BNP PARIBAS

Agenda

Metody działania przestępców

Od socjotechniki po AI – jak rozpoznać próby wyłudzenia

Jak chronić swoją firmę przed oszustami i atakami

Bezpieczna bankowość dla firm – korzystaj z gotowych rozwiązań

Q&A- zachęcamy do zadawania pytań

ZAGROŻENIA CYBERBEZPIECZEŃSTWA

WSPÓLNE ZAGROŻENIA

- **PHISHING I SOCJOTECHNIKA**
oszustwa nakierowane na pracowników.
- **RANSOMWARE**
blokowanie dostępu do danych w zamian za okup.
- **ZŁOŚLIWE OPROGRAMOWANIE**
infekowanie systemów w celu kradzieży danych.
- **ATAKI NA ŁAŃCUCH DOSTAW**
wykorzystanie zaufanych partnerów jako wektora ataku.

KORPORACJE

Zaawansowane ataki APT (Advanced Persistent Threats)
długotrwałe, ukierunkowane kampanie.

Ataki typu insider threat
większe ryzyko zagrożeń wewnętrznych (np. nieuczciwi pracownicy).

Kradzież danych wrażliwych i własności intelektualnej
celowane kampanie.

Skoordynowane ataki DDoS
próba destabilizacji usług lub reputacji.

MŚP

Masowe, zautomatyzowane ataki
wykorzystanie popularnych luk bezpieczeństwa.

Brak segmentacji sieci i słabe zabezpieczenia końcówek
łatwiejsze przejęcie całej infrastruktury.

Niewystarczająca kopia zapasowa i plan reakcji
większe skutki ataku ransomware.

Braki kadrowe i technologiczne
mniejsza zdolność do wykrywania i reagowania.

METODY DZIAŁANIA PRZESTĘPCÓW

Wycieki danych ostatnio coraz częściej pojawiają się w nagłówkach prasowych, ich ofiarami padają często duże firmy, również w Polsce

/ Ekonomia / BIZNES

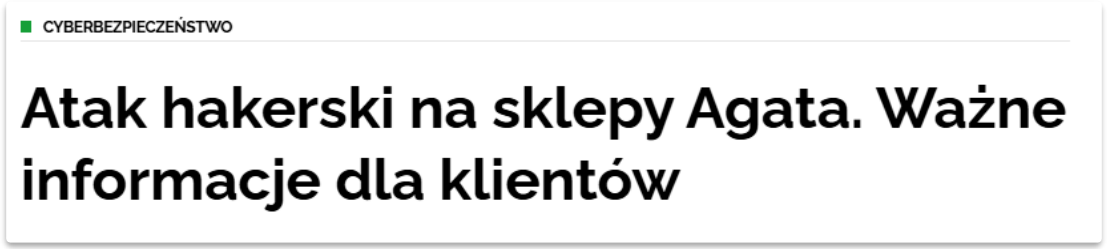
Polskie firmy są bombardowane przez hakerów. Tak źle jeszcze nie było

Trzy na cztery firmy doświadczyły już cyberataku. Tylko w sektorze handlu detalicznego straty z tego tytułu sięgają niemal 90 mld zł. Eksperci są pesymistami. Przewidują, że jeszcze w tym roku liczba hakerskich ciosów na nasz kraj skoczy o 25 proc.

Źródło: Informacje publiczne online

METODY DZIAŁANIA PRZESTĘPCÓW

Wycieki danych ostatnio coraz częściej pojawiają się w nagłówkach prasowych, ich ofiarami padają często duże firmy, również w Polsce


CYBERBEZPIECZEŃSTWO

Atak hakerski na sklepy Agata. Ważne informacje dla klientów

cyberdefence24.pl, 24.06.2024


22.11.2024 / 11:12

Auchan ofiarą cyberataku! Wykradziono dane osobowe 500 tysięcy klientów

wiadomoscihandlowe.pl, 22.11.2024


Atak hakerski na Super-Pharm. Masz tam konto? Lepiej uważaj

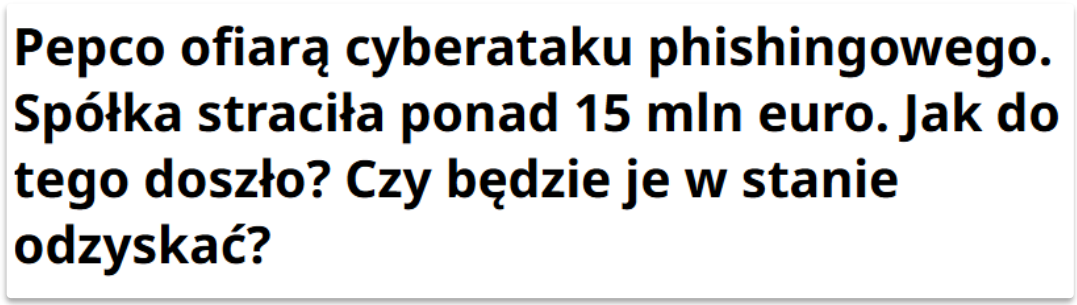
businessinsider.com.pl, 29.10.2024


Polska firma z biżuterią ma nowy e-sklep. Wszystko przez cyberatak

dlahandlu.pl, 15.01.2025


Ochnik i New Balance ofiarami ataku hakerskiego. Jaka jest skala wycieku danych i jakie informacje wykradli cyberprzestępcy?

wiadomoscihandlowe.pl, 25.09.2024


Pepco ofiarą cyberataku phishingowego. Spółka straciła ponad 15 mln euro. Jak do tego doszło? Czy będzie je w stanie odzyskać?

wiadomoscihandlowe.pl, 27.02.2024

Źródło: Informacje publiczne online

METODY DZIAŁANIA PRZESTĘPCÓW

Przykłady – jak wyciek danych może zagrozić Tobie i Twojej firmie

TY	HAKER	TY lub TWOJA FIRMA
1 ...podajesz swoje dane kontaktowe na www żeby pobrać raport branżowy	...ma dostęp do adresu email i telefonu pracownika + wie jaką firmę reprezentuje; dzwoni podszywając się pod dostawcę i wyłudza płatność za raport	... firma traci pieniądze i naraża dane finansowe na nieuprawnione użycie
2 ... zakładasz konto w dużym sklepie online, podając adres email, imię, nazwisko i ustawiając takie samo hasło jak wszędzie	... mając dostęp do hasła użytego w sklepie online próbuje za jego pomocą dostać się na pocztę oraz social media	tracisz kontrolę nad swoją tożsamością w sieci, haker może wysyłać wiadomość, publikować treści w Twoim imieniu, wykorzystać prywatną korespondencję do szantażu, etc.
3 ... na służbowym komputerze korzystasz z prywatnej poczty	...mając dane prywatne pracownika, dopasowuje do niego phishing i skłania do kliknięcia	...przez zainfekowanie sieci wewnętrznej złośliwym oprogramowaniem firma narażona jest na straty finansowe, wizerunkowe i zamknięcie działalności

PHISHING

Forma cyberataku polegająca na podszywaniu się pod zaufane podmioty w celu wyłudzenia poufnych danych, takich jak hasła, dane logowania czy informacje finansowe, najczęściej poprzez fałszywe e-maile, strony internetowe lub wiadomości.

