



BNP PARIBAS



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

Agenda

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 przejście 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. Ekspertci są pesymistami. Przewidują, że jeszcze w tym roku liczba hakerskich ciosów na nasz kraj skoczy o 25 proc.



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



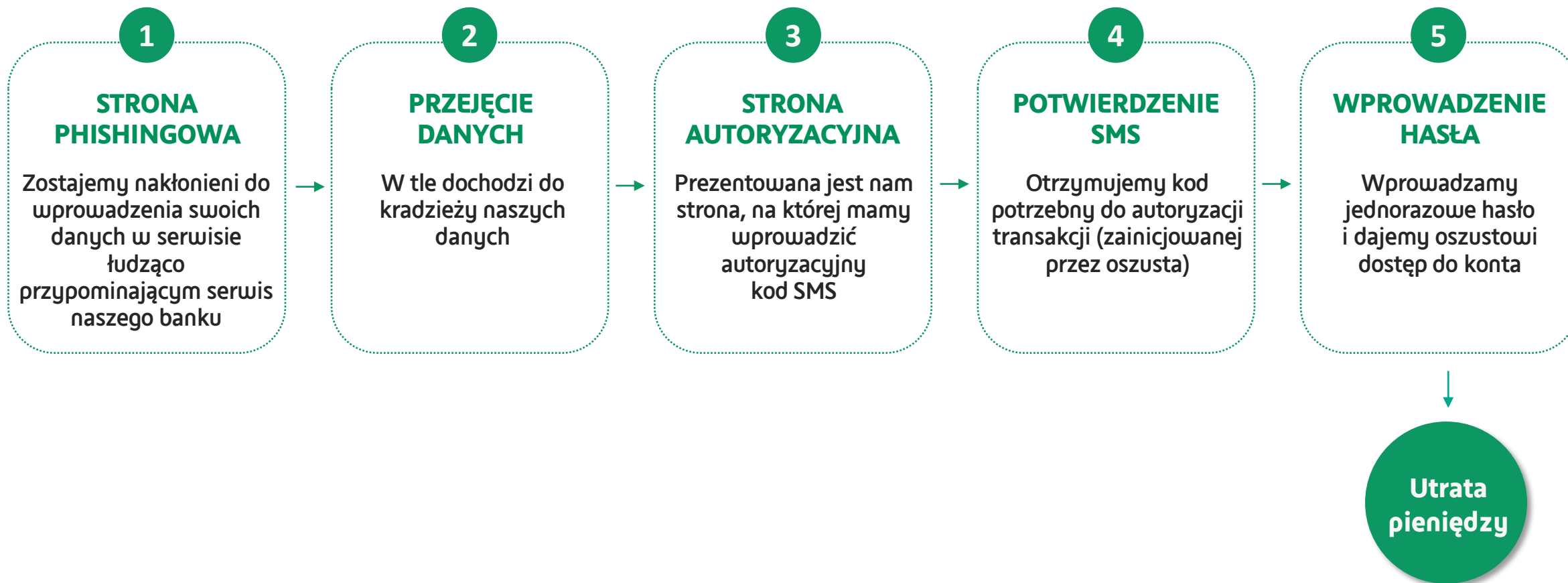
...przez zainfekowanie sieci wewnętrznej złośliwym oprogramowaniem firma narażona jest na **straty finansowe, wizerunkowe i zamknięcie działalności**



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.



