazowych ani haseł do bankowości.
3. Bank NIGDY nie prosi też o podanie całego hasła do kontaktu telefonicznego, a jedynie o wskazane znaki z hasła.
4. NIGDY nie otwieraj podejrzanych załączników. Przestępcy bardzo często wysyłają wiadomości z informacją o zaległych fakturach, podszywają się np. pod urząd skarbowy itp. Otwarcie załącznika (najczęściej .pdf, .doc, .exe, .xls, .zip) skutkuje zainfekowaniem komputera i wykradzeniem informacji.
5. Jeśli otworzyłeś podejrzany e-mail lub załącznik, NIE BAGATELIZUJ tego błędu – niezwłocznie oddaj komputer do wyczyszczenia przez specjalistów, zaloguj się do bankowości z innego urządzenia i zmień hasło, w razie pytań skontaktuj się z infolinią Banku.
6. Pobierz i zainstaluj system IBM Trusteer (dostępny na stronie logowania do bankowości Idea Cloud).

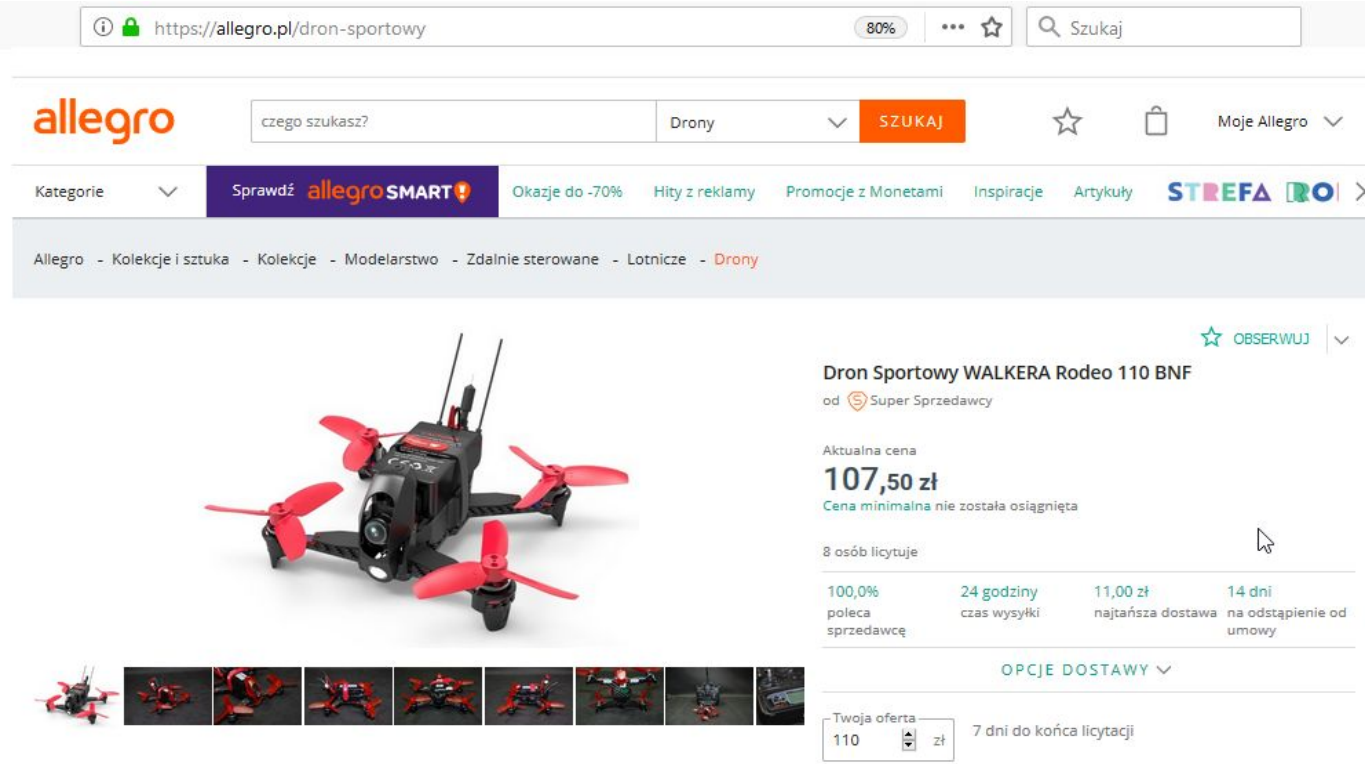
Socjotechnika

Konto w portalu ogłoszeniowym



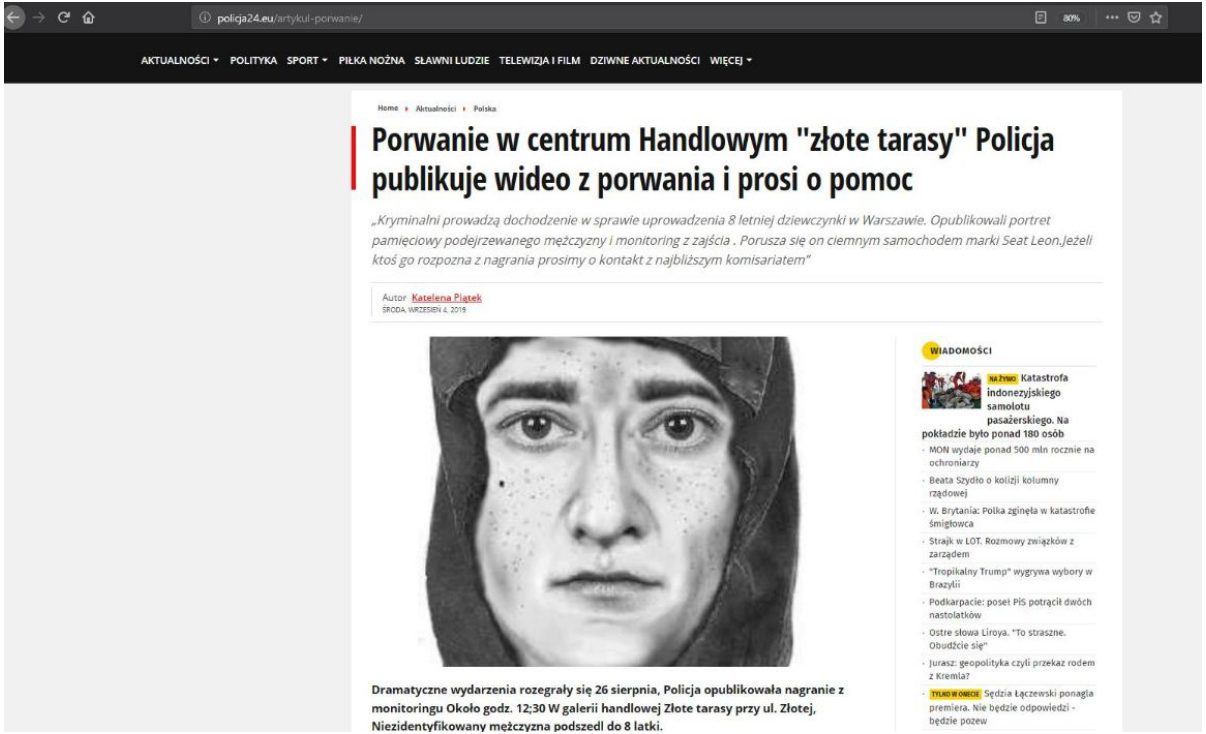
Socjotechnika

Konto w serwisie aukcyjnym



Socjotechnika

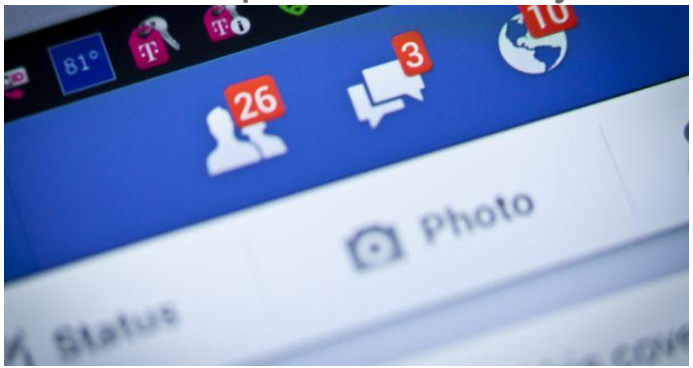
Konto w serwisie społecznościowym

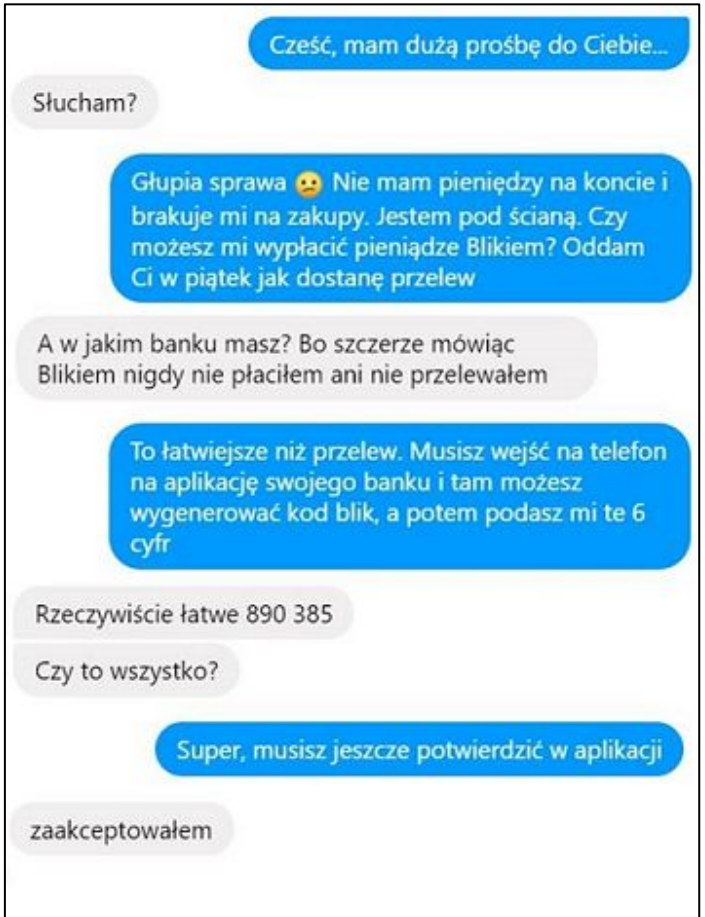


źródło: https://twitter.com/AdamLangePL/status/1169167754278133760/photo/1

Socjotechnika

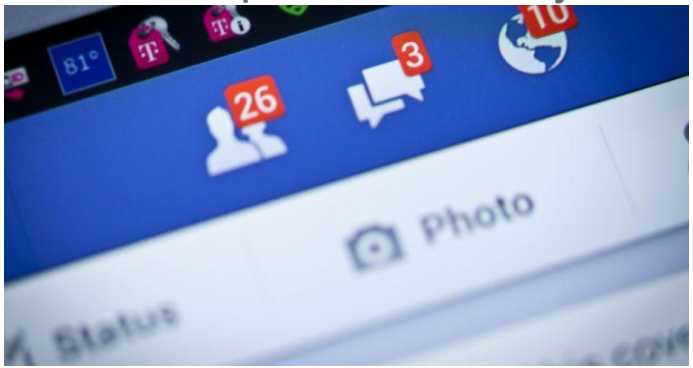
Konto w serwisie społecznościowym

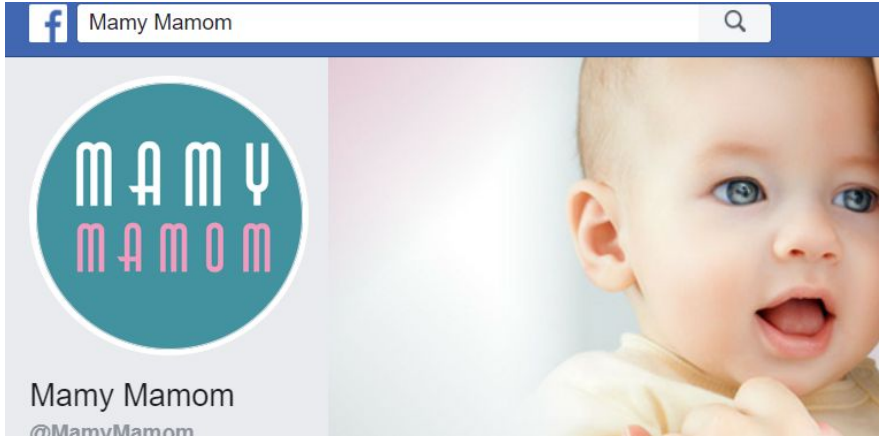




Socjotechnika

Konto w serwisie społecznościowym



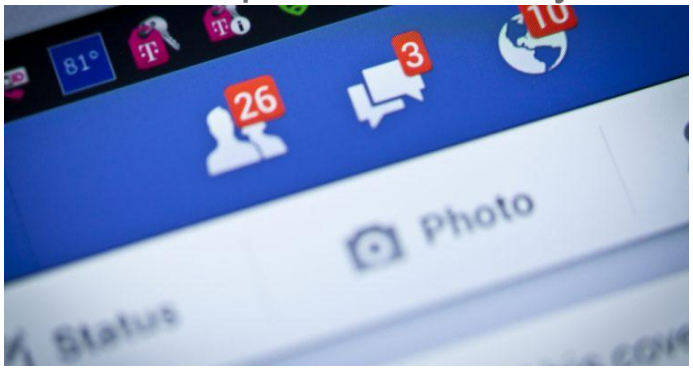


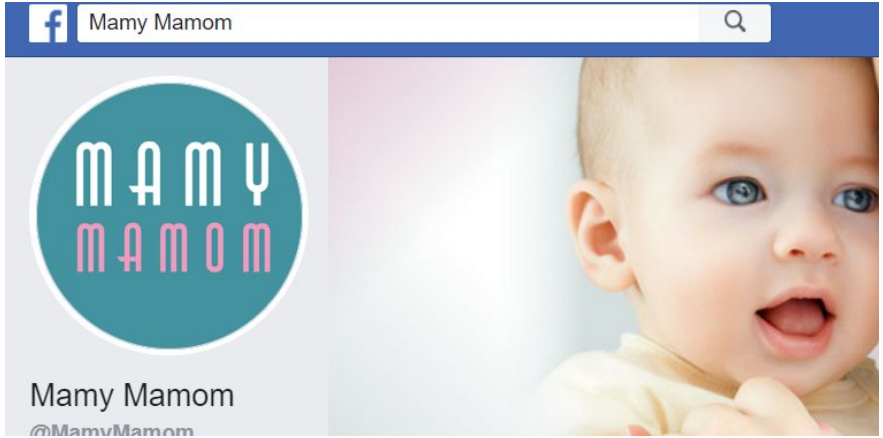
Czyli wszystko dograne? Jak mogę zapłacić?

Najtaniej i najszybciej będzie przez bramkę płatności: **https://dotpay.pl.platnosci.link/index.php?TransactioID=XXX**

Socjotechnika

Konto w serwisie społecznościowym



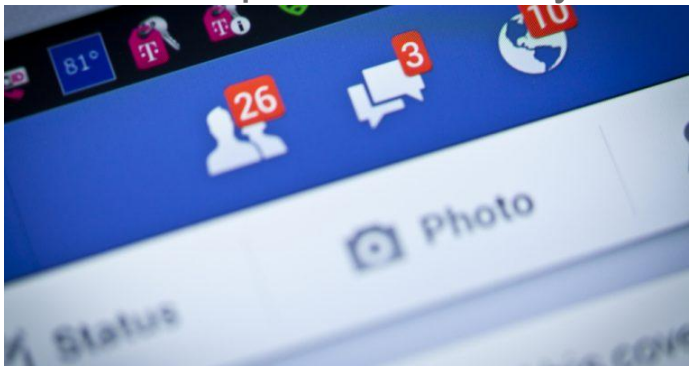


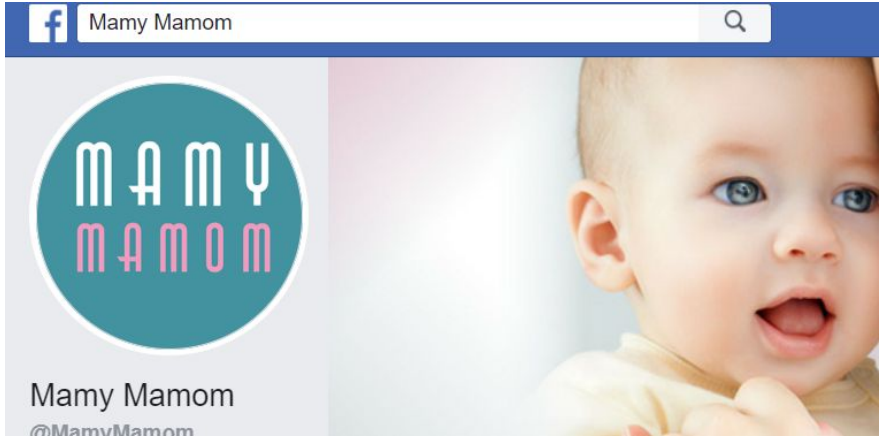
Czyli wszystko dograne? Jak mogę zapłacić?

Najtaniej i najszybciej będzie przez bramkę płatności:
https://dotpay.pl.platnosci.link/index.php?TransactioID=XXX

Socjotechnika

Konto w serwisie społecznościowym

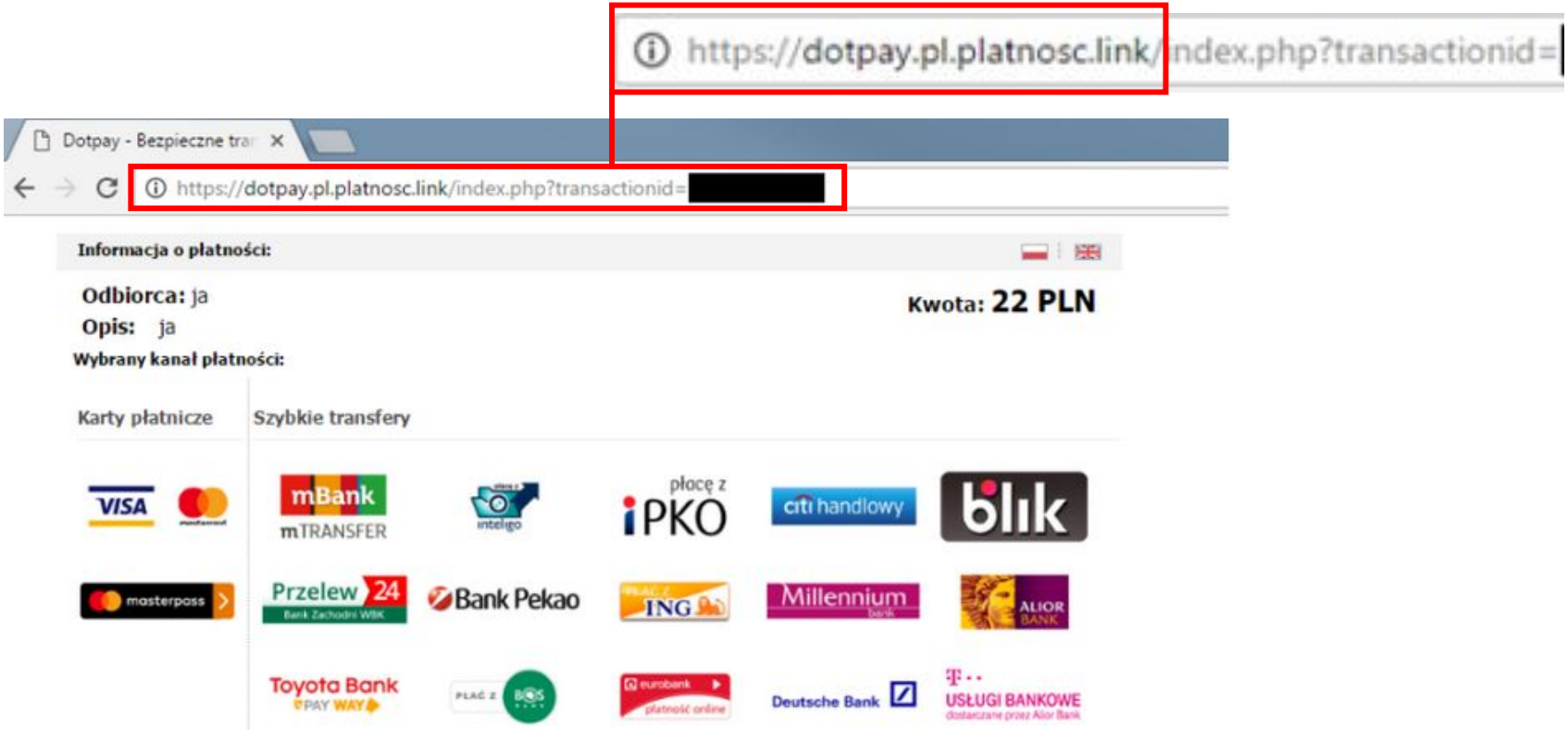




Czyli wszystko dograne? Jak mogę zapłacić?

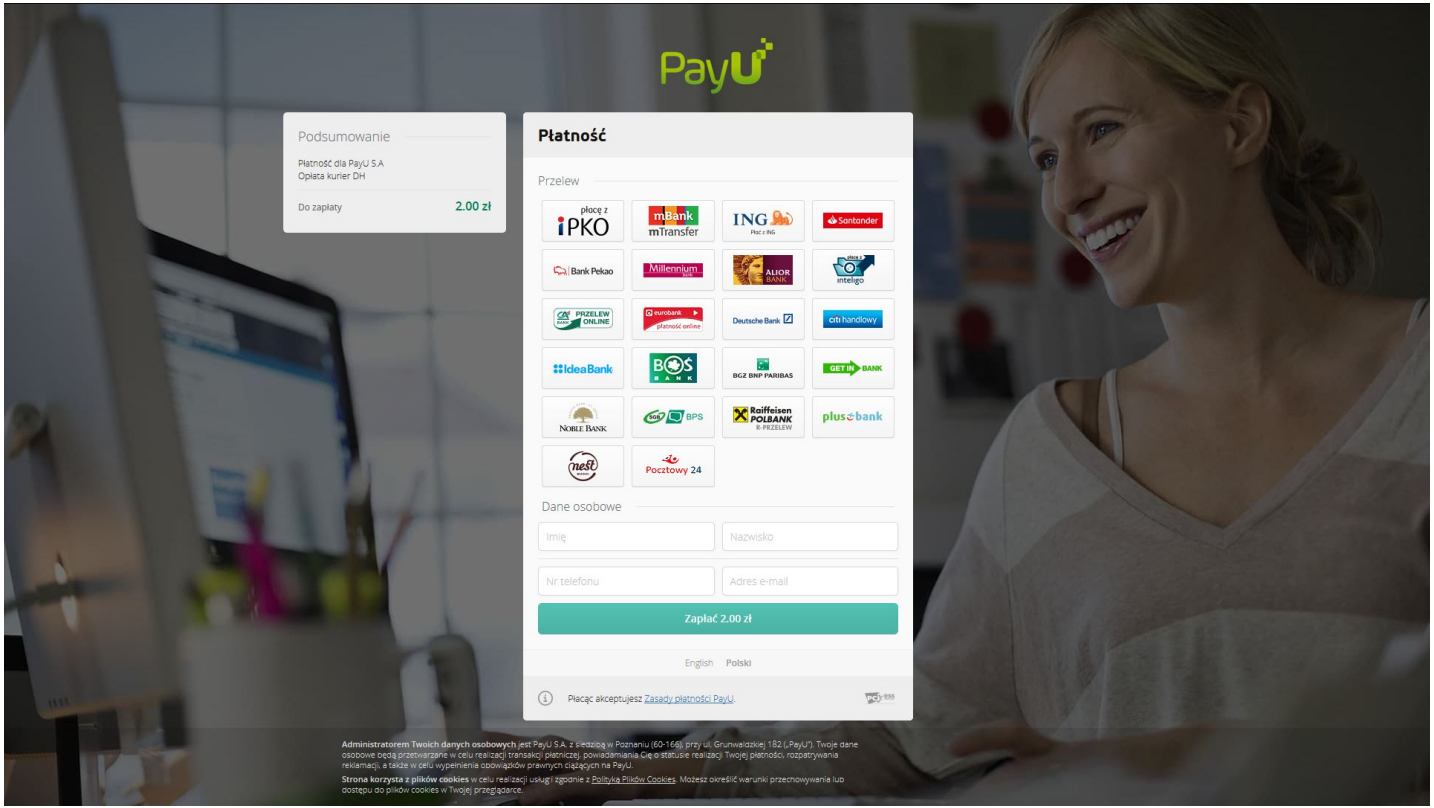
Najtaniej i najszybciej będzie przez bramkę płatności: **https://dotpay.pl.platnosci.link/index.php?TransactioID=XXX**

Fałszywi pośrednicy płatności

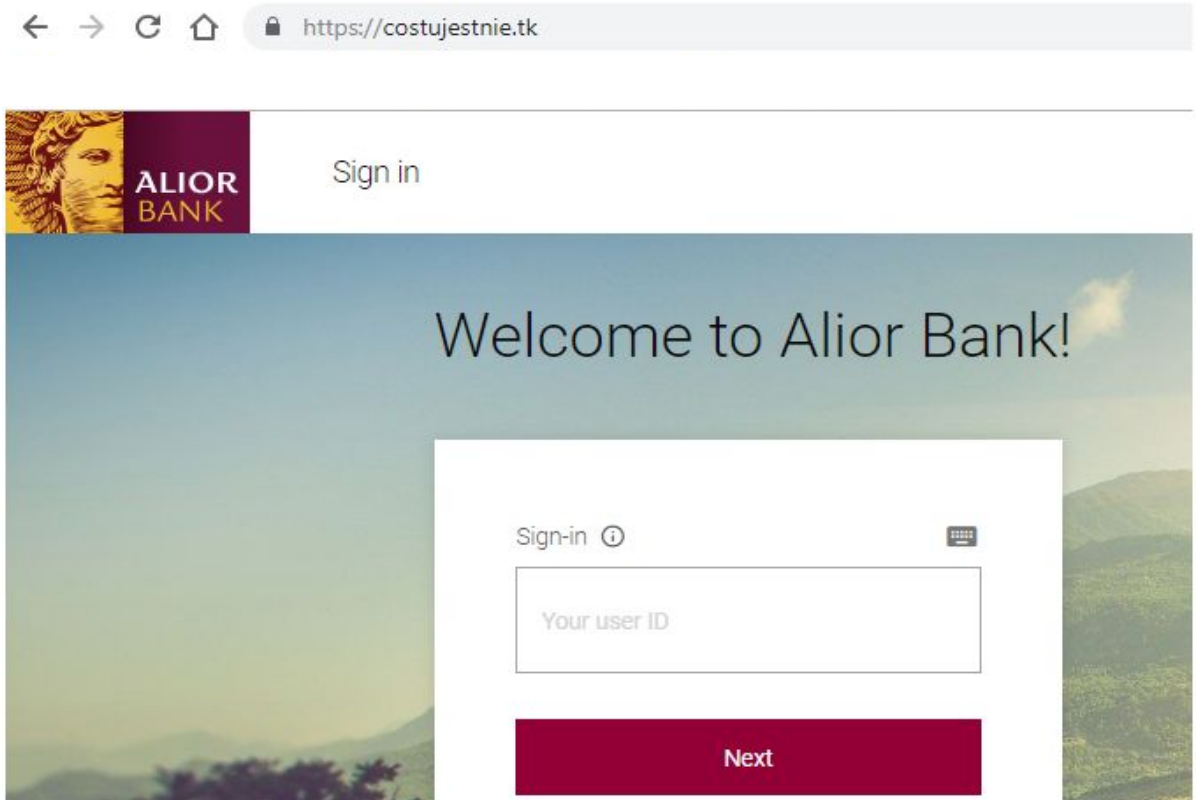


Źródło: https://badcyber.com/from-full-facebook-account-takeover-to-an-empty-bank-account/

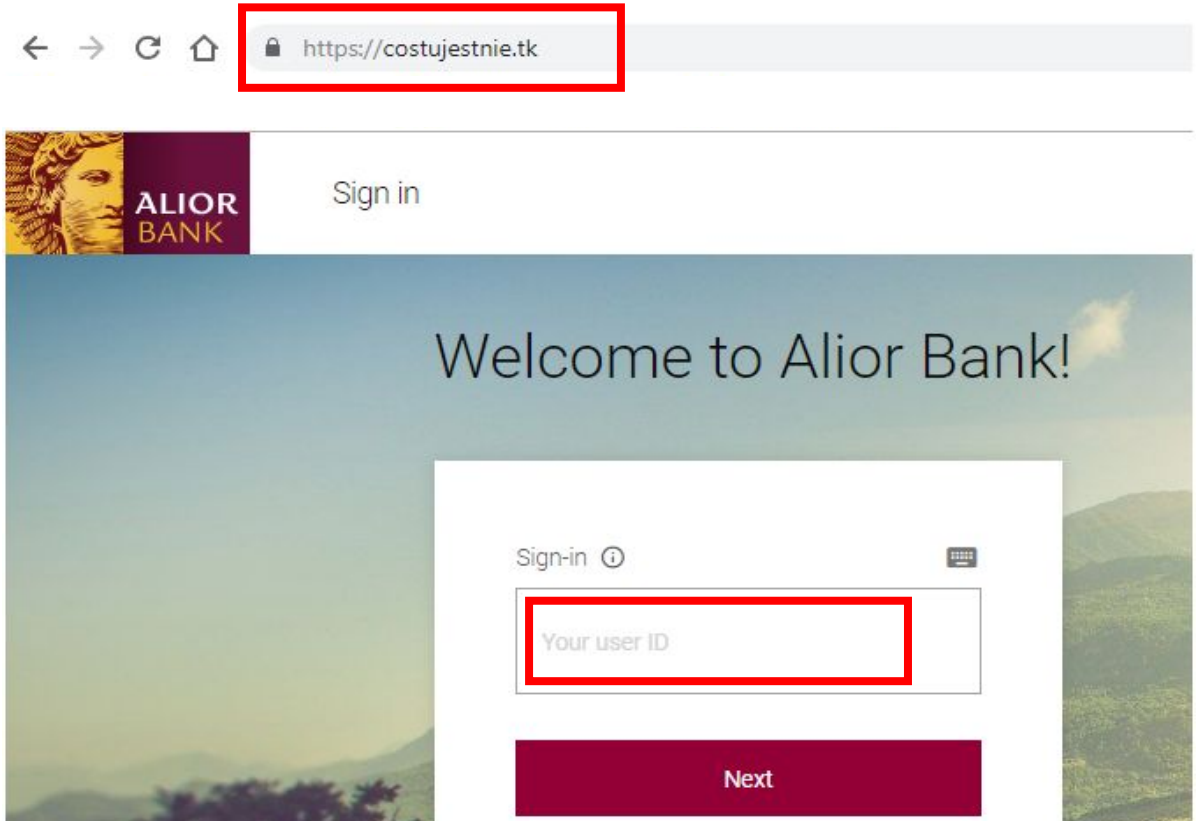
Fałszywi pośrednicy płatności



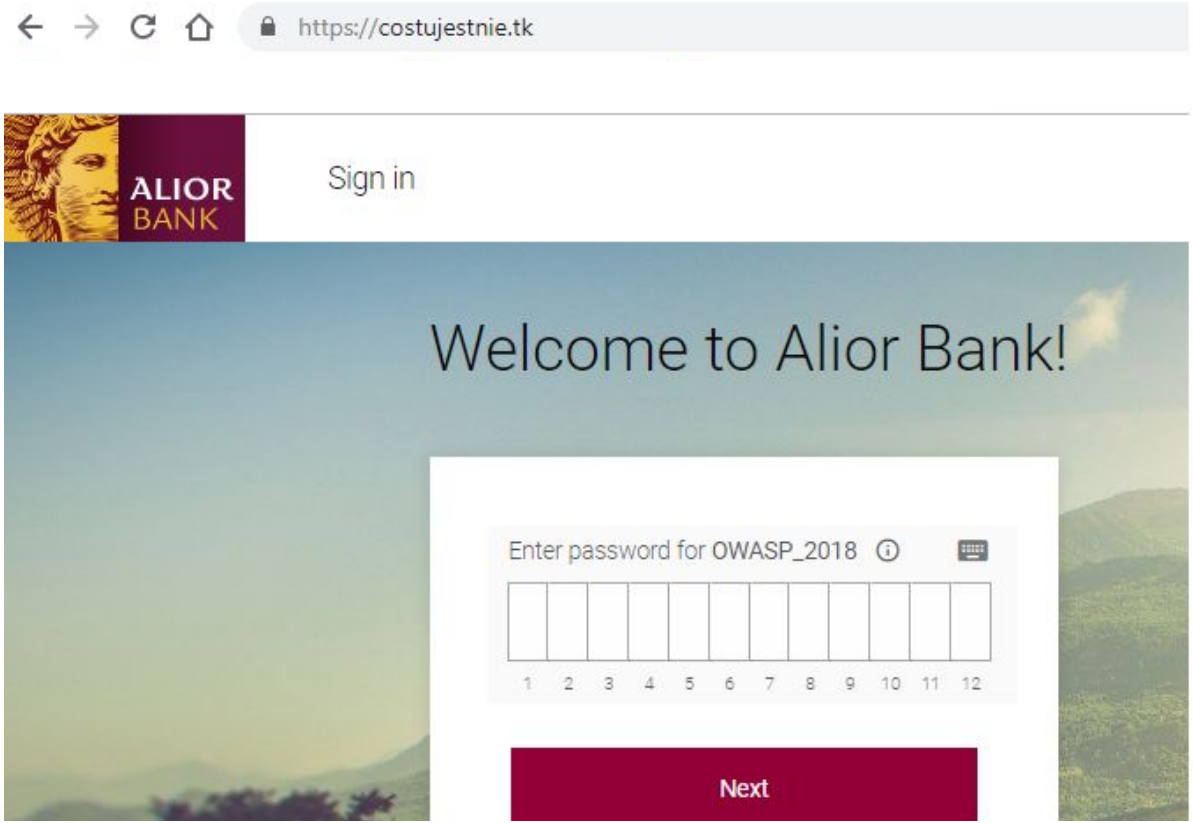
Fałszywi pośrednicy płatności



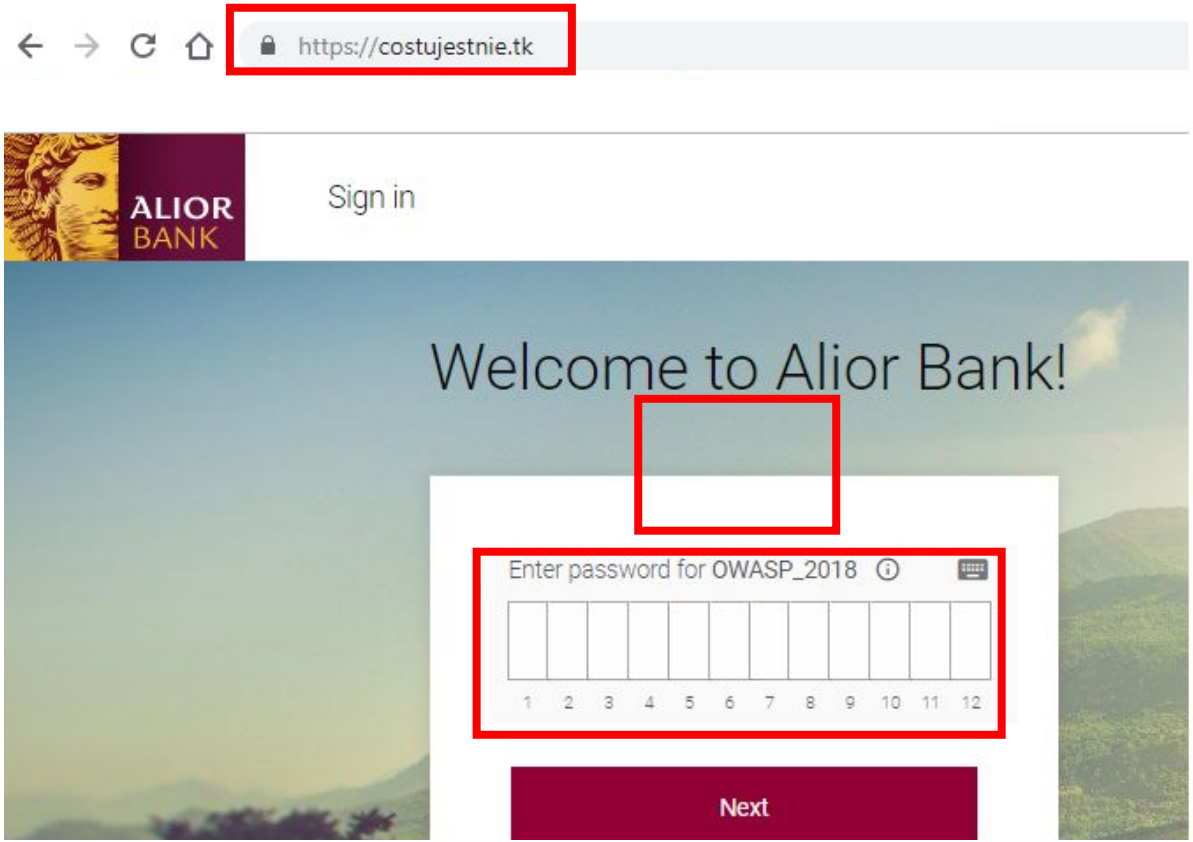
Fałszywi pośrednicy płatności



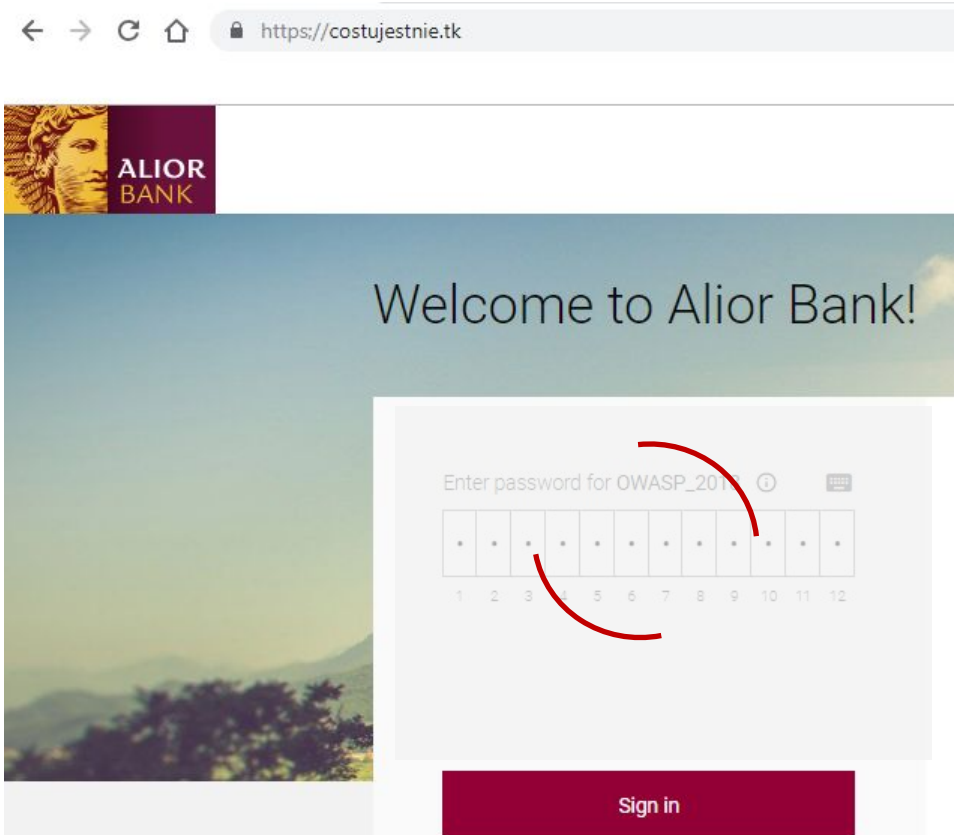
Fałszywi pośrednicy płatności



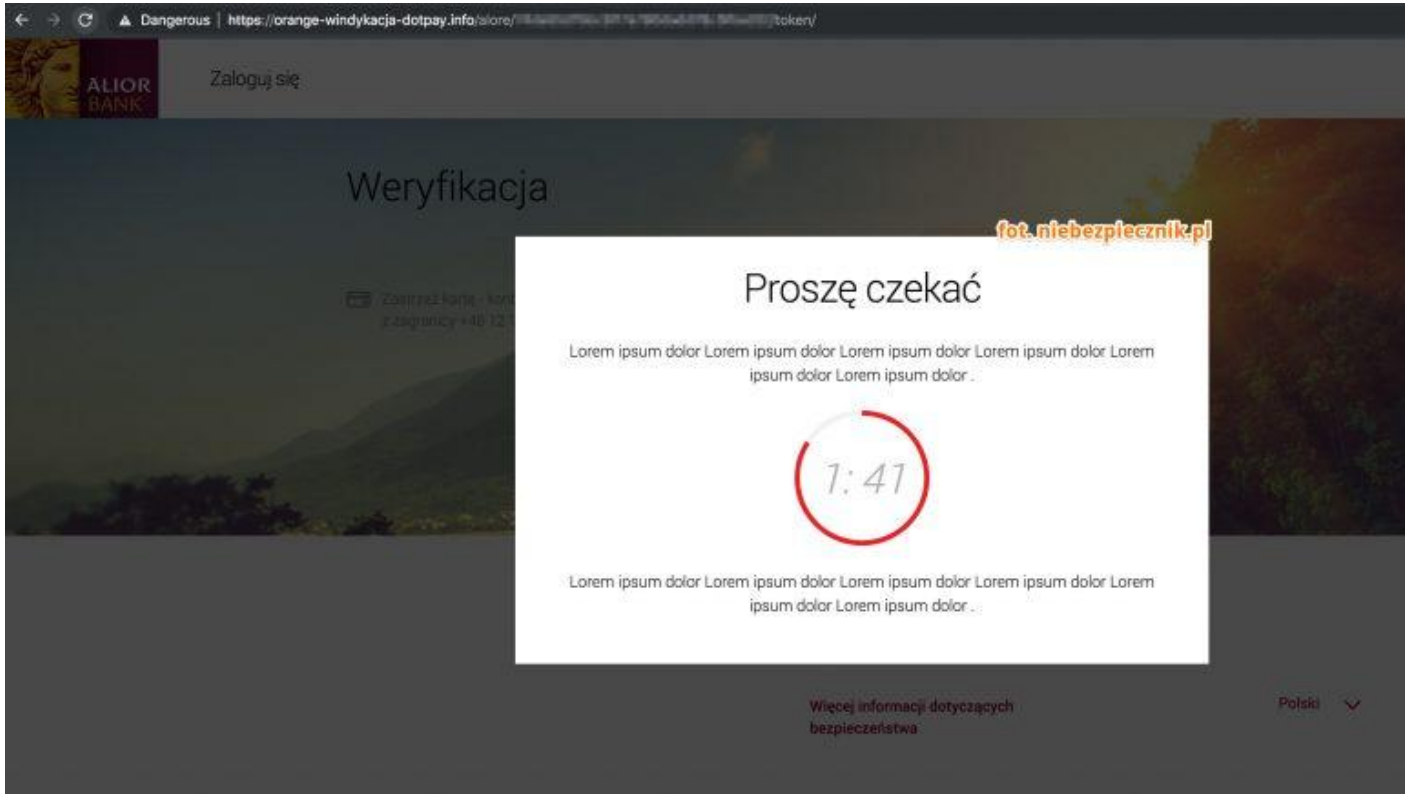
Fałszywi pośrednicy płatności



Fałszywi pośrednicy płatności

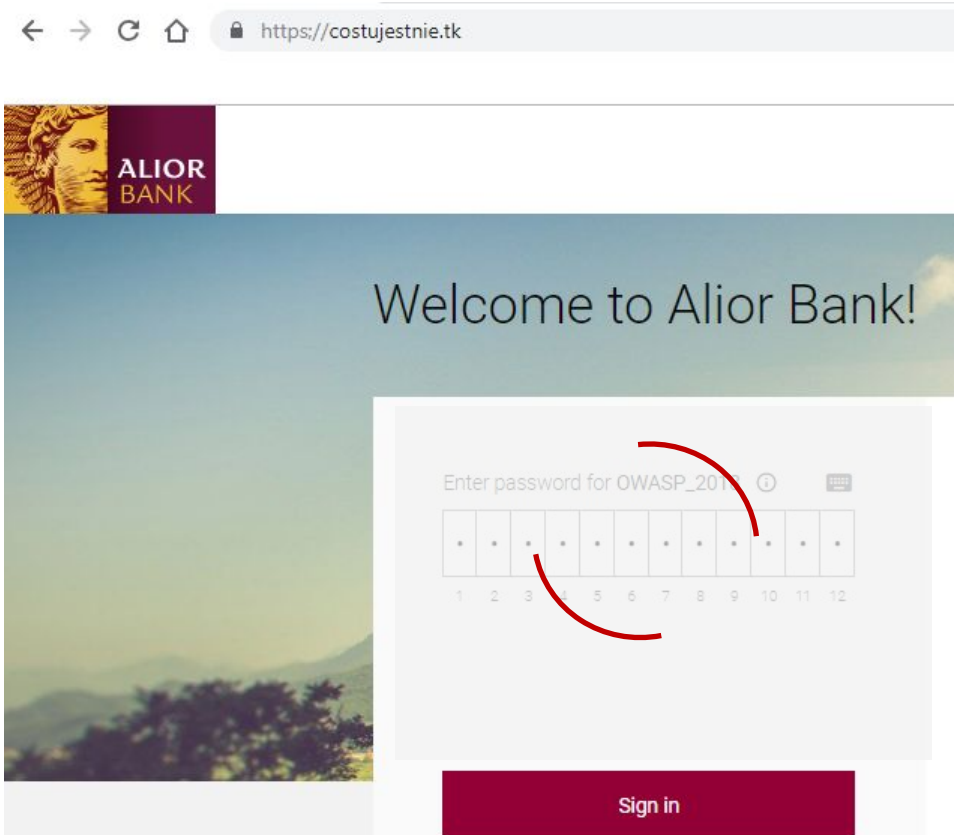


Fałszywi pośrednicy płatności

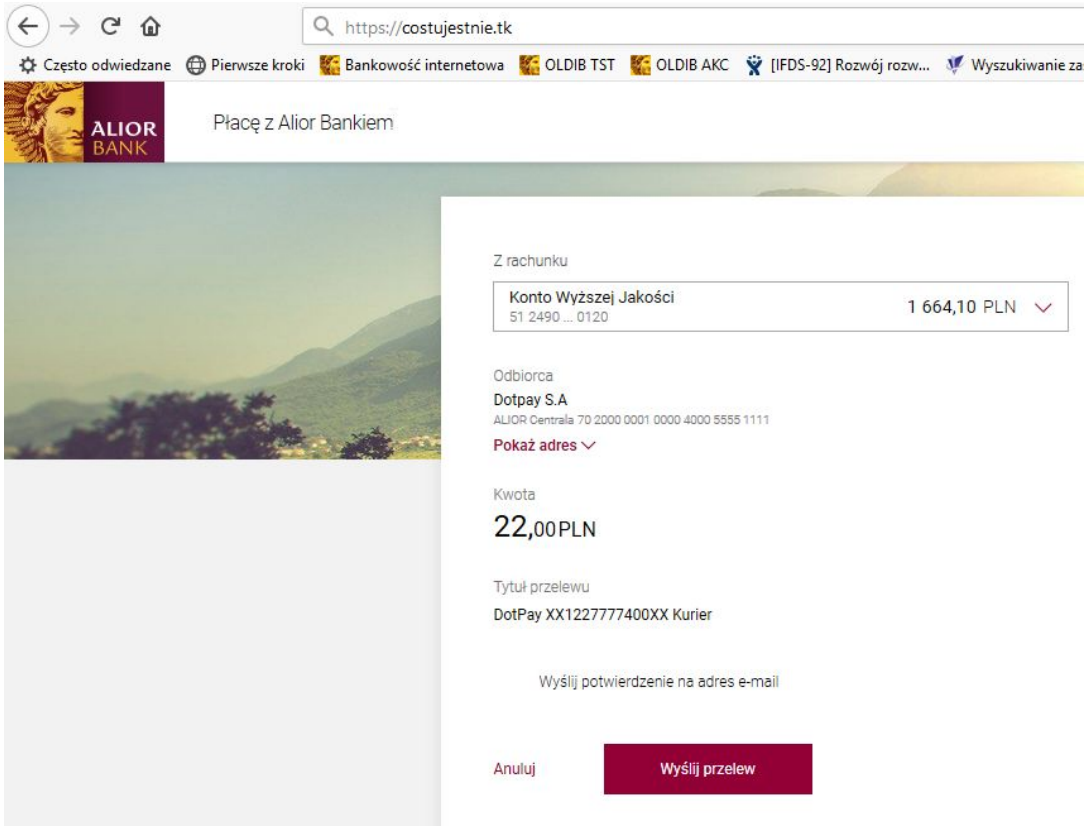


źródło: https://www.niebezpiecznik.pl/

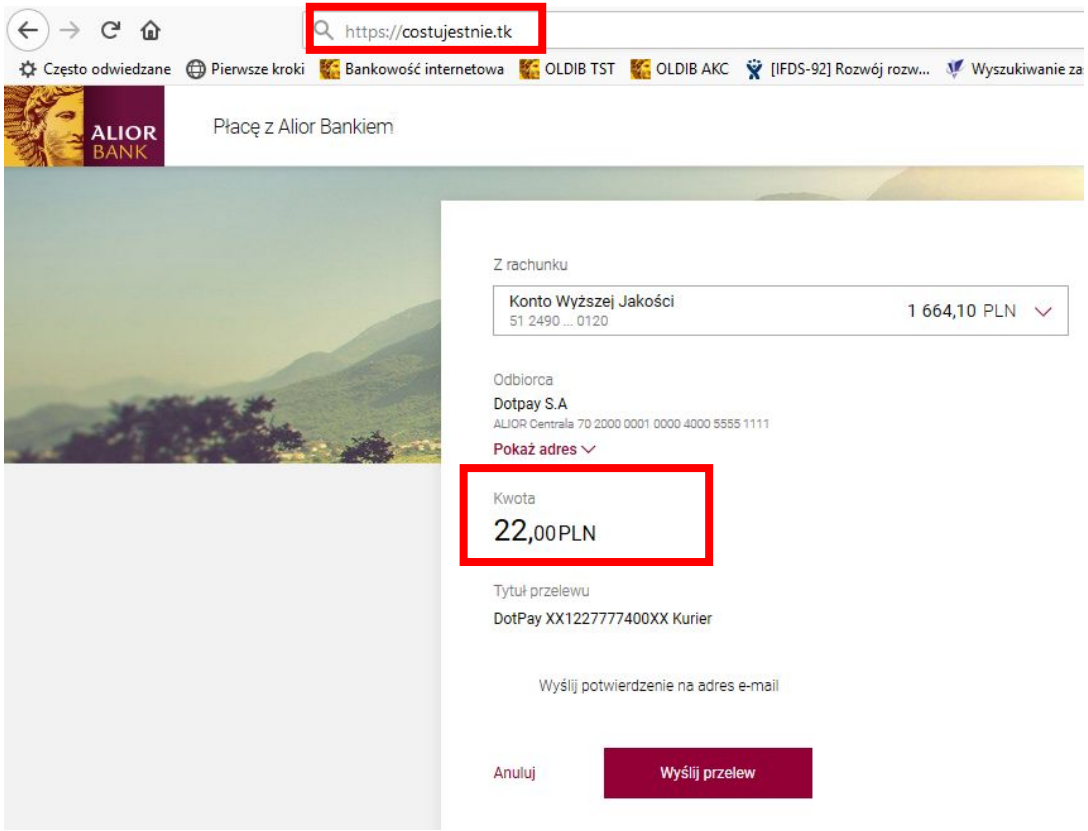
Fałszywi pośrednicy płatności



Fałszywi pośrednicy płatności

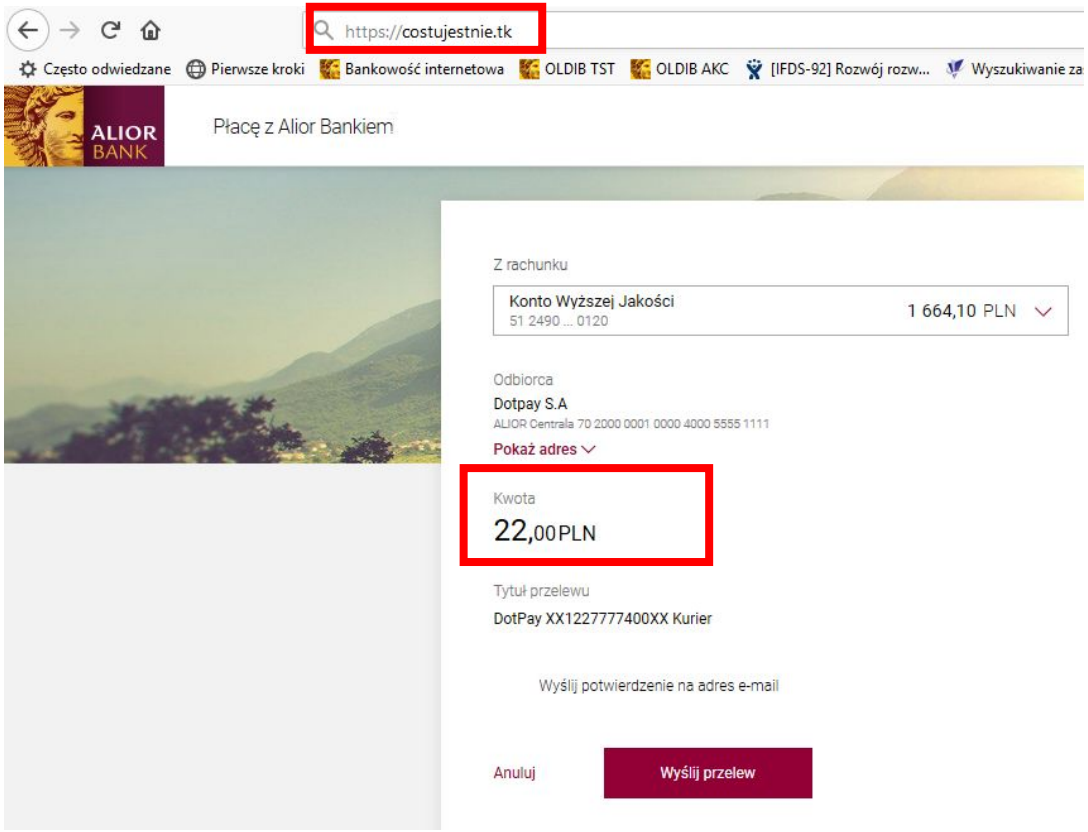


Fałszywi pośrednicy płatności



Przelew na rachunek 70… 1000 z zapisem szablonu zaufanego DotPay; odbiorca: DotPay S.A.; kwota 22,00 PLN. Kod SMS nr 4 z dn. 27-11-2018: 12345

Fałszywi pośrednicy płatności



Przelew na rachunek 70… 1000 **z zapisem szablonu zaufanego DotPay**; odbiorca: DotPay S.A.; kwota 22,00 PLN. Kod SMS nr 4 z dn. 27-11-2018: 12345

Google | Historia | PayU

Niezabezpieczona | anetakurier.info/oplata1412/

Aplikacje

PayU English Polski

Podsumowanie

Płatność dopłata za przesyłkę 4182552

Całkowity 1.16 PLN

Wybierz sposób zapłaty

Metody płatności

Przelew bankowy
online lub przelewem

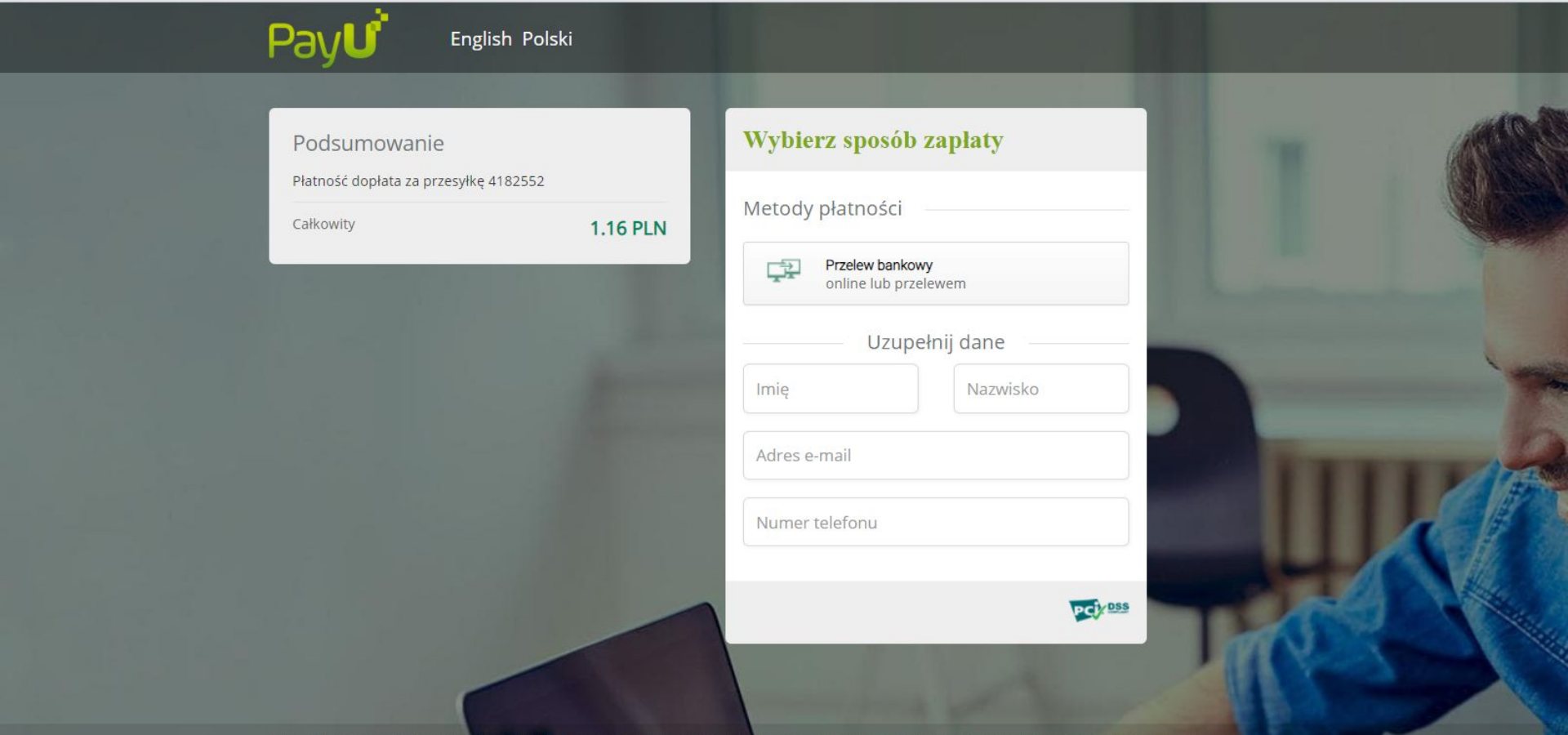
Uzupełnij dane

Imię

Nazwisko

Adres e-mail

Numer telefonu



Alior Bank

Niezabezpieczona | anetakurier.info/oplata1412/aliorbank/sign-in

Aplikacje

ALIOR BANK

Zaloguj się

Witamy w Alior Banku!

Login

Wpisz identyfikator klienta

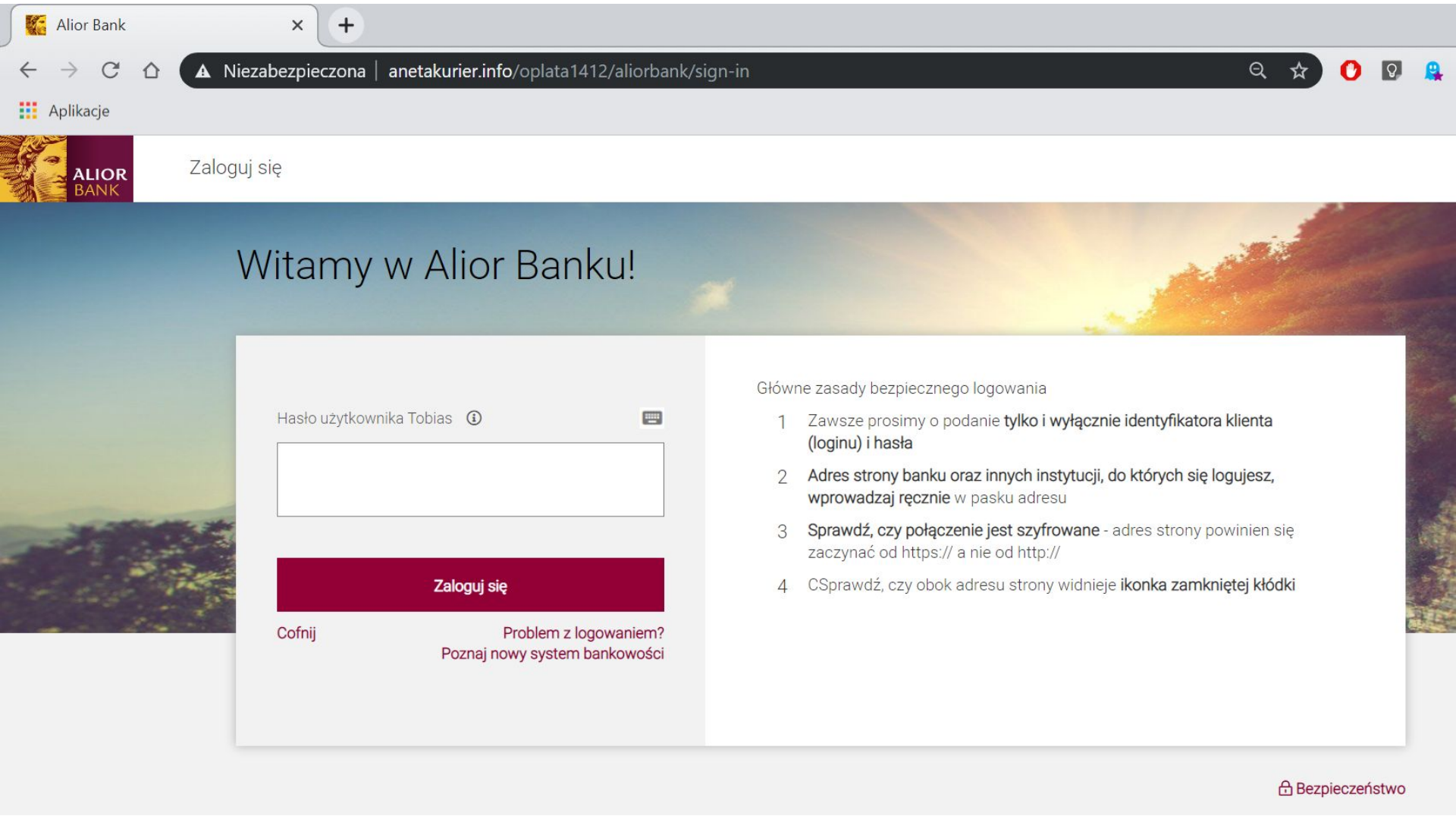
Dalej

Problem z logowaniem?
Poznaj nowy system bankowości

Sprawdź certyfikat

Pamiętaj o ochronie antywirusowej

Chroń swoje dane


Alior Bank
Niezabezpieczona | anetakurier.info/oplata1412/aliorbank/sign-in
Aplikacje
ALIOR BANK
Zaloguj się
Witamy w Alior Banku!
Hasło użytkownika Tobias
Zaloguj się
Cofnij
Problem z logowaniem?
Poznaj nowy system bankowości
Główne zasady bezpiecznego logowania
1 Zawsze prosimy o podanie tylko i wyłącznie identyfikatora klienta (loginu) i hasła
2 Adres strony banku oraz innych instytucji, do których się logujesz, wprowadzaj ręcznie w pasku adresu
3 Sprawdź, czy połączenie jest szyfrowane - adres strony powinien się zaczynać od https:// a nie od http://
4 CSprawdź, czy obok adresu strony widnieje ikonka zamkniętej kłódki
Bezpieczeństwo

Alior Bank

Niezabezpieczona | anetakurier.info/oplata1412/aliorbank/sign-in

Aplikacje

ALIOR BANK

Zaloguj się

Witamy w Alior Banku!

Enter SMS code to sign-in

This is one-time SMS code has been sent to your trusted phone number. After receiving code enter it below to sign-in.

Authorization with SMS code

Before typing in the SMS code and confirming the transation, please check the details in the message match the intended transation details. In case of a money transfer please check that the last few digits of the account number and amount are correct. If you find the details are incorrect, please contact our hotline at 19 502 (overseas +48 12 19 502) immediately

Enter SMS Code

Enter SMS code

Sign in

Back

Resend the SMS code

Download the following Documents

↓ Regulamin korzystania z Kanałów Elektronicznych dla Klientów Indywidualnych

Alior Bank

Niezabezpieczona | anetakurier.info/oplata1412/aliorbank/sign-in

Aplikacje

ALIOR BANK

Zaloguj się

Witamy w Alior Banku!

Enter SMS code to sign-in

This is one-time SMS code has been sent to your trusted phone number. After receiving code enter it below to sign-in.

Authorization with SMS code

Before typing in the SMS code and confirming the transation, please check the details in the message match the intended transation details. In case of a money transfer please check that the last few digits of the account number and amount are correct. If you find the details are incorrect, please contact our hotline at 19 502 (overseas +48 12 19 502) immediately

Enter SMS Code

665703

Sign in

Back

Resend the SMS code

Download the following Documents

Regulamin korzystania z Kanałów Elektronicznych dla Klientów Indywidualnych

Alior Bank

Niezabezpieczona | anetakurier.info/oplata1412/aliorbank/sign-in

Aplikacje

ALIOR BANK

Zaloguj się

Witamy w Alior Banku!

Enter SMS code to sign-in

This is one-time SMS code has been sent to your trusted phone number. After receiving code enter it below to sign-in.

Authorization with SMS code

Before typing in the SMS code and confirming the transation, please check the details in the message match the intended transation details. In case of a money transfer please check that the last few digits of the account number and amount are correct. If you find the details are incorrect, please contact our hotline at 19 502 (overseas +48 12 19 502) immediately

Enter SMS Code

665703

Sign in

Back

Resend the SMS code

Download the following Documents

Regulamin korzystania z Kanałów Elektronicznych dla Klientów Indywidualnych

Burp Suite Community Edition v2.1.02 - Temporary Project

Burp Project Intruder Repeater Window Help

Dashboard | Target | Proxy | Intruder | Repeater | Sequencer | Decoder | Comparer | Extender | Project options | User options

Intercept | HTTP history | WebSockets history | Options

Filter: Hiding CSS, image and general binary content

#	Host	Method	URL	Params	Edited	Status	Length	MIME t...	Extension	Title	Comment	SSL	IP	Cookies	Time	Listener port
82	http://anetakurier.info	POST	/oplata1412/loginApproval	✓									47.88.220.69		12:50:49 1...	8080
81	http://anetakurier.info	POST	/oplata1412/loginApproval	✓		200	1018	JSON					47.88.220.69	XSRF-TOKEN=...	12:50:47 1...	8080
80	http://anetakurier.info	POST	/oplata1412/loginApproval	✓		200	1018	JSON					47.88.220.69	XSRF-TOKEN=...	12:50:45 1...	8080
79	http://anetakurier.info	POST	/oplata1412/loginApproval	✓		200	1018	JSON					47.88.220.69	XSRF-TOKEN=...	12:50:43 1...	8080
78	http://anetakurier.info	POST	/oplata1412/loginApproval	✓		200	1018	JSON					47.88.220.69	XSRF-TOKEN=...	12:50:41 1...	8080
77	http://anetakurier.info	POST	/oplata1412/loginApproval	✓		200	1020	JSON					47.88.220.69	XSRF-TOKEN=...	12:50:39 1...	8080
76	http://anetakurier.info	POST	/oplata1412/loginApproval	✓		200	1020	JSON					47.88.220.69	XSRF-TOKEN=...	12:50:37 1...	8080
75	http://anetakurier.info	POST	/oplata1412/loginApproval	✓		200	1024	JSON					47.88.220.69	XSRF-TOKEN=...	12:50:35 1...	8080
74	http://anetakurier.info	POST	/oplata1412/loginApproval	✓		200	1018	JSON					47.88.220.69	XSRF-TOKEN=...	12:50:33 1...	8080
73	http://anetakurier.info	POST	/oplata1412/loginApproval	✓		200	1018	JSON					47.88.220.69	XSRF-TOKEN=...	12:50:31 1...	8080
72	http://anetakurier.info	POST	/oplata1412/loginApproval	✓		200	1014	JSON					47.88.220.69	XSRF-TOKEN=	12:50:29 1...	8080

Request | Response

Raw | Params | Headers | Hex

```
POST /oplata1412/loginApproval HTTP/1.1
Host: anetakurier.info
Content-Length: 138
Accept: application/json, text/javascript, */*; q=0.01
Origin: http://anetakurier.info
X-Requested-With: XMLHttpRequest
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/77.0.3865.75 Safari/537.36
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
Referer: http://anetakurier.info/oplata1412/aliorbank/sign-in
Accept-Encoding: gzip, deflate
Accept-Language: pl-PL,pl;q=0.9,en-US;q=0.8,en;q=0.7
Cookie:
XSRF-TOKEN=eyJpdiI6InA5Qm1pTGR3ZnhCZFN5MnR2Zzk2N2c9PSIsInZhbHVlIjoiRDdDYk83QzhERWUxZGR3ZTRONGxoc2QxMTlKcVlXSU9MbkhxWWt2eVwvM0k5VndGS0NWd0ZYV0ExTUhldXJieXliLCJtYWMiOiJlNDcwOGM4MTA1MzNkYmZmMjEzYzhlNmM0OTRiMzQyNzA1YWNlMDC
ZTI2In0%3D;
laravel_session=eyJpdiI6IjF1K0IwU3F6eVRnZU1vOGJ4MTNQanc9PSIsInZhbHVlIjoiS2piQm42UDhJdVQ2Wk8xTlVadFpTbUp5U2dNRUtvSmNKa3F3RnJBOVdxY1I3V241XC9YMU9IOTVob2VsZVVoNWUiLCJtYWMiOiIwZDEwNWY3ZGFmODFiZmM5MGQ0MWI3YTRlYjAxNTdmZjIxMTgzYzg0Nn
OTJkIn0%3D
Connection: close

_token=B9V9CVKrCOTrlPVqljhV2QhX2BBVL9f4y03HWfi0&paymentType=Alior+Bank&contactType=User+ID&redirectNext=aliorIndiStruck&email=&u_password=
```

```
HTTP/1.1 200 OK
Server: nginx
Date: Wed, 18 Sep 2019 11:00:00 GMT
Content-Type: application/json
Connection: close
Vary: Accept-Encoding
Vary: Accept-Encoding
Cache-Control: no-cache, private
Set-Cookie:
XSRF-TOKEN=eyJpdiI6Im5JdmFseGJ5WDJ3Mmw1aFJXaGtuY1E9PSIsInZhbHVlIjoiMVlIVmx5OERMRjBIY3YwckpIdWpDa
U2YTcifQ%3D%3D; expires=Wed, 18-Sep-2019 12:59:59 GMT; Max-Age=7200; path=/
Set-Cookie:
laravel_session=eyJpdiI6Ijh4SFVIcTc0b0J2dzRranpiN1NjNEE9PSIsInZhbHVlIjoibVBIYzlRMkc3QjNGQzA4N3Q4QmV3dVE3
FIln0%3D; expires=Wed, 18-Sep-2019 12:59:59 GMT; Max-Age=7200; path=/; httponly
X-XSS-Protection: 1; mode=block
X-Content-Type-Options: nosniff
X-Server-Powered-By: Engintron
Content-Length: 19

{"msg":"keepStuck"}
```


BRACE YOURSELF
WINTER IS COMING
quickmeme.com

Co nas czeka?

Forbes Billionaires Innovation Leadership

23,361 views | Sep 3, 2019, 04:42pm

A Voice Deepfake Was Used To Scam A CEO Out Of $243,000

Jesse Damiani Contributor ⓘ
Consumer Tech
I cover the human side of VR/AR, Blockchain, AI, Startups, & Media.

ScienceAlert Trending

TECH

Unnerving Chinese Deepfake App Lets You Replace Celebrity Faces With Your Own

BI ISOBEL ASHER HAMILTON, BUSINESS INSIDER
3 SEP 2019

*source:*https://www.forbes.com/sites/jessedamiani/2019/09/03/a-voice-deepfake-was-used-to-scam-a-ceo-out-of-243000/#54ebc8f02241

Jak zareagują banki?

- Będą starały się edukować klientów

PHISHING STOP
BY ALIOR BANK

NAUKI MISTRZA BAN-KING:

Przestępcy nie włamują się do banku. Oni włamują się do Twojego komputera.

PKO BP: nadchodzi „Bitwa o Neta", gra edukacyjna z zakresu cyberbezpieczeństwa

Bezpieczne Finanse / Bezpieczny Klient / Z rynku

14.10.2019 19:00| Autor: awi, aleBank.pl

Source: https://alebank.pl/pko-bp-nadchodzi-bitwa-o-neta-gra-edukacyjna-z-zakresu-cyberbezpieczenstwa/

Jak zareagują banki?

- Będą starały się edukować klientów
- Będą wdrażały i rozwijały systemy FDS
- Będą wdrażały dodatkowe mechanizmy (biometrię behawioralną)
- Będą świadczyły dodatkowe usługi (???)
    - Cyber Threat Inteligence
    - Symulowane kampanie phishingowe na klientów
- …

Czytaj ucz się, bez tego jesteś słaby…

Sokół - Orientuj się

Polska youtuberka okradziona. Oszuści wyczyścili jej konto z oszczędności

Nie wierzcie we wszystkie oferty, jakie znajdziecie w internecie. Jedna z nich, która zainteresowała być pułapką, przez którą kobieta została okradziona na ponad 3000 zł. Jak do tego doszło?

10:56

Vinted

Forum ▾ Szukaj na forum

Strona główna ▸ Forum ▸ NIE MÓW NIKOMU, ALE... ▸ Okradziona w ciazy

Okradziona w ciazy

« 1 2 3 4 5 »

na stronie: 20 50 100

(anonimowy) 3 dni temu

Bardzo proszę o pomoc, jestem w 6 miesiącu ciąży. Zawsze zylam dość skromnie i biednie. Z anonim bo mi wstyd... Ostatnio sytuacja mnie przycisnela i zylam jeszcze skromniej. Miałam odlozone na koncie 5 tys, zaczęłam wyprawkę dla dziecka, wczoraj na fb dałam się nabrać, miałam odkupić ciuszki za koszt przesyłki. Nie znam się na informatyce, zrobiłam przelew na 15 zł na kuriera... Dziś o 12 okazało się że moje konto jest wyczyszczone... Byłam na policji i w banku, wszystko zgłoszone mam czekać... Siedzę i płacze cały dzień 😔 proszę o pomoc

Lubię!

+1 sherlock.holmes

kukulka20 706 3 dni temu

Wchodziłaś w jakiegoś linka?

Lubię! (16)

(anonimowy) 3 dni temu

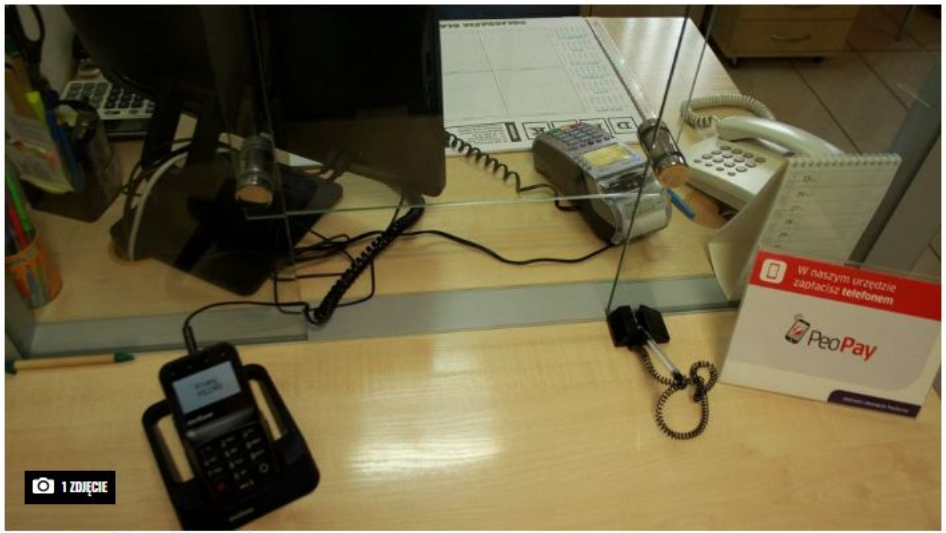
Tak. Ale potwierdzam płatność na 15 zł tylko. Były tam dane

Konsekwencje

policja

Oszustwo "na BLIK-a". Tylko w Płocku pieniądze straciło kilkadziesiąt osób

Milena Orłowska 6 września 2019 | 11:56



Policja ostrzega (Fot. Maciej Bednarek)

NAJCZĘŚCIEJ CZYTANE

Ankieta dla Czytelników na 30-lecie "Gazety Wyborczej"

PŁOCK
Szpital Św. Trójcy w Płocku. Przenosiny detoksu, mniej łóżek na psychiatrii

PŁOCK
Zaczynają się remonty kolejnych płockich ulic, będzie nowa trasa rowerowa. Co mają z tym wspólnego posłowie?

(fot. YAY Foto)

Straciła przez oszustów 9 tys. zł. Bank odrzuca reklamację

Wojciech Boczoń
2019-03-11 06:00

Opisywany przez nas przypadek klientki, która, chcąc dopłacić do faktury 3 zł, straciła 9 tys. zł nie ma szczęśliwego finału. Bank odrzucił jej reklamację, twierdząc, że nie doszło do włamania na konto.

SMS z prośbą o dopłatę i fałszywi znajomi z Facebooka – to dwie metody, które bezlitośnie zbierają żniwo wśród klientów banków. Kilka dni temu opisywaliśmy przypadek klientki, która dostała SMS-a rzekomo od firmy telekomunikacyjnej z prośbą o dopłatę do rachunku 3 zł. "Zaległość w fakturze telekomunikacyjnej. Prosimy o dopłatę 3 zł do dnia 27.01.2019 lub Twój numer zostanie zablokowany https://payu.oplaty.eu(...)". W treści wiadomości znajdował się link kierujący na podrobioną bramkę płatniczą. Wpisała tam dane logowania do swojego banku, a złodzieje wyprowadzili z jej konta 9 tys. zł.

Banki negatywnie rozpatrują reklamacje

W odpowiedzi na złożoną reklamację bank odpisał, że nie doszło do naruszenia sieci teleinformatycznej, a klient zlecił przelew dobrowolnie. Tym samym nie ma pods
sam

Pytania?

kontakt@wiktorszymanski.pl

@wikszymans

Bezpieczny.blog