1

STRONA PHISHINGOWA

Zostajemy nakłonieni do wprowadzenia swoich danych w serwisie łudząco przypominającym serwis naszego banku

→

2

PRZEJĘCIE DANYCH

W tle dochodzi do kradzieży naszych danych

→

3

STRONA AUTORYZACYJNA

Prezentowana jest nam strona, na której mamy wprowadzić autoryzacyjny kod SMS

→

4

POTWIERDZENIE SMS

Otrzymujemy kod potrzebny do autoryzacji transakcji (zainicjowanej przez oszusta)

→

5

WPROWADZENIE HASŁA

Wprowadzamy jednorazowe hasło i dajemy oszustowi dostęp do konta

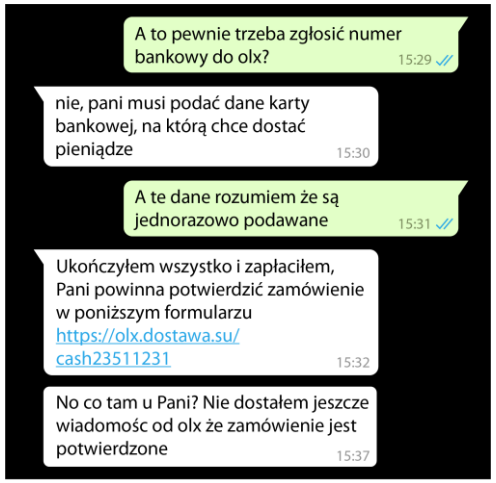
↓

Utrata pieniędzy

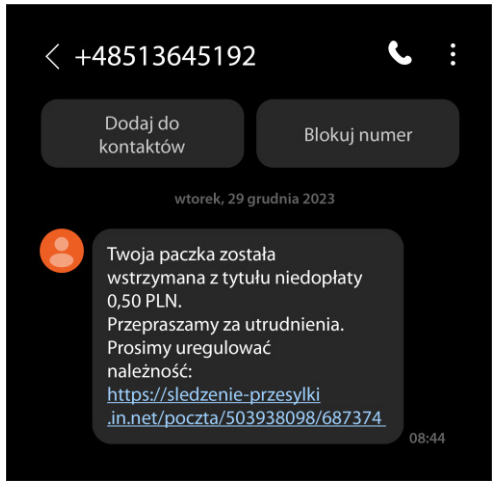
3,4 miliarda dziennie – tyle phishingowych maili wysyłanych jest na całym świecie

PRZYKŁADY MANIPULACJI

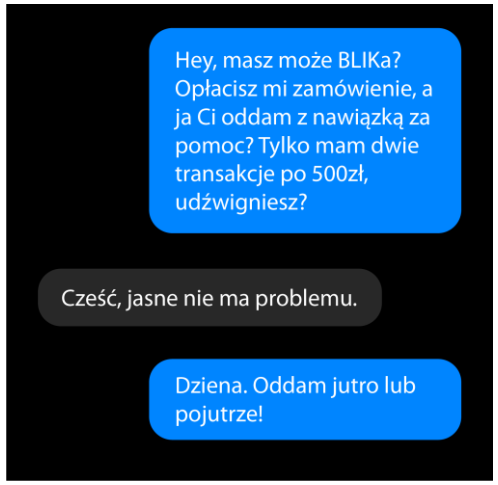
Na OLX



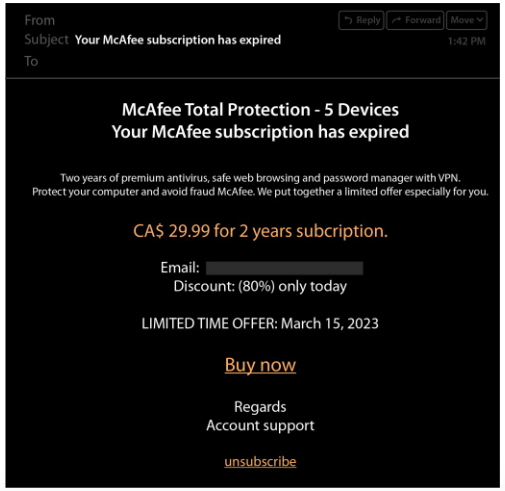
Na kuriera



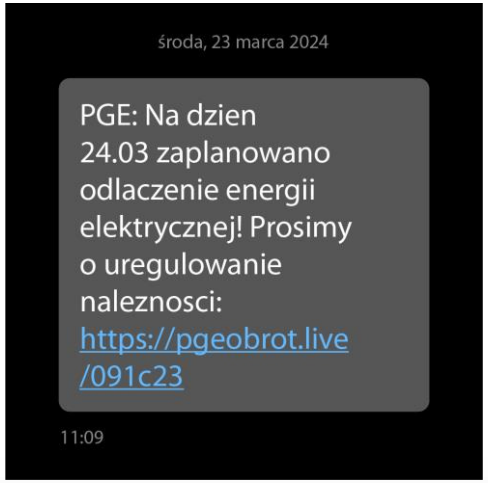
Na BLIKa



Na wygasłą subskrypcję



Dopłata do rachunku



Na urząd skarbowy

BUSINESS EMAIL COMPROMISE

BEC (Business Email Compromise) – oszustwo, w którym przestępcy podszywają się pod zaufane osoby lub firmy (np. dyrektora, kontrahenta), wykorzystując fałszywe lub przejęte konta e-mail, aby nakłonić ofiarę do przelania pieniędzy lub ujawnienia poufnych danych.

Oszuści tworzą adres email łudząco podobny do prawdziwego adresu firmy

Przestępcy uzyskują dostęp do skrzynki e-mail pracownika firmy

Przestępcy wysyłają wiadomość e-mail z fałszywą fakturą zawierającą podmieniony numer rachunku

Informacja o zmianie numeru rachunku

[redacted]

Szanowni Państwo,

Informujemy, że zmienił się numer rachunku należący do Naszej firmy. Wszelkie płatności proszę przekazywać na numer:

10[redacted]55

Z poważaniem,

[redacted]

Nieświadomy pracownik firmy wysyła przelew na rachunek przestępców

BUSINESS EMAIL COMPROMISE

BEC (Business Email Compromise) – oszustwo, w którym przestępcy podszywają się pod zaufane osoby lub firmy (np. dyrektora, kontrahenta), wykorzystując fałszywe lub przejęte konta e-mail, aby nakłonić ofiarę do przelania pieniędzy lub ujawnienia poufnych danych.

8,5 mld GLOBALNE STRATY FINANSOWE:

W 2024 roku straty spowodowane przez BEC przekroczyły **8,5 miliarda** dolarów, a w ciągu ostatnich pięciu lat wyniosły łącznie 52 miliardy dolarów.

42% WZROST LICZBY ATAKÓW:

W pierwszej połowie 2024 roku liczba ataków BEC **wzrosła o 42%** w porównaniu do tego samego okresu w 2023 roku.

21% UDZIAŁ W ATAKACH E-MAILOWYCH:

BEC stanowi obecnie **21% wszystkich ataków** e-mailowych, w porównaniu do 15% w 2023 roku.

POMIMO ROSNĄCEJ ŚWIADOMOŚCI OKOŁO

17%

ataków BEC kończy się sukcesem, prowadząc do kompromitacji co najmniej jednego pracownika w zaatakowanej organizacji .

40% WYKORZYSTANIE SZTUCZNEJ INTELIGENCJI:

Aż 40% wiadomości BEC jest generowanych **przy użyciu narzędzi AI**, co zwiększa ich skuteczność i trudność w wykryciu.

5 mln ŚREDNI KOSZT INCYDENTU:

W 2025 roku średni koszt pojedynczego ataku BEC wynosił 125 000 dolarów, a w niektórych przypadkach **przekraczał 5 milionów dolarów.**

SCAM

Co widzi użytkownik vs co naprawdę się dzieje

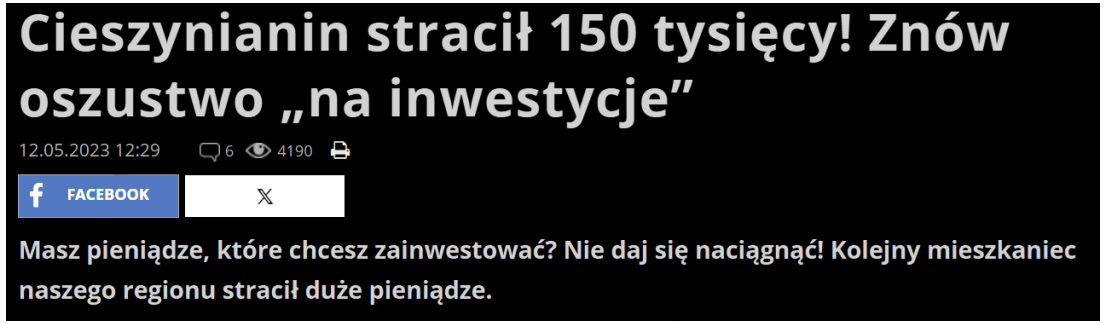
Oszustwo internetowe polegające na manipulacji i wprowadzaniu ofiary w błąd w celu wyłudzenia pieniędzy, danych osobowych lub innych wartościowych informacji, często poprzez fałszywe oferty, inwestycje, loterie czy podszywanie się pod zaufane instytucje.

Co się dzieje wg użytkownika	UŻYTKOWNIK vs RZECZYWISTOŚĆ	Co się dzieje w rzeczywistości
„Atrakcyjna reklama inwestycji"		Strona kontrolowana przez oszustów
„Rejestracja, by otrzymać ofertę"		Przekazanie danych osobowych i firmowych
„Rozmowa z doradcą przez telefon"		Atak socjotechniczny – profilowanie ofiary
„Weryfikacja konta inwestora"		Ujawnienie numeru konta i dokumentów firmowych
„Wpłata zaliczki z konta firmowego"		Środki trafiają na konto oszusta – nie do odzyskania
„Brak kontaktu po kilku dniach"		Kradzież tożsamości, możliwe dalsze próby wyłudzeń

Ponad 300 fałszywych aplikacji inwestycyjnych zostało znalezionych w oficjalnych sklepach z aplikacjami mobilnymi

PRZYKŁADY MANIPULACJI

Inwestycja w kryptowaluty



Cieszynianin stracił 150 tysięcy! Znów oszustwo „na inwestycje”

12.05.2023 12:29 6 4190

FACEBOOK

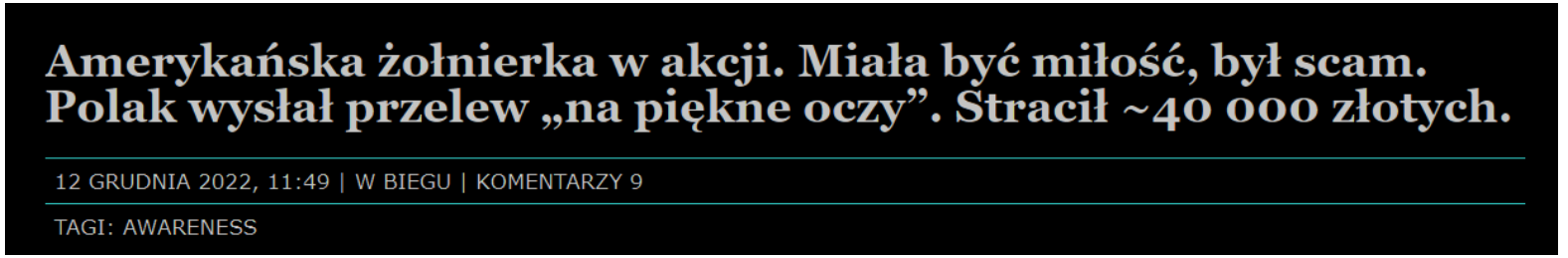
Masz pieniądze, które chcesz zainwestować? Nie daj się naciągnąć! Kolejny mieszkaniec naszego regionu stracił duże pieniądze.

Inwestycja biznesowa

Zainwestował w "azjatycki sklep", stracił ponad 300 tysięcy złotych

TVN Warszawa | Okolice 28 kwietnia 2024, 9:05 Źródło: tvnarszawa.pl

Romans scam



Amerykańska żołnierka w akcji. Miała być miłość, był scam. Polak wysłał przelew „na piękne oczy”. Stracił ~40 000 złotych.

12 GRUDNIA 2022, 11:49 | W BIEGU | KOMENTARZY 9

TAGI: AWARENESS

PRZYKŁADY MANIPULACJI

Chciał zainwestować w kryptowaluty. Zamiast zyskać, stracił setki tysięcy

44-LATEK STRACIŁ PÓŁ MILIONA ZŁOTYCH. INWESTYCJA W KRYPTOWALUTY OKAZAŁA SIĘ OSZUSTWEM

Z zadowoleniem oglądał swoje zyski z kryptowalut. Jeszcze nie wiedział, że dał się oszukać

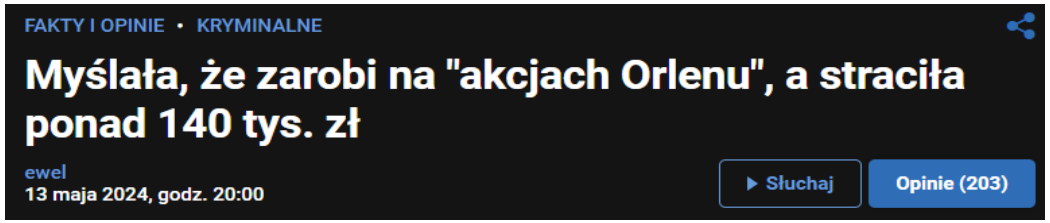
CYBERBEZPIECZEŃSTWO

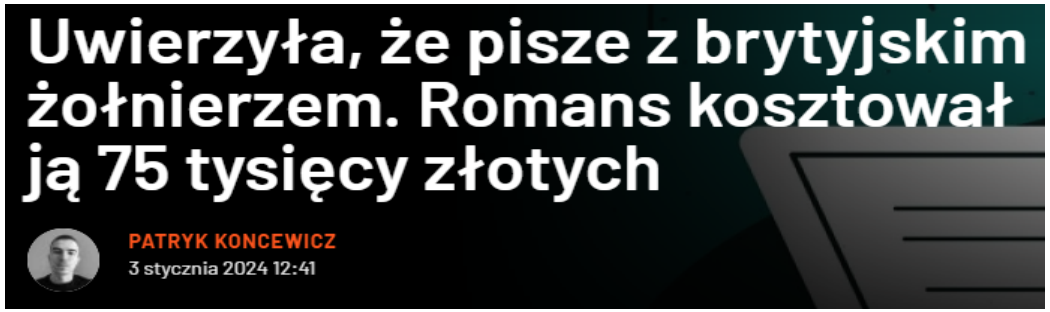
Oszuści wyłudzili 139 mln dolarów w kryptowalutach. Schemat działania opierał się o... romans

24 CYBERDEFENCE24
11.03.2022 13:48

DRUKUJ PDF

ZAMIAST DUŻYCH ZYSKÓW SĄDECZANKA STRACIŁA 170 TYS. ZŁOTYCH. OSZUSTWO NA „ZDALNY PULPIT" Z KRYPTOWALUTAMI W TLE





DEEP FAKE

Technologia oparta na sztucznej inteligencji, wykorzystująca algorytmy uczenia maszynowego do tworzenia realistycznych, ale fałszywych obrazów, nagrań wideo lub audio, które mogą przedstawiać osoby wykonujące lub mówiące rzeczy, których nigdy nie zrobiły.

1

STWORZENIE DEEPFAKE'U

Oszuści tworzą realistyczny materiał wideo lub audio (deepfake), aby podszyć się pod znaną osobę lub zaufaną instytucję

2

KONTAKT Z OFIARĄ

Otrzymujemy wiadomość, e-mail, telefon lub wideorozmowę

3

PRZEDSTAWIENIE FAŁSZYWEJ OFERTY

Oszuści przedstawiają atrakcyjną ofertę inwestycyjną, prośbę o pilny przelew, lub inną formę oszustwa finansowego

4

ZBUDOWANIE ZAUFANIA

Znajomość tej osoby budzi w nas poczucie zaufania przez jej autorytet lub kompetencje

5

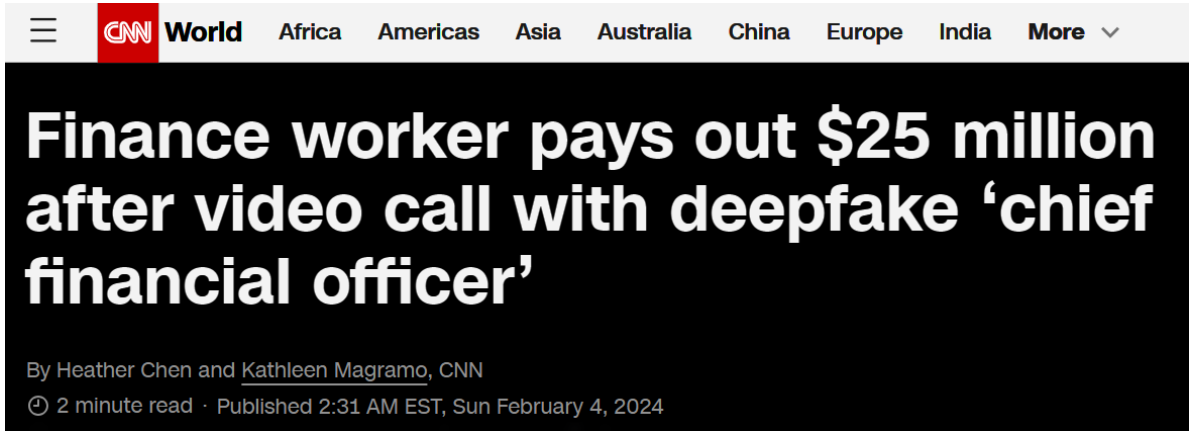
WYŁUDZENIE ŚRODKÓW

Dokonujemy przelewu na wskazane konto, wierząc, że pomaga zaufanej osobie lub inwestuje w obiecującą ofertę

Utrata pieniędzy

68% ataków phishingowych w 2024 roku wykorzystywało AI, co czyni je trudniejszymi do odróżnienia od prawdziwej korespondencji

DEEP FAKE - SCENARIUSZ



Pracownik wypłaca 25 milionów dolarów po rozmowie wideo z fałszywym CEO

Oszuści, używając technologii deepfake, podali się za dyrektora generalnego firmy, skłonili pracownika do przelania dużej sumy pieniędzy.

1

WPROWADZENIE

Pracownik został poproszony o przeprowadzenia tajnej transakcji przez dyrektora generalnego firmy z Wielkiej Brytanii

2

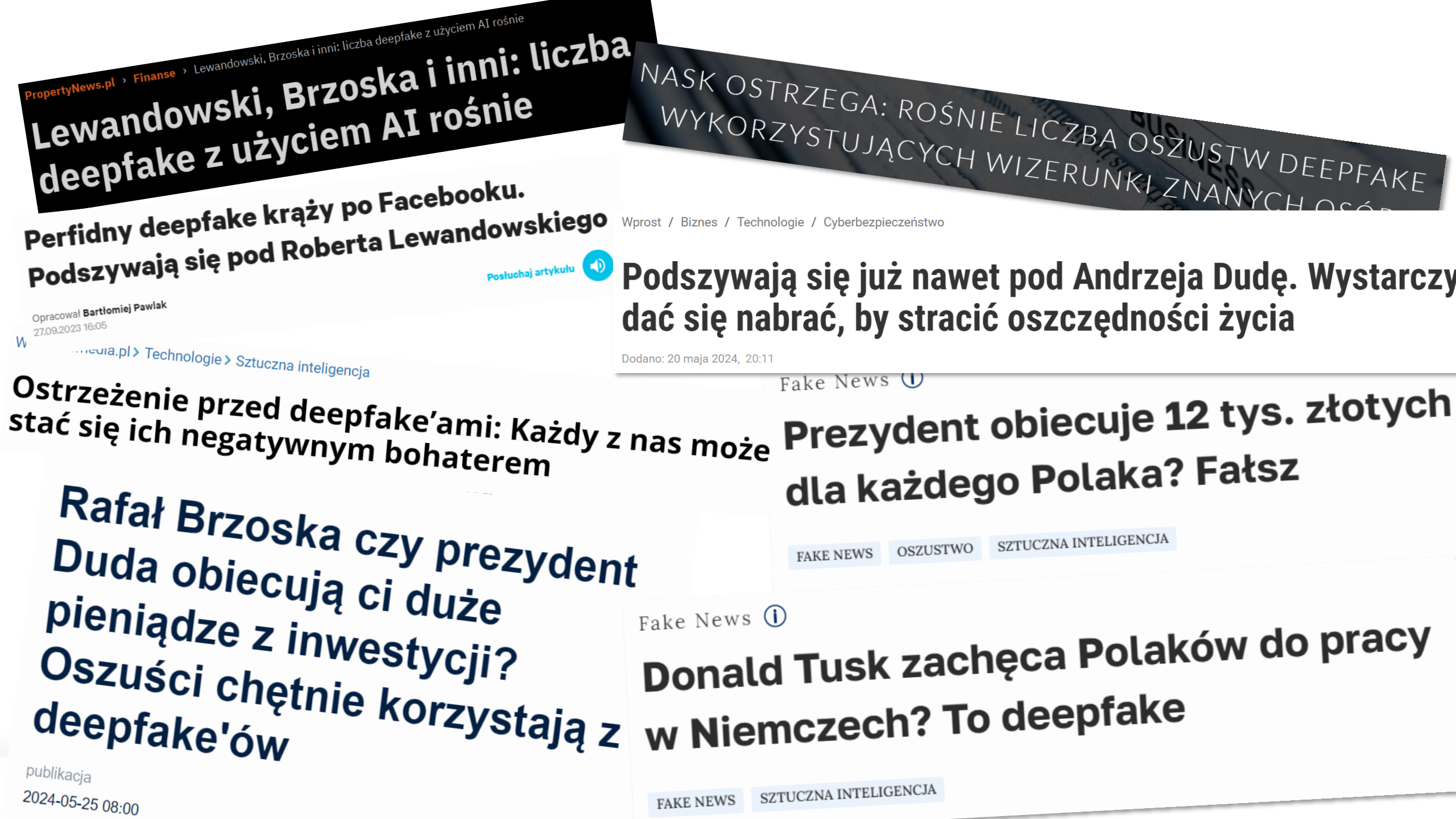
OPIS

Początkowo pracownik podejrzewał, że to phishing, ale po wideokonferencji, na której inni uczestnicy wyglądali i brzmieli jak znani mu koledzy, porzucił swoje wątpliwości

3

SKUTEK

Przekonany, że wszyscy na spotkaniu są prawdziwi, zgodził się przelać 200 milionów dolarów hongkońskich – około 25,6 miliona dolarów


PropertyNews.pl › Finanse › Lewandowski, Brzoska i inni: liczba deepfake z użyciem AI rośnie
Lewandowski, Brzoska i inni: liczba deepfake z użyciem AI rośnie
NASK OSTRZEGA: ROŚNIE LICZBA OSZUSTW DEEPFAKE WYKORZYSTUJĄCYCH WIZERUNKI ZNANYCH
Perfidny deepfake krąży po Facebooku.
Podszywają się pod Roberta Lewandowskiego
Posłuchaj artykułu
Opracował Bartłomiej Pawlak
27.09.2023 16:05
Wprost / Biznes / Technologie / Cyberbezpieczeństwo
Podszywają się już nawet pod Andrzeja Dudę. Wystarczy dać się nabrać, by stracić oszczędności życia
Dodano: 20 maja 2024, 20:11
Technologie › Sztuczna inteligencja
Ostrzeżenie przed deepfake'ami: Każdy z nas może stać się ich negatywnym bohaterem
Fake News
Prezydent obiecuje 12 tys. złotych dla każdego Polaka? Fałsz
FAKE NEWS
OSZUSTWO
SZTUCZNA INTELIGENCJA
Rafał Brzoska czy prezydent Duda obiecują ci duże pieniądze z inwestycji? Oszuści chętnie korzystają z deepfake'ów
publikacja
2024-05-25 08:00
Fake News
Donald Tusk zachęca Polaków do pracy w Niemczech? To deepfake
FAKE NEWS
SZTUCZNA INTELIGENCJA

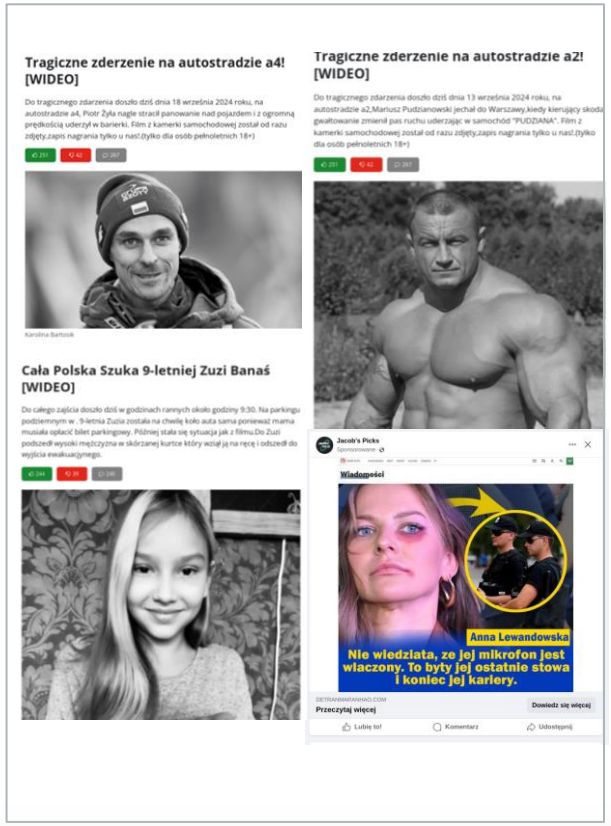
PSYCHOLOGIA OSZUSTW - JAK MANIPULACJA EMOCJAMI DOPROWADZA DO UTRATY PIENIĘDZY

WYKORZYSTANIE ZAUFANIA

podszycia pod znane instytucje/banki

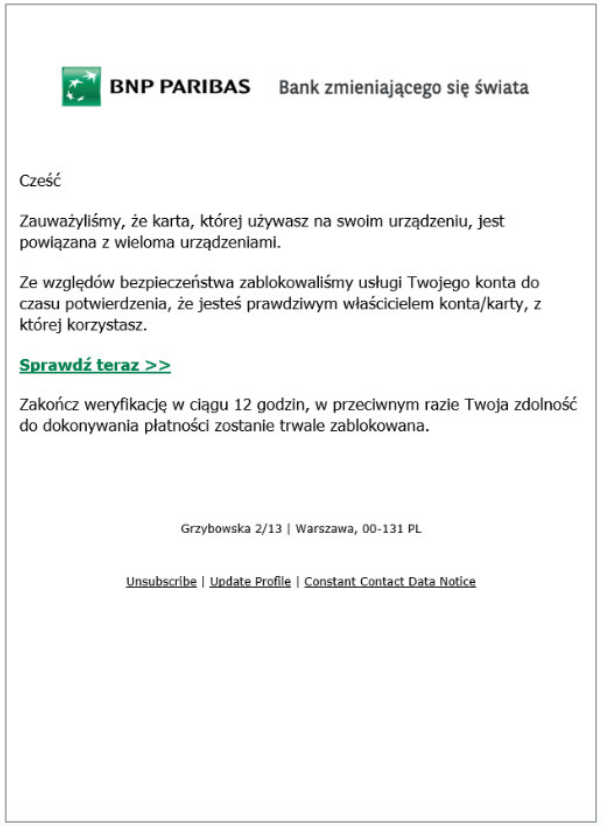
GRA NA EMOCJACH

ciekawość, strach, chęć zysku



PRESJA CZASU

nacisk na szybkie działanie



POTRZEBA POMOCY

Nie szukaj jej w reklamach

BNP PARIBAS

Dodatkowe zabezpieczenia

KORZYSTAJ Z GOTOWYCH ROZWIĄZAŃ!

USTAW LIMITY

- **Ustaw limity przelewów i płatności kartą** – to prosta, ale skuteczna forma ochrony środków.
- **Dopasuj limity do swoich codziennych potrzeb** – unikniesz niepotrzebnych blokad i ryzyka.
- **Regularnie przeglądaj i aktualizuj limity** w ustawieniach bankowości internetowej lub mobilnej.

SILNE HASŁO TO PODSTAWA!

81% wycieków danych zaczyna się od słabych lub skradzionych haseł. Cyberprzestępcy łamią proste hasło w **mniej niż 1 sekundę.**

Jak tworzyć silne hasła?

- ✓ **Min. 15 znaków**
- ✓ **Duże i małe litery, cyfry, znaki specjalne**
- ✓ **Unikaj oczywistych kombinacji (np. „123456”)**
- ✓ **Nie używaj tego samego hasła w różnych serwisach**

T0m0je$ilneH@$ło!

LOGUJ SIĘ ZE WSKAZANEGO ADRESU IP

Ustaw adres IP, z którego chcesz logować się do bankowości.

- Możesz to zrobić bezpośrednio w GOonline Biznes w panelu administratora (jeśli posiadasz uprawnienia)
- Wniosek możesz złożyć również dla innych użytkowników w firmie w systemie GOonline Biznes (jeśli posiadasz uprawnienia)

WIELOSKŁADNIKOWE UWIERZYTELNIENIE

To najskuteczniejsza metoda **zabezpieczenia konta przed nieautoryzowanym dostępem.**

- **Zwiększa bezpieczeństwo logowania** — nawet jeśli ktoś pozna Twoje hasło, nie zaloguje się bez drugiego składnika.
- **Działa na różnych urządzeniach** — kody SMS, aplikacje, klucze sprzętowe.
- **Proste wdrożenie i użytkowanie** — nie wymaga wiedzy technicznej.
- **Minimalny wysiłek, maksymalna ochrona** — sprawdza się w życiu prywatnym i biznesie.

O USŁUDZE

Mastercard ID Theft Protection umożliwia kontrolę własnej tożsamości w Internecie

OCHRONA

WYKRYCIE

Aktywny monitoring wycieku danych w Internecie*

ALERT

Natychmiastowe poinformowanie klienta o zagrożeniu

ROZWIĄZANIE

Instrukcje zabezpieczenia się przed konsekwencjami wycieku

*W tym darkweb i deepweb

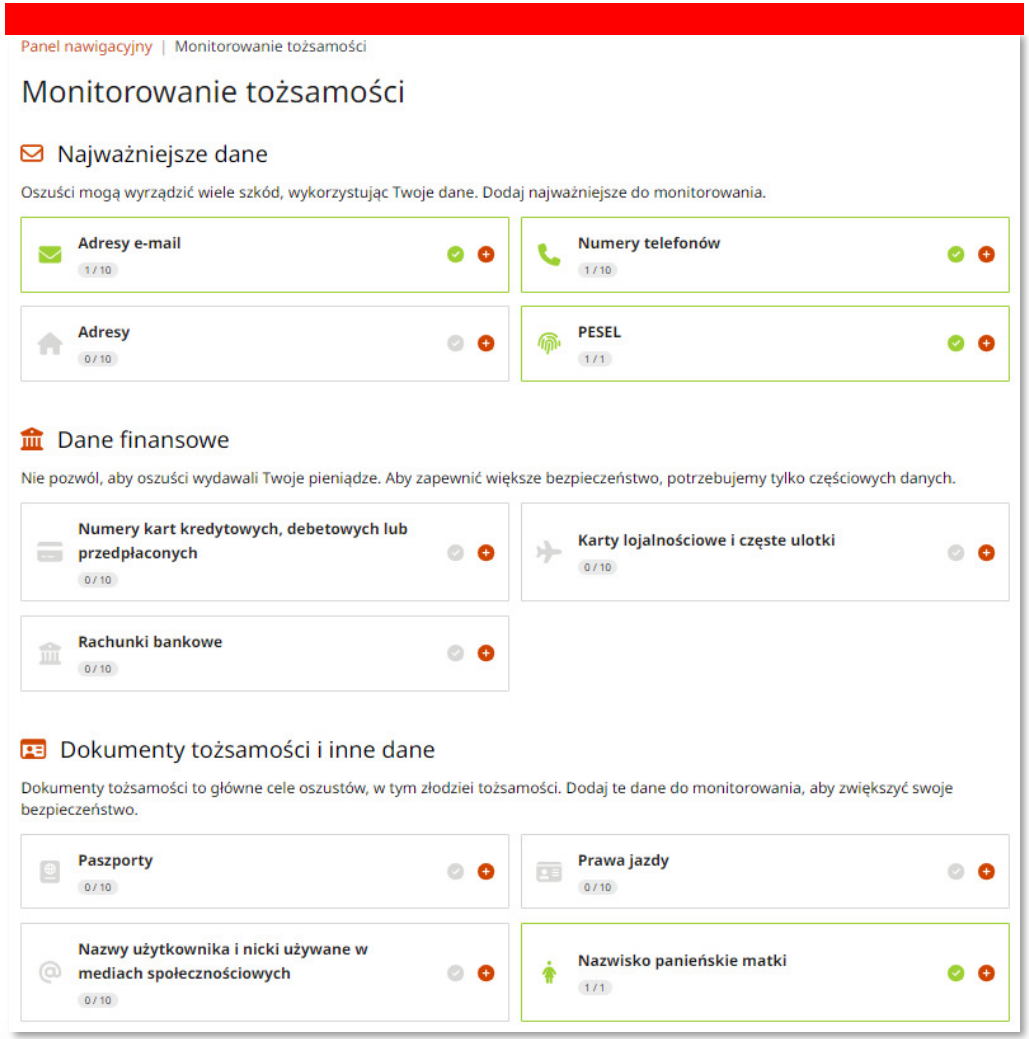
O USŁUDZE

Mastercard ID Theft Protection umożliwia kontrolę własnej tożsamości w Internecie

WYKRYCIE ⬇

na bieżąco monitorujemy czy nie wyciekły Twoje dane, np:

- OSOBOWE
- FINANSOWE
- KONTAKTOWE
- SOCIAL MEDIA



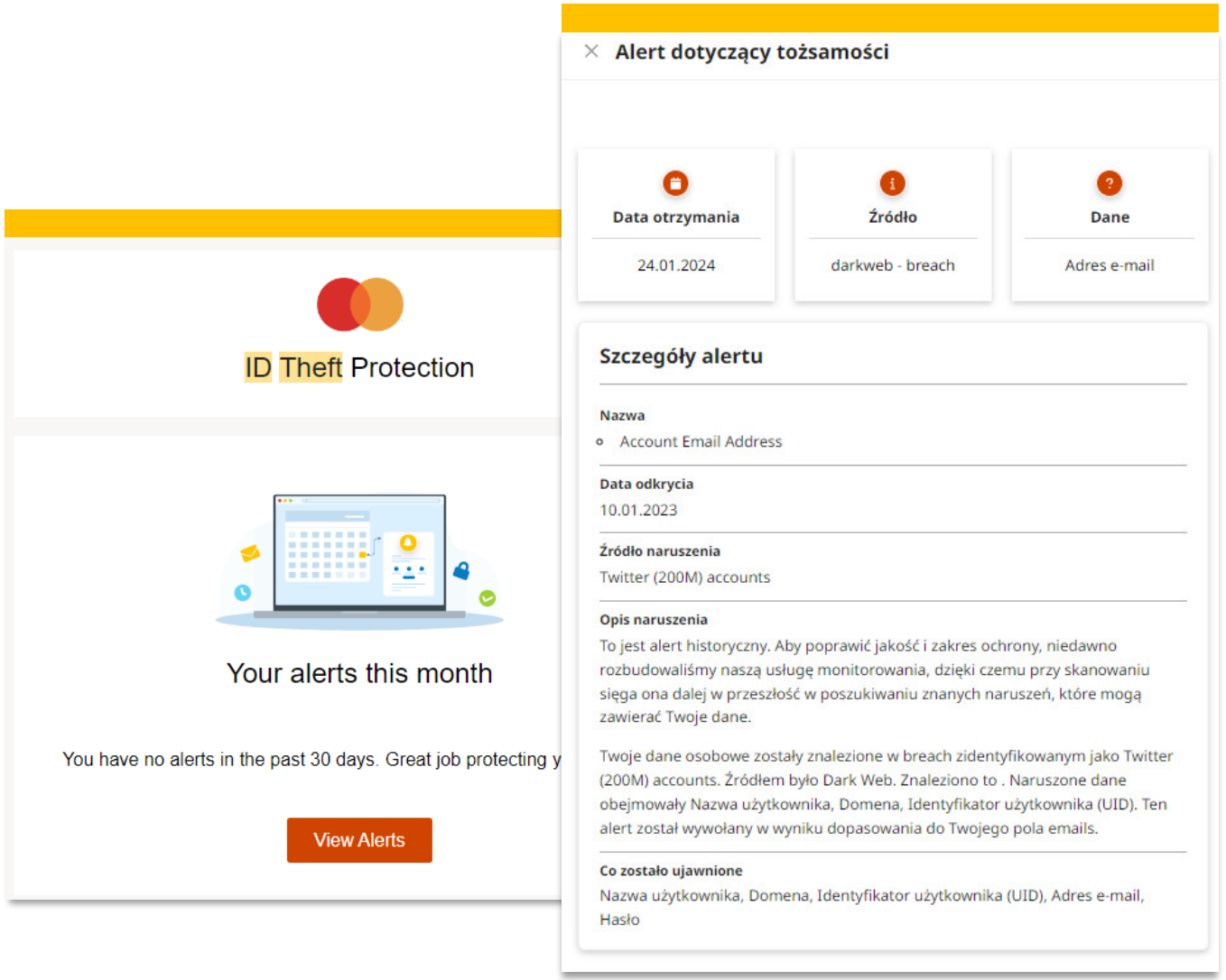
O USŁUDZE

Mastercard ID Theft Protection umożliwia kontrolę własnej tożsamości w Internecie

ALERT

natychmiast powiadamiamy o podejrzanej aktywności przez:

Email



O USŁUDZE

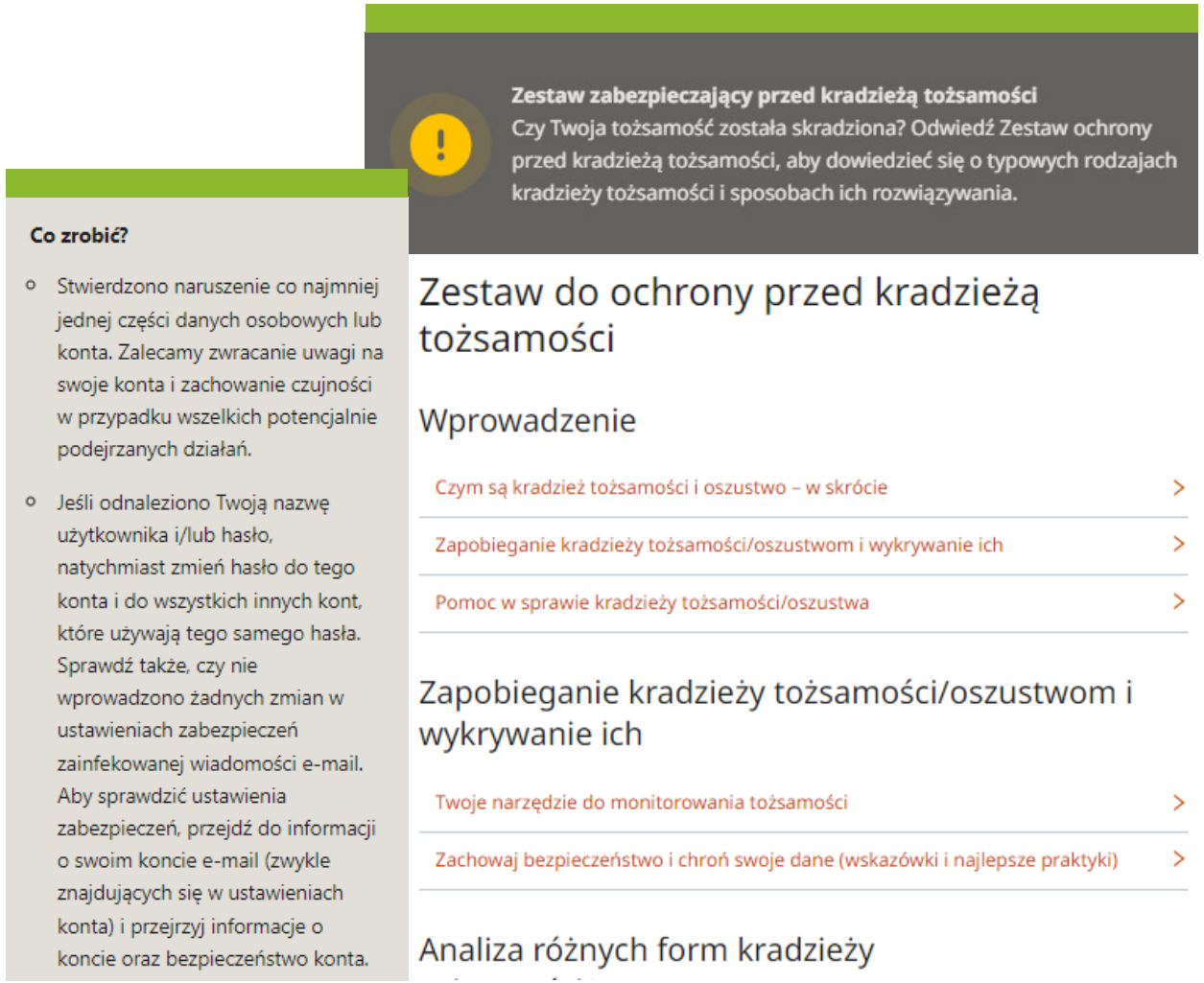
Mastercard ID Theft Protection umożliwia kontrolę własnej tożsamości w Internecie

ROZWIĄZANIE⬇

podpowiadamy jak rozwiązać problem i zabezpieczyć przed atakiem

Wszystkie alerty o oszustwach dostępne online

Samoobsługowy poradnik ID Theft Resolution Kit



PODSUMOWANIE

10 ZASAD BEZPIECZNEJ BANKOWOŚCI ELEKTRONICZNEJ

BNP PARIBAS

PRACOWNICY BANKU NIGDY NIE PROSZĄ O:

- Twój login lub hasło do bankowości,
- instalację dodatkowego oprogramowania,
- uzyskanie zdalnego dostępu do komputera/telefonu,
- pełen numer karty i kod CVV/CVC,
- podanie kodu BLIK, wykonanie przelewu,
- wpłatę lub wypłatę pieniędzy w bankomacie czy oddziale banku.

Zgłoś taki przypadek pod numerem telefonu czynnym 24/7:
+48 22 548 29 40
(koszt połączenia wg stawki operatora).

ODWIEDZAJ! STREFĘ BEZPIECZEŃSTWA NA: www.bnpparibas.pl/bezpieczenstwo

GOmobile Biznes TO DOSTĘP DO RACHNKÓW BANKOWYCH ZAWSZE POD RĘKĄ

Autoryzacja mobilna

Przy pomocy wbudowanego tokena mobilnego szybko i bezpiecznie podpiszesz operacje w systemie bankowości internetowej GOonline Biznes. Możliwość podpisywania zleceń za pomocą PIN oraz z wykorzystaniem biometrii.

Logowanie biometryczne

Logowanie do aplikacji z wykorzystaniem odcisku palca oraz rozpoznawania twarzy.

Kursy walutowe

Prezentacja bankowych kursów kupna i sprzedaży walut, które wybrano w ustawieniach aplikacji.

Wskaźnik salda

Procentowy wskaźnik sumy sald na rachunkach pozwala szybko sprawdzić stan finansów firmy. W ustawieniach aplikacji należy zdefiniować kwotę stanowiącą 100% salda.

ZACHĘCAMY DO ZADAWANIA PYTAŃ

Dziękuję merci

mèsitak GRAZIE chokrane

dhanyavad ARIGATÔ THANK YOU

GRACIAS danke ευχαριστώ NANDRI

спасибо MAHALO teşekkür

ederim spas JËRËJËF