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

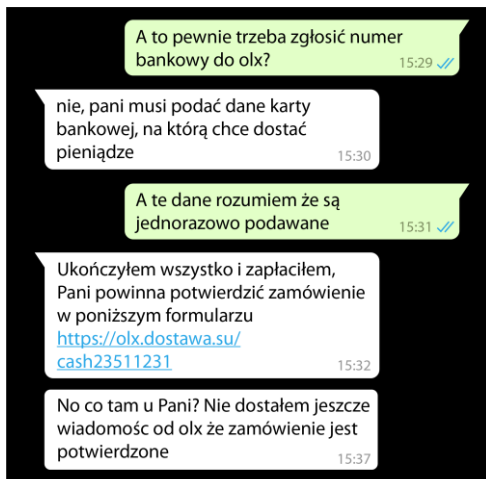


BNP PARIBAS

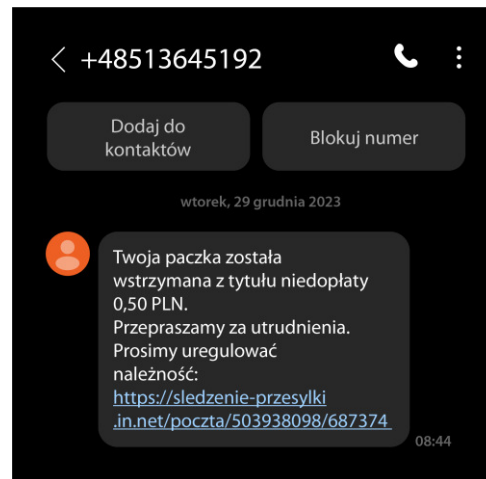


PRZYKŁADY MANIPULACJI

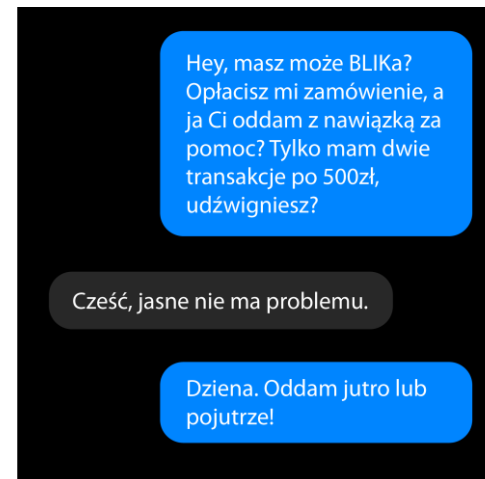
Na OLX



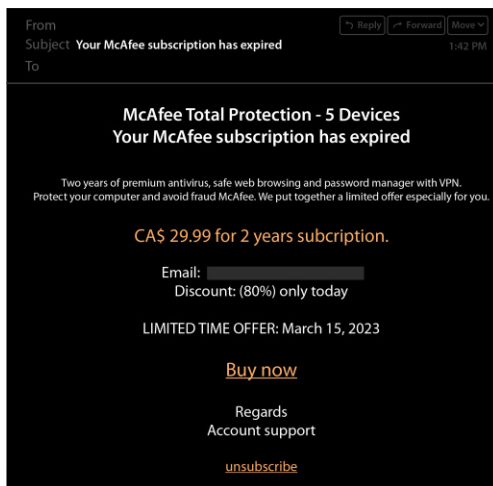
Na kuriera



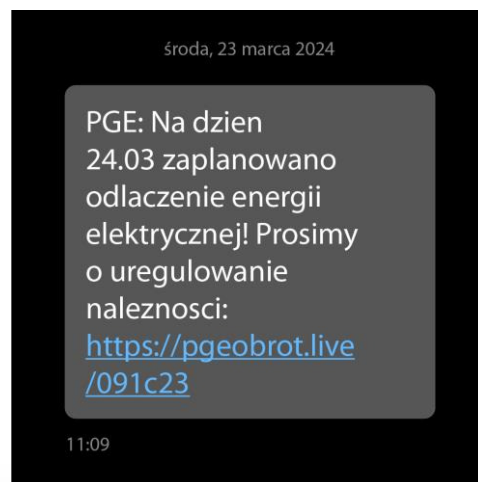
Na BLIKa



Na wygaśnięcie subskrypcji



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

Przestępcy uzyskują dostęp do skrzynki e-mail pracownika firmy

Informacja o zmianie numeru rachunku

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



BNP PARIBAS



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.

8,5mld 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.

5mln ŚREDNI KOSZT
INCYDENTU:

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

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

- „Atrakcyjna reklama inwestycji”
- „Rejestracja, by otrzymać ofertę”
- „Rozmowa z doradcą przez telefon”
- „Weryfikacja konta inwestora”
- „Wpłata zaliczki z konta firmowego”
- „Brak kontaktu po kilku dniach”

UŻYTKOWNIK
VS
RZECZYWISTOŚĆ

Co się dzieje w rzeczywistości



- Strona kontrolowana przez oszustów
- Przekazanie danych osobowych i firmowych
- Atak socjotechniczny – profilowanie ofiary
- Ujawnienie numeru konta i dokumentów firmowych
- Środki trafiają na konto oszusta – nie do odzyskania
- 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

f FACEBOOK

X

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



BNP PARIBAS



PRZYKŁADY MANIPULACJI

Chciał zainwestować w kryptowaluty. Zamiast zyskać, stracił setki tysięcy

FAKTY I OPINIE • KRYMINALNE

Oszustwo na "akcje Baltic Pipe" wciąż działa

ms
27 lutego 2024, godz. 20:30

▶ Słuchaj

Opinie (71)

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

f

t

in

o

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

Strona główna > Fake News > TVP Info zachęca do inwestycji w Baltic...

24.11.2022 godz. 12:45 • 7 min czytania

Fake News ⓘ

TVP Info zachęca do inwestycji w Baltic Pipe? Uwaga na oszustwo!

FAKE NEWS OSZUSTWO

FAKTY I OPINIE • KRYMINALNE

Myślała, że zarobi na "akcjach Orlenu", a straciła ponad 140 tys. zł

ewel
13 maja 2024, godz. 20:00

▶ Słuchaj

Opinie (203)

Uwierzyła, że pisze z brytyjskim żołnierzem. Romans kosztował ją 75 tysięcy złotych

 **PATRYK KONCEWICZ**
3 stycznia 2024 12:41

DEEP FAKE

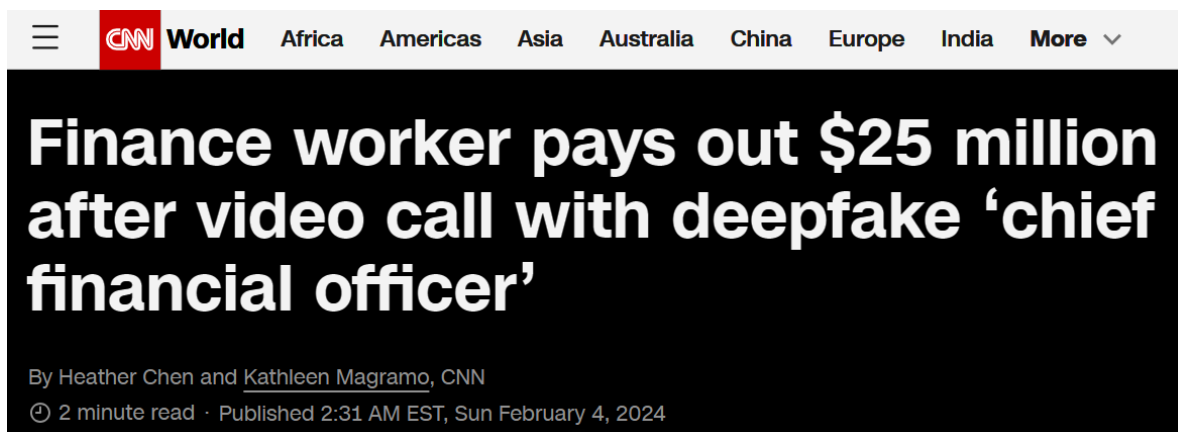


Technologia oparta na sztucznej inteligencji, wykorzystująca algorytmy uczenia maszynowego do tworzenia realistycznych, ale fałszywych obrazów, nagrań wideo lub audio, które mogą przedstawiać osoby wykonujące lub mówiące rzeczy, których nigdy nie zrobiły.



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





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 brzmiali jak znani mu koledzy, porzucił swoje wątpliwości

3

SKUTEK

Przekonany, że wszyscy na spotkaniu są prawdziwi, zgodził się przełać 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

Perfidny deepfake krąży po Facebooku. Podszrywają się pod Roberta Lewandowskiego

Opracował **Bartłomiej Pawlak**
27.09.2023 16:05

Posłuchaj artykułu 

W [PropertyNews.pl](#) > [Technologie](#) > [Sztuczna inteligencja](#)

Ostrzeżenie przed deepfake'ami: Każdy z nas może stać się ich negatywnym bohaterem

Rafał Brzoska czy prezydent Duda obiecują ci duże pieniądze z inwestycji? Oszuści chętnie korzystają z deepfake'ów

publikacja
2024-05-25 08:00

NASK OSTRZEGA: ROŚNIE LICZBA OSZUSTW DEEPPFAKE WYKORZYSTUJĄCYCH WIZERUNKI ZNANYCH OSÓB

Wprost / Biznes / Technologie / Cyberbezpieczeństwo

Podszrywają się już nawet pod Andrzeja Dudę. Wystarczy dać się nabrać, by stracić oszczędności życia

Dodano: 20 maja 2024, 20:11

Fake News 

Prezydent obiecuje 12 tys. złotych dla każdego Polaka? Fałsz

FAKE NEWS OSZUSTWO SZTUCZNA INTELIGENCJA

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



Dostęp pacjenta

Strona główna > Obowiązkowa aktualizacja > Aktualizacja NFZ

Moje dane osobowe

Nowa wersja karty NFZ jest już dostępna dla wszystkich świadczeniobiorców. Aktualizacja ta oznacza możliwość uregulowania i aktualizacji uprawnień oraz gwarantuje skuteczniejsze pokrycie kosztów opieki zdrowotnej.

Aby w praktyczny i bezpieczny sposób złożyć wniosek o nową kartę NFZ, prosimy o wypełnienie poniższego formularza:

Prosimy o sprawdzenie poprawności danych przed wysłaniem formularza.

Tragiczne zderzenie na autostradzie a4! [WIDEO]

Do tragicznego zdarzenia doszło dziś dnia 18 września 2024 roku, na autostradzie a4. Pasażer 3-letniego samochodu dostawczego i z ogromną prędkością uderzył w barierki. Film z kamery samochodowej został od razu zdjęty, zapis nagrania tylko u nas! (tylko dla osób pełnoletnich 18+)



Cała Polska Szuka 9-letniej Zuzi Banas! [WIDEO]

Do całego zapisu doszło dziś w godzinach rannych około godziny 9:30. Na parkingu podziemnym w 9-lecia Zuzi została na chwilę sama sama ponieważ miała musiała opuścić teren parkingowy. Później stała się sytuacja jak u filmu. Do Zuzi podszedł wysoki mężczyzna w skórzanej kurtce który wstał jak na ręce i odurzył do wyjścia z parkingu.



Tragiczne zderzenie na autostradzie a4! [WIDEO]

Do tragicznego zdarzenia doszło dziś dnia 13 września 2024 roku, na autostradzie a4. Mariusz Pustkiewicz jechał do Warszawy, kiedy kierujący skodą gwałtownie zmienił pas ruchu uderzając w samochód "PUDZANA". Film z kamery samochodowej został od razu zdjęty, zapis nagrania tylko u nas! (tylko dla osób pełnoletnich 18+)



BNP PARIBAS Bank zmieniającego się świata

Cześć

Zauważyliśmy, że karta, której używasz na swoim urządzeniu, jest powiązana z wieloma urządzeniami.

Ze względów bezpieczeństwa zablokowaliśmy usługi Twojego konta do czasu potwierdzenia, że jesteś prawdziwym właścicielem konta/karty, z której korzystasz.

[Sprawdź teraz >>](#)

Zakończ weryfikację w ciągu 12 godzin, w przeciwnym razie Twoja zdolność do dokonywania płatności zostanie trwale zablokowana.

Grzybowska 2/13 | Warszawa, 00-131 PL

[Unsubscribe](#) | [Update Profile](#) | [Constant Contact Data Notice](#)



BNP PARIBAS





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@\$ł0!

> 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.



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



BNP PARIBAS





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

Panel nawigacyjny | Monitorowanie tożsamości

Monitorowanie tożsamości

Najważniejsze dane

Oszuści mogą wyrządzić wiele szkód, wykorzystując Twoje dane. Dodaj najważniejsze do monitorowania.

Adresy e-mail 1 / 10	Numery telefonów 1 / 10
Adresy 0 / 10	PESEL 1 / 1

Dane finansowe

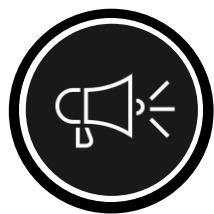
Nie pozwól, aby oszuści wydawali Twoje pieniądze. Aby zapewnić większe bezpieczeństwo, potrzebujemy tylko częściowych danych.

Numery kart kredytowych, debetowych lub przedpłaconych 0 / 10	Karty lojalnościowe i częste ulotki 0 / 10
Rachunki bankowe 0 / 10	

Dokumenty tożsamości i inne dane

Dokumenty tożsamości to główne cele oszustów, w tym złodziei tożsamości. Dodaj te dane do monitorowania, aby zwiększyć swoje bezpieczeństwo.

Paszporty 0 / 10	Prawa jazdy 0 / 10
Nazwy użytkownika i nicki używane w mediach społecznościowych 0 / 10	Nazwisko panięskie matki 1 / 1



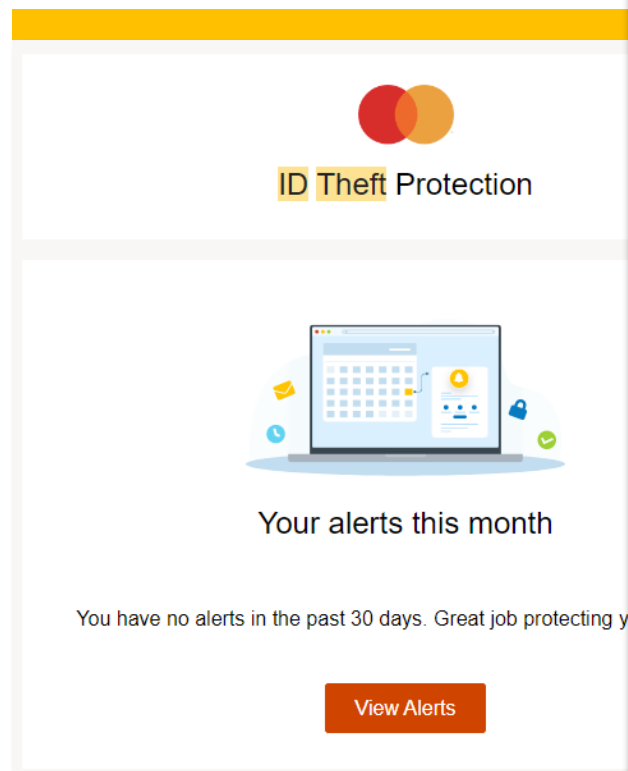
Mastercard ID Theft Protection umożliwia kontrolę własnej tożsamości w Internecie

ALERT ↓

natychmiast powiadamy o podejrzanej aktywności przez:



Email



×

Alert dotyczący tożsamości

Data otrzymania 24.01.2024	Źródło darkweb - breach	Dane Adres e-mail
--	---	---

Szczegóły alertu

Nazwa

◦ Account Email Address

Data odkrycia

10.01.2023

Źródło naruszenia

Twitter (200M) accounts

Opis naruszenia

To jest alert historyczny. Aby poprawić jakość i zakres ochrony, niedawno rozbudowaliśmy naszą usługę monitorowania, dzięki czemu przy skanowaniu sięga ona dalej w przeszłość w poszukiwaniu znanych naruszeń, które mogą zawierać Twoje dane.

Twoje dane osobowe zostały znalezione w breach zidentyfikowanym jako Twitter (200M) accounts. Źródłem było Dark Web. Znalezione to . Naruszone dane obejmowały Nazwa użytkownika, Domena, Identyfikator użytkownika (UID). Ten alert został wywołany w wyniku dopasowania do Twojego pola emails.

Co zostało ujawnione

Nazwa użytkownika, Domena, Identyfikator użytkownika (UID), Adres e-mail, Hasło



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



Zestaw zabezpieczający przed kradzieżą tożsamości

Czy Twoja tożsamość została skradziona? Odwiedź Zestaw ochrony przed kradzieżą tożsamości, aby dowiedzieć się o typowych rodzajach kradzieży tożsamości i sposobach ich rozwiązywania.

Co zrobić?

- Stwierdzono naruszenie co najmniej jednej części danych osobowych lub konta. Zalecamy zwracanie uwagi na swoje konta i zachowanie czujności w przypadku wszelkich potencjalnie podejrzanych działań.
- Jeśli odnaleziono Twoją nazwę użytkownika i/lub hasło, natychmiast zmień hasło do tego konta i do wszystkich innych kont, które używają tego samego hasła. Sprawdź także, czy nie wprowadzono żadnych zmian w ustawieniach zabezpieczeń zainfekowanej wiadomości e-mail. Aby sprawdzić ustawienia zabezpieczeń, przejdź do informacji o swoim koncie e-mail (zwykle znajdujących się w ustawieniach konta) i przejrzyj informacje o koncie oraz bezpieczeństwo konta.

Zestaw do ochrony przed kradzieżą tożsamości

Wprowadzenie

[Czym są kradzież tożsamości i oszustwo – w skrócie](#) >

[Zapobieganie kradzieży tożsamości/oszustwom i wykrywanie ich](#) >

[Pomoc w sprawie kradzieży tożsamości/oszustwa](#) >

Zapobieganie kradzieży tożsamości/oszustwom i wykrywanie ich

[Twoje narzędzie do monitorowania tożsamości](#) >

[Zachowaj bezpieczeństwo i chroń swoje dane \(wskazówki i najlepsze praktyki\)](#) >

Analiza różnych form kradzieży

PODSUMOWANIE

> 10 ZASAD BEZPIECZNEJ BANKOWOŚCI ELEKTRONICZNEJ



> 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

> G0mobile Biznes TO DOSTĘP DO RACHUNKÓW BANKOWYCH ZAWSZE POD RĘKĄ



Autoryzacja mobilna

Przy pomocy wbudowanego tokena mobilnego szybko i bezpiecznie podpiszesz operacje w systