

NoSuchMeetup
28.10.2019

Ewolucja phishingu i socjotechniki oraz ich wpływ na sektor bankowy

Wiktor Szymański

kontakt@wiktorszymanski.pl 

[@wikszymans](https://twitter.com/wikszymans) 

Who am I?



Wiktor Szymański

DBE @ Alior Bank

kontakt@wiktorszymanski.pl

[@wikszymans](https://twitter.com/wikszymans)

[@bezpiecznyblog](https://twitter.com/bezpiecznyblog)

Bezpieczny.blog



Long time ago in a galaxy far, far away...

15 years

ago

- 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 assist me for more details.

Your urgent response will be appreciated.

Talk to you the more sincerely.

Regards Mis.Zalanda Mubarak

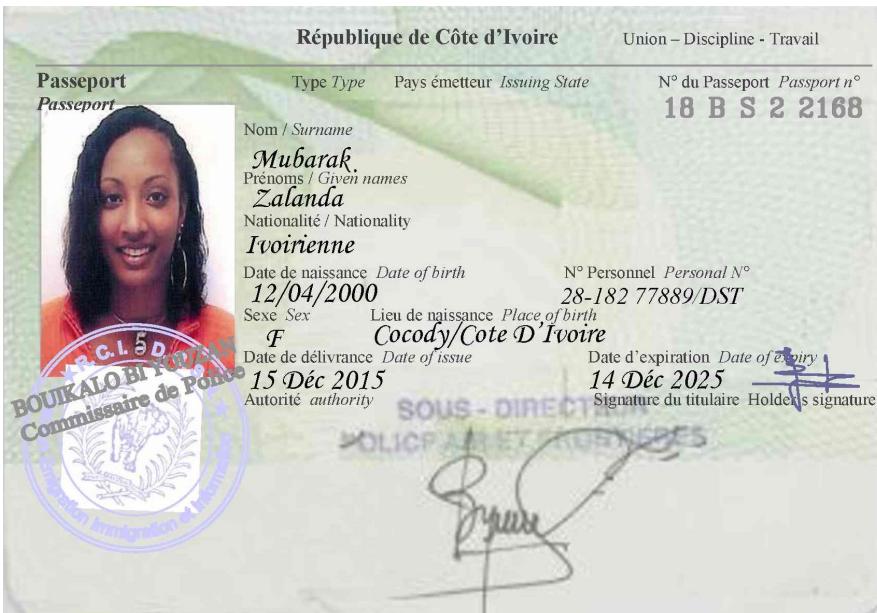


This is what happens when you reply to spam email | James Veitch

TED 43 mln wyświetleń • 3 lata temu

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

napisy



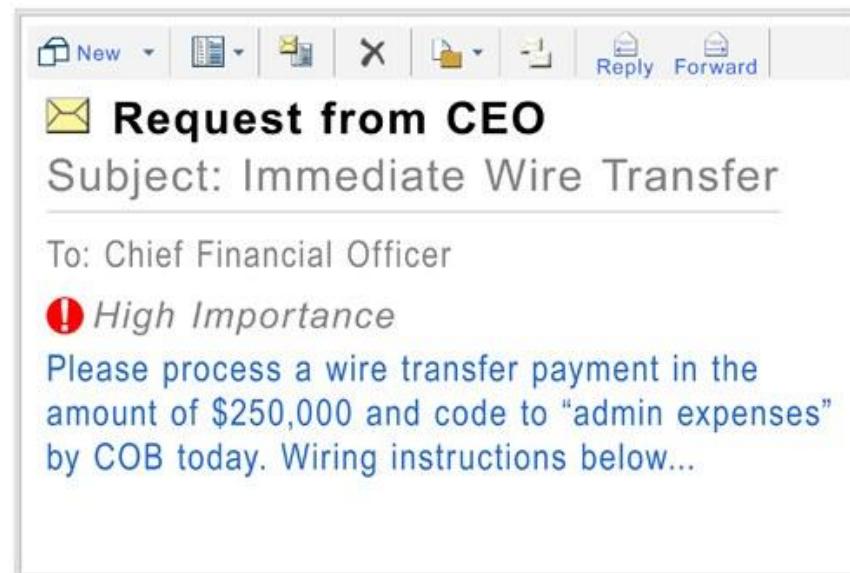
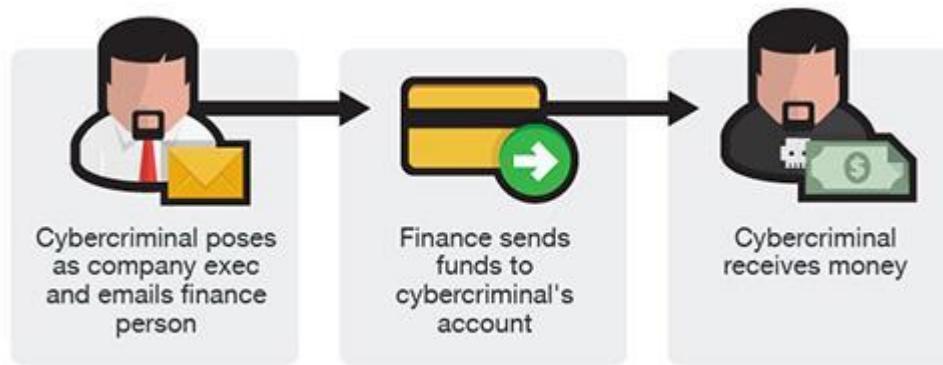
 rescam.org

After sending
1,012,531 emails

and wasting more than
5 years of scammers' time,

I'm currently offline while Phase II is being tested for launch.

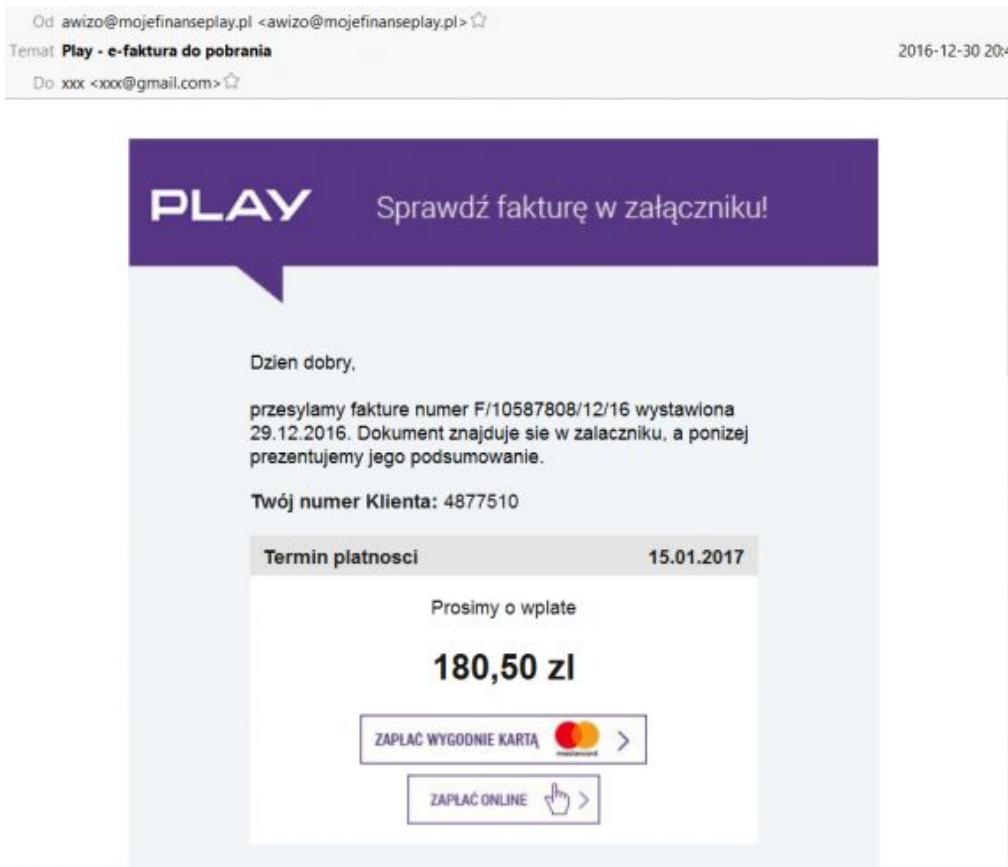
Business e-mail compromise (BEC)



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->

Casual Phishing



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

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.

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 wręczyć ;-).  W tym badaniu pokazano podatne systemy PACS (Picture Archiving and Communication Systems) rozsiane po całym świecie. Wyniki są zatrważające:

 **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



Report: Smart Home Manufacturer Leaks Billions of Records



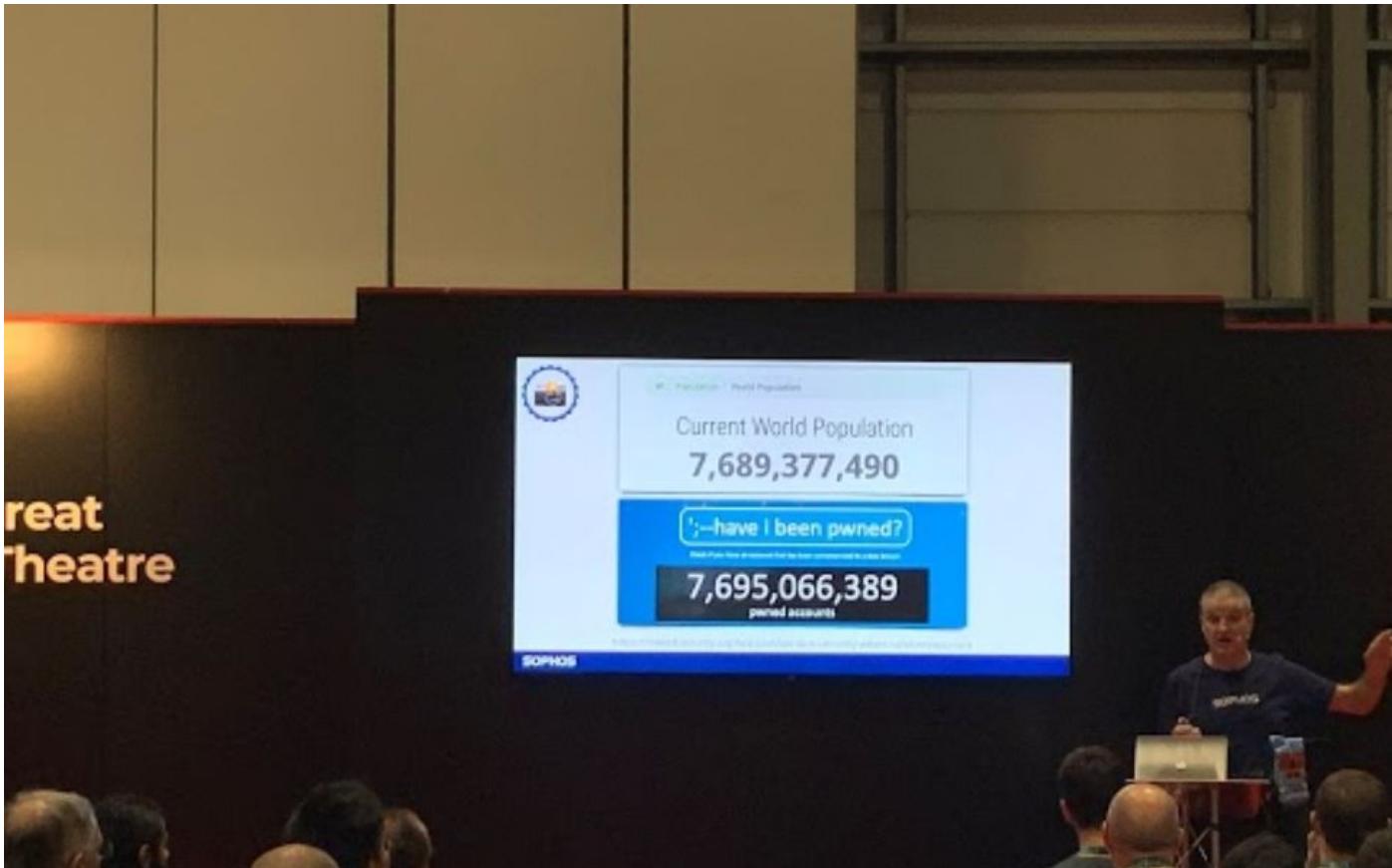
Krypto Mobilne Prawo Prywatność Wpadki Włamania Złożniki SZKOLENIA

Zaufana Trzecia Strona

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

Najlepsze w tym
Jak bankowi złodzieje zmian w logowaniu

Jak to jest możliwe?



Wektory ataku



Direct contact



Text messages



Phone call



Social media



Traditional mail



E-mail



Online services

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 possibility to become a Member of the Royal Warrant Holders Association.

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.

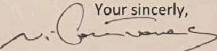
We want this letter to remain anonymous as we do not wish the subject to go viral. This could affect the agreements we have in order to obtain the bilateral agreement.

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 will 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



Your sincerely,


Edward Young
Private Secretary to HM the Queen Elizabeth II

Mr. Ridden

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's 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
- ...



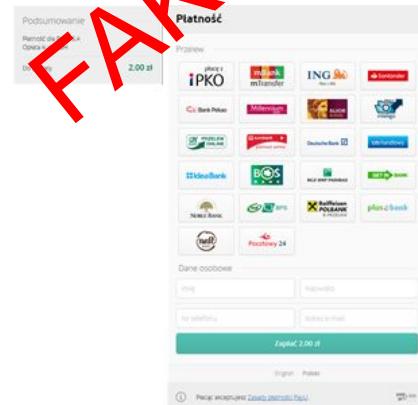
Socjotechnika

czyli hakujemy człowieka, a nie komputer...

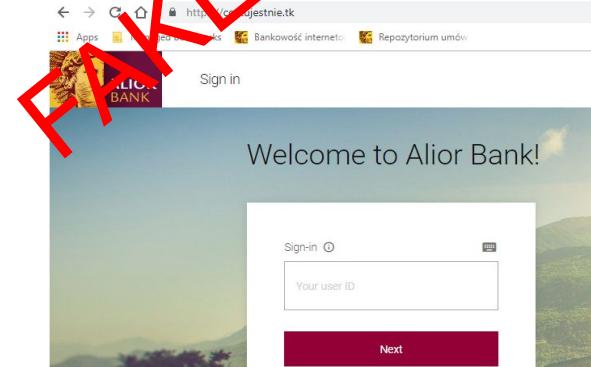
1.

Fałszywa strona
Prawdziwa strona
E-mail
SMS
Socialmedia

2.



3.





Socjotechnika

Fałszywy sklep

→ ⌛ ⌂ ⓘ Niezabezpieczona | stylishsunglass.co

WELCOME TO STYLISH SUNGLASS 100% AUTHENTIC. SECURE SHOPPING. EASY RETURNS. CURRENCY € £ \$ MY ACCOUNT CHECKOUT

AUTHENTIC GLASSES INTEGRATED STATION WE SHIP WORLDWIDE

 **STYLISHSUNGLASS**

Search...

BRANDS HERS HIS FRAME SHAPE LIFESTYLE

100% AUTHENTIC. SECURE SHOPPING. EASY RETURNS. WELCOME TO STYLISH SUNGLASS

OUR FAVORITE SHADES



RAY BAN AVIATOR OUTDOORSMAN II RB3407 001/3K

OUR PRICE \$99.83

SALE PRICE \$28.99



RAY BAN AVIATOR OUTDOORSMAN SUNGLASSES RB3422Q 004/52

OUR PRICE \$99.83

SALE PRICE \$28.99



OAKLEY 03-909 FLAK JACKET XLJ POL BLK W/

OUR PRICE \$96.90

SALE PRICE \$26.98



Socjotechnika

Fałszywy sklep + fałszywa strona z opiniami

The screenshot shows the header of the Opineo.pl website. A red box highlights the URL 'opi neo.pl' in the address bar. Below it, the Opineo logo is displayed, followed by navigation links for 'E-SKLEPY', 'PRODUKTY', and 'FIRMY'. A search bar with the placeholder 'Szukaj E-sklepu lub Firmy' and a magnifying glass icon is also visible. On the far right, there are buttons for '+ DODAJ' and a user profile icon.

Opineo.pl > CREATIVE IMPACT

Nie przepłacaj!

Porównaj oferty polis i **ubezpiecz swoją nieruchomości** już od 89 zł rocznie

[Sprawdź oferty →](#)



przewodnik
ubezpieczeniowy



Obecnie **CREATIVE IMPACT** wyjaśnia ze swoimi klientami reklamacje w OpiConnect.
Ilość trwających reklamacji: 14

CREATIVE IMPACT

99% Klientów poleca ten sklep

4.9 ★★★★★

6 540 opinii

Historia ocen: 12 miesięcy



Socjotechnika

Fałszywy sklep + prawdziwa strona z opiniami

The screenshot shows the top navigation bar of Opineo.pl. It features a logo with a green checkmark icon followed by the text "OPINEO.pl". To the right are four main categories: "E-SKLEPY", "PRODUKTY", and "FIRMY", each with a dropdown arrow. A search bar on the far right contains the placeholder text "Szukaj E-sklepu lub Fir".

Opineo.pl > Lokikoki.pl

KlawySklep.pl



5 ★★★★★ 3 213 opinii

- 4.9 ★★★★★ Szybkość realizacji zamówienia
- 5 ★★★★★ Poziom obsługi klienta
- 4.9 ★★★★★ Jakość zapakowania przesyłki
- 5 ★★★★★ Polecił(a)bym ten sklep znajomym

<https://klawysklep.pl>

CERTYFIKATY



Kategorie: AGD | Zdrowie | Uroda



Socjotechnika

Fałszywy sklepy + prawdziwe płatności

Zawartość koszyka

Laptop Apple MacBook Air 13 Intel® Dual Core™ i5 1,8GHz, 13,3", 8GB, 128GB SSD, Intel® HD Graphics 6000, ROM KB, Silver

Cena (1 szt.): 4 599,00 PLN
Ponadanie: 2 699,10 PLN

Metoda dostawy: Kurier DHL

Kraj dostawy: Polska

● Kurier DHL 0,00 PLN

○ Kureir Inpost 0,00 PLN

Metoda płatności: Szybkie Płatności Payu

● Szybkie Płatności Payu

Wsparcie
Zapytaj o cokolwiek

Vitam i Panie, wysyłam okrą w Pan zamówieniach, prosimy złożyć je ponownie, a stare zostaną anulowane, prosimy o złożenie ponownie zamówienia za pół godziny - działa techniczny już naprawia błęd

Ja 10:22
Witam, czy płatność będzie przez payu czy przelew bankowy?

Wsparcie 10:22
platność jest przez payu

Wsparcie pisze...

Napisz tutaj, wciśnij Enter, aby wysłać

Powered by Smartsupp Wyślij

MIH PayU B.V. [NL] https://secure.payu.com/pay/?orderId=5L3SZHDVX7190610GUEST000P01

Podsumowanie

Płatność dla www.neonet.pl

Do zapłaty 3997.99 zł

Zmień walutę

Aby uniknąć kosztów przewalutowania, wybierz metodę płatności w walucie swojej karty.

Karta

Numer karty

Ważna do MM/RRRR CVV

Adres e-mail qulik.sc@wp.pl

Zapłać 3997.99 zł

LUB

G Pay Google Pay

Wybierz inną metodę płatności

Placąc akceptujesz [Zasady płatności Payu](#)

paySSL

źródło: <https://zaufanatrzeciastrona.pl>

Socjotechnika

Prawdziwe usługi + fałszywe smsy



Szukany produkt...

wszystkie działy



Konfigurator PC

Alarm Cenowy

Wyprzedaż

Karta Podarunkowa

Outlet

KATEGORIE ▾

Uwaga na SMSy

Morele.net / Wszystkie artykuły / Promocje i konkursy / Uwaga na SMS-y proszące o dopłatę 1 PLN do zamówienia w sklepach Grupy Morele.

Uwaga na SMS-y proszące o dopłatę 1 PLN do zamówienia w sklepach Grupy Morele.

Otrzymaliśmy od Państwa niepokojące informacje o smsach, które przychodzą na Państwa nr telefonów, w których są Państwo nakłaniani do zapłaty dodatkowej kwoty (w dotychczasowych przypadkach smsy mówiły o kwocie 1 PLN) do złożonego zamówienia w sklepach GRUPY MORELE.

Informujemy, że nie jesteśmy nadawcą tych smsów i jest to prawdopodobnie próba oszustwa i wyłudzenia.

Nigdy nie wysyłamy smsów do Klientów z prośbą o dopłatę do zamówienia. Nie wysyłają ich również w naszym imieniu firmy kurierskie, ani żadne inne, związane z nami podmioty. Najprawdopodobniej jest to próba wyłudzenia pieniędzy. Bardzo prosimy o ignorowanie ich oraz w żadnym wypadku nie klikanie w link wysyłany smsem.

OTOMOTO

piątek, 1 lutego 2019

Twoje konto w serwisie OTOMOTO zostało zablokowane. Oplac zaledwie 0.76 PLN, by ponownie aktywować ogłoszenia - <https://tinyurl.com/kontoOTOMOTO>

12:32

czwartek, 8 listopada 2018

Wysyłka pod wskazany adres jest drozsza.
Prosimy dopłacić 1PLN,
brak dopłaty oznacza anulowanie zamówienia.
<http://pm.tk/uy63CI/1>

10:32



Socjotechnika

Vishing



Uslugi Finansowanie dla firm Konta Oszczędności



Kontakt



Zaloguj

Ostrzeżenie przed nowym rodzajem cyberataków na klientów!

Bank zidentyfikował nowy sposób działania przestępcołów 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 przestępcaًmi:

1. Pamiętaj, NIE PODAWAJ NIKOMU haseł do bankowości ani kodów jednorazowych, które otrzymujesz w momencie dokonywania transakcji w bankowości.
2. Bank NIGDY nie просi o podanie haseł jednorazowych ani haseł do bankowości.
3. Bank NIGDY nie просi 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, podszywając 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

OLX Global B.V. [NL] | <https://www.olx.pl/oferta/duze-klocki-IDxDQy4.html#Id00s<12>

 Mój OLX + DODAJ OGŁOSZENIE

< Wróć Ogłoszenia Warszawa > Dla Dzieci Warszawa > Zabawki Warszawa Następne ogłoszenie >





Za darmo

Napisz wiadomość

Warszawa, Mazowieckie, Targówek
Pokaż na mapie

Agnieszka
Na OLX.pl od ██████████

Ogłoszenia użytkownika

Zgłoś naruszenie

Duże klocki
Warszawa, Mazowieckie, Targówek | Dodane z telefonu o ██████████ listopada 2018,
ID ogłoszenia: 49712572



Socjotechnika

Konto w serwisie aukcyjnym

https://allegro.pl/dron-sportowy 80% ... ☆ Szukaj

allegro czego szukasz? Drony SZUKAJ ☆ Moje Allegro

Kategorie Sprawdź allegroSMART! Okazje do -70% Hity z reklamy Promocje z Monetami Inspiracje Artykuły STREFĄ RO >

Allegro - Kolekcje i sztuka - Kolekcje - Modelarstwo - Zdalnie sterowane - Lotnicze - Drony

OBSERWUJ Dron Sportowy WALKERA Rodeo 110 BNF od Super Sprzedawcy Aktualna cena 107,50 zł Cena minimalna nie została osiągnięta 8 osób liczytuje 100,0% poleca sprzedawcę 24 godziny czas wysyłki 11,00 zł najtańsza dostawa na odstąpienie od umowy OPCJE DOSTAWY ▾ Twoja oferta 110 zł 7 dni do końca licytacji



Socjotechnika

Konto w serwisie społecznościowym

Aktualności • POLITYKA • SPORT • PIŁKA NOŻNA • SLAWNI LUDZIE • TELEWIZJA I FILM • DZIWNIE AKTUALNOŚCI • WIĘCEJ •

Home • Aktualności • Polska

Porwanie w centrum Handlowym "złote tarasy" Policja publikuje wideo z porwania i prosi o pomoc

„Kryminalni prowadzą dochodzenie w sprawie uprowadzenia 8 letniej dziewczynki w Warszawie. Opublikowali portret pamięciowy podejrzanego mężczyzny i monitoring z zajścia. Porusza się on ciemnym samochodem marki Seat Leon. Jeżeli ktoś go rozpozna z nagrania prosimy o kontakt z najbliższym komisariatem”

Autor: Katarzyna Piatek
SRODA WRZESIEN 4, 2019



Dramatyczne wydarzenia rozegrały się 26 sierpnia. Policja opublikowała nagranie z monitoringu. Około godz. 12:30 W galerii handlowej Złote tarasy przy ul. Złotej, Niezidentyfikowany mężczyzna podszedł do 8 latki.

WIADOMOŚCI

- na żywo** Katastrofa indonezyjskiego samolotu pasażerskiego. Na pokładzie było ponad 180 osób
- MON wystaje ponad 500 mln rocznie na ochronę
- Beata Szydło o kolizji kolumny rządowej
- W. Brytania: Polka zgłębiła w katastrofie smigłowca
- Strajk w LOT: Rozmowy związków z zarządem
- “Tropikalny Trump” wygrywa wybory w Brazylii
- Podkarpackie: poseł PiS potrącił dwóch nastolatków
- Ostre słowa Liroya. “To straszne. Obudźcie się”
- Jurasz: geopolityka czyli przekaz rodem z Kremla?

TYTUŁ W DÓŁ Sędzia Łyczeński ponagliła premiera. Nie będzie odpowiedzi – będzie pocew

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

Socjotechnika

Konto w serwisie społecznościowym



Cześć, mam dużą prośbę do Ciebie...

Słucham?

Głupia sprawa 😢 Nie mam pieniędzy na koncie i brakuje mi na zakupy. Jestem pod ścianą. Czy możesz mi wypłacić pieniądze Blikiem? Oddam Ci w piątek jak dostanę przelew

A w jakim banku masz? Bo szczerze mówiąc Blikiem nigdy nie płaciłem ani nie przelewałem

To łatwiejsze niż przelew. Musisz wejść na telefon na aplikację swojego banku i tam możesz wygenerować kod blik, a potem podasz mi te 6 cyfr

Rzeczywiście łatwe 890 385

Czy to wszystko?

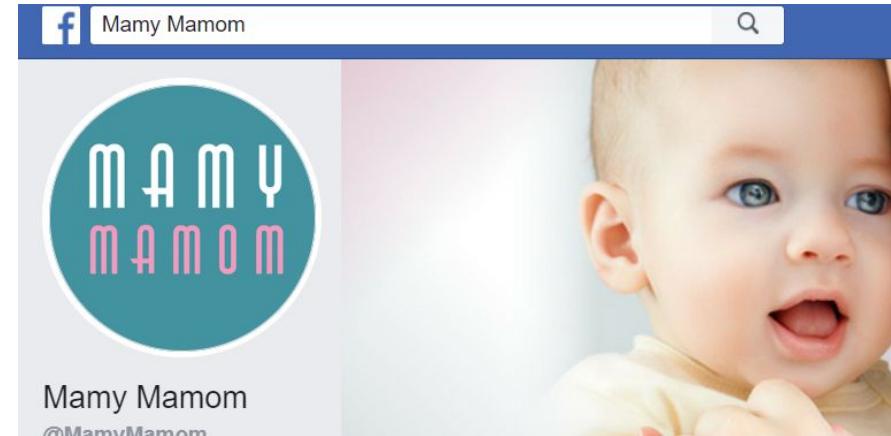
Super, musisz jeszcze potwierdzić w aplikacji

zaakceptowałem



Socjotechnika

Konto w serwisie społecznościowym



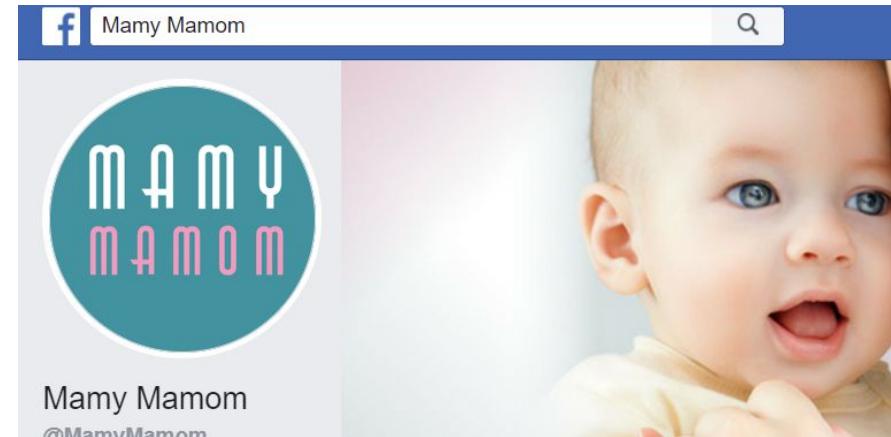
Czyli wszystko dobrane? Jak mogę zapłacić?

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



Socjotechnika

Konto w serwisie społecznościowym



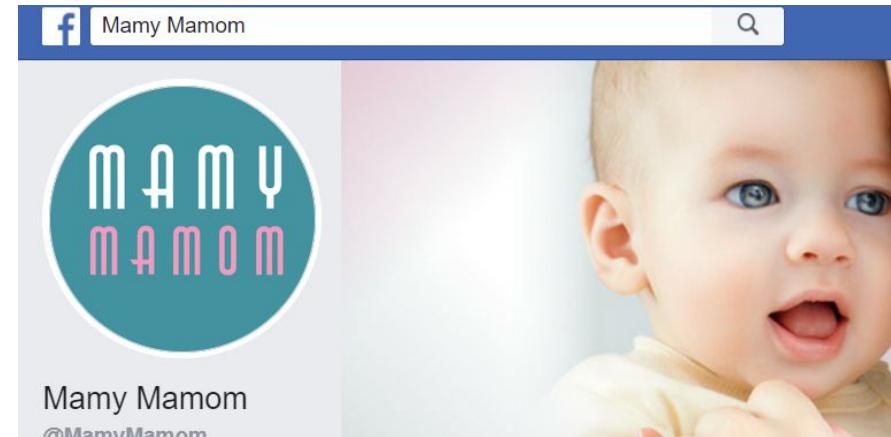
Czyli wszystko dobrane? Jak mogę zapłacić?

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



Socjotechnika

Konto w serwisie społecznościowym



Czyli wszystko dobrane? Jak mogę zapłacić?

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



Fałszywi pośrednicy płatności

Informacja o płatności:

Odbiorca: ja Kwota: **22 PLN**

Opis: ja

Wybrany kanał płatności:

Karty płatnicze	Szybkie transfery



Fałszywi pośrednicy płatności

The image shows a woman smiling while sitting at a desk with a computer monitor. A payment interface for 'PayU' is overlaid on the screen. The interface includes a summary box showing a payment of 2.00 zł from 'iPKO' to 'PayU S.A.' and a delivery fee of 0.50 zł from 'DHL'. Below this is a large 'Płatność' button. To its left is a grid of payment method logos, including iPKO, mBank, ING, Santander, Bank Pekao, Millennium, Allianz BANK, inteligo, PRZELEW ONLINE, eurobank, Deutsche Bank, citi handlowy, IdeaBank, BOS BANK, BGŻ BNP PARIBAS, GETIN BANK, NOBLE BANK, BPS, Raiffeisen POLBANK, plus ebank, nest, and Pocztyowy 24. At the bottom of the interface are fields for 'Imię' (Name), 'Nazwisko' (Surname), 'Nr telefonu' (Phone number), 'Adres e-mail' (Email address), and a large green 'Zapłać 2.00 zł' (Pay 2.00 zł) button. Below the button are language links for 'English' and 'Polski'. At the very bottom, there is a note about accepting PayU's terms and conditions and a small logo.

Podsumowanie

Płatność dla PayU S.A
Opłata kurier DHL

Do zapłaty 2.00 zł

Płatność

Przelew

Do zapłaty 2.00 zł

Administratorem Twoich danych osobowych jest PayU S.A. z siedzibą w Poznaniu (60-168) przy ul. Grunwaldzkiej 182 („PayU”). Twoje dane osobowe będą przetwarzane w celu realizacji transakcji pieniężnej, powiadomienia Cię o statusie realizacji Twojej płatności, rozpatrywania reklamacji, a także w celu wypierania obowiązków prawnych ciągłyco na PayU.

Strona korzysta z plików cookies w celu realizacji usług zgodnie z [Polityką Plików Cookies](#). Możesz określić warunki przechowywania lub dostępu do plików cookies w swojej przeglądarce.



Fałszywi pośrednicy płatności

← → ⌛ ⌂ https://costujestnie.tk

Sign in

Welcome to Alior Bank!

Sign-in ⓘ

Your user ID

Next



Fałszywi pośrednicy płatności

The screenshot shows a web browser window with a redacted URL bar containing `https://costujestnie.tk`. The main content is a仿冒的Alior Bank login page. It features the Alior Bank logo (a golden profile of Medusa) and a "Sign in" button. A large banner in the background says "Welcome to Alior Bank!". A central sign-in form has a redacted input field for "Your user ID". A redacted "Next" button is at the bottom of the form.

← → ⌛ ⌂ https://costujestnie.tk

ALIOR BANK

Sign in

Welcome to Alior Bank!

Sign-in ⓘ

Your user ID

Next



Fałszywi pośrednicy płatności

← → C ⌂



<https://costujestnie.tk>

Sign in

Welcome to Alior Bank!

Enter password for OWASP_2018 ⓘ ⌂

1	2	3	4	5	6	7	8	9	10	11	12
---	---	---	---	---	---	---	---	---	----	----	----

Next



Fałszywi pośrednicy płatności

← → ⌂ ⌄ https://costujestnie.tk

ALIOR BANK

Sign in

Welcome to Alior Bank!

Enter password for OWASP_2018 ⓘ

1	2	3	4	5	6	7	8	9	10	11	12

Next



Fałszywi pośrednicy płatności

← → ⌛ ⌂ https://costujestnie.tk

Welcome to Alior Bank!

Enter password for OWASP_2017

*	*	*	*	*	*	*	*	*	*	*	*
1	2	3	4	5	6	7	8	9	10	11	12

Sign in



Fałszywi pośrednicy płatności

The screenshot shows a web browser window with a dark-themed background image of a landscape. At the top, the address bar displays "Dangerous | https://orange-windykacja-dotpay.info/store/.../token/". The page itself has a header with the Alior Bank logo and a "Zaloguj się" button. The main content area is titled "Weryfikacja" and contains a message "Proszę czekać". Below this, there is placeholder text "Lorem ipsum dolor Lorem ipsum dolor Lorem ipsum dolor Lorem ipsum dolor Lorem ipsum dolor...". In the center of the page is a red circle containing the time "1:41". At the bottom, there is a link "Więcej informacji dotyczących bezpieczeństwa" and a language selection "Polski". A watermark "fot. niebezpiecznik.pl" is visible in the upper right of the page content.

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



Fałszywi pośrednicy płatności

← → ⌛ ⌂ https://costujestnie.tk

Welcome to Alior Bank!

Enter password for OWASP_2017

*	*	*	*	*	*	*	*	*	*	*	*
1	2	3	4	5	6	7	8	9	10	11	12

Sign in



Fałszywi pośrednicy płatności

The screenshot shows a web browser window with the URL <https://costujestnie.tk>. The page is designed to look like a payment interface for Alior Bank. It features the Alior Bank logo (a golden Medusa head) and the text "Płacę z Alior Bankiem". The background image is a scenic view of mountains and hills under a clear sky.

Z rachunku

Konto Wyższej Jakości 51 2490 ... 0120	1 664,10 PLN
---	--------------

Odbiorca
Dotpay S.A
ALIOR Centralna 70 2000 0001 0000 4000 5555 1111
[Pokaż adres](#) ▾

Kwota
22,00 PLN

Tytuł przelewu
DotPay XX122777400XX Kurier

[Wyślij potwierdzenie na adres e-mail](#)

Anuluj Wyślij przelew



Fałszywi pośrednicy płatności

The screenshot shows a web browser window with the URL <https://costujestnie.tk> highlighted by a red box. The page content is as follows:

Płacę z Alior Bankiem

Z rachunku

Konto Wyższej Jakości 51 2490 ... 0120	1 664,10 PLN
---	--------------

Odbiorca
Dotpay S.A.
ALIOR Centrala 70 2000 0001 0000 4000 5555 1111
Pokaż adres ▾

Kwota
22,00PLN

Tytuł przelewu
DotPay XX1227777400XX Kurier

Wyślij potwierdzenie na adres e-mail

Anuluj Wyślij przelew

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

The screenshot shows a web browser window with the URL <https://costujestnie.tk> highlighted by a red box. The page content is as follows:

Płacę z Alior Bankiem

Z rachunku

Konto Wyższej Jakości 51 2490 ... 0120	1 664,10 PLN
---	--------------

Odbiorca
Dotpay S.A.
ALIOR Centrala 70 2000 0001 0000 4000 5555 1111
Pokaż adres ▾

Kwota
22,00PLN

Tytuł przelewu
DotPay XX1227777400XX Kurier

Wyślij potwierdzenie na adres e-mail

Anuluj Wyślij przelew

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**



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





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



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



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 transaction, please check the details in the message match the intended transaction 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

Sign in[Back](#)[Resend the SMS code](#)

Download the following Documents

[↓ Regulamin korzystania z Kanałów Elektronicznych dla Klientów Indywidualnych](#)



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 transaction, please check the details in the message match the intended transaction 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](#)



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 transaction, please check the details in the message match the intended transaction 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](#)

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=eyJpdii6lnA5Qm1pTGR3ZnhCZFN5MnR2Zzk2N2c9PSlslnZhbHViIjoiRDdDYk83QzhERWUxZGR3ZTRONGxoc2QxMTIKcVIXSU9MbkhxWWWt2eVvwM0k5VndGS0NWd0ZY0ExTUhdXJieXilCJtYWMiOijNDcwOGM4MTA1MzNkYmZmMjEzYzhNmM0OTriMzQyNzA1YWNIMDZTl2In0%3D; laravel_session=eyJpdii6ljF1K0lwJ3F6eVRnZU1vOGJ4MTNQanc9PSlslnZhbHViIjoiS2piQm42UDhJdVQ2Wk8xTIVadFpTbUp5U2dNRUtvSmNKa3F3RnJBOvdxY1I3V241XC9YMU9lOTVob2VsZvv0NWUiLCJtYWMiOiwZDEwNWY3ZGFmODFiZmM5MGQ0MWi3YTRlYjAxNTdmZlxMTgZygzgONnOTJkh0%3D;

Connection: close
_token=B9V9CVKrCOTriPVqjhV2QhX2BBVL9f4y03HWfi0&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=eyJpdil6lm5JdmFseGJ5WDJ3Mmw1aFJXaGtuY1E9PSIsInZhbHVljoiMVIIVmx5OERMRjBIY3YwckpldWpDaI
U2YTcifQ%3D%3D; expires=Wed, 18-Sep-2019 12:59:59 GMT; Max-Age=7200; path=/

Set-Cookie:

laravel_session=eyJpdil6jh4SFVlcTcOb0J2dzRranpiN1NjNEE9PSIsInZhbHVljoibVBIYzIRMkc3QjNGQzA4N3Q4QmV3dVE3
FII0%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



A man with a beard and a fur-trimmed coat, holding a sword hilt, looking off to the side.

WINTER IS COMING

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.



science alert

Trending



(Allan Xia/Twitter)

TECH

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



ISOBEL ASHER HAMILTON, BUSINESS INSIDER

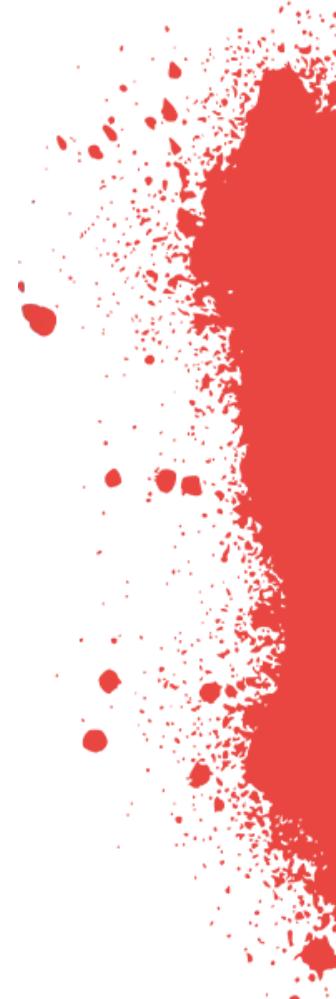
3 SEP 2019

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





„

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



Jak zareagują banki?

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

Czytaj ucz się, bez tego jesteś słaby...

Sokół - Orientuj się

10:56



Forum ▾

Szukaj na forum



Strona główna ▶ Forum ▶ NIE MÓW NIKOMU, ALE... ▶ Okradziona w ciąży

Okradziona w ciąży



« 1 2 3 4 5 »

na stronie: 20 50 100

(anonymowy) | 3 dni temu

Bardzo proszę o pomoc, jestem w 6 miesiącu ciąży. Zawsze zylam dość skromnie i biednie. Z anoniem bo mi wstydzę... Ostatnio sytuacja mnie przycisnęła i zylam jeszcze skromnie. Miałam odlożone na koncie 5 tys, zaczęłam wyprawkę dla dziecka, wczoraj na fb dałam się nabräć, miałam odkupić ciuszki za koszt przesyłki. Nie znam się na informacie, 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)

(anonymowy) | 3 dni temu

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

Polska youtuberka okradziona. Oszuści wyczyściли jej konto z oszczędności

Nie wierciecie 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?



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)

NAJCIĘŚCIEJ 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?

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. Kilkadziesiąt 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\(...\)](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 podstawy do reklamacji. Dzieki Tobie WOSP Sam Gramy razem otrzymało od mBanku nawet 600 zł.

Pytania?

kontakt@wiktorszymanski.pl 

[@wikszymans](https://twitter.com/wikszymans) 



Bezpieczny.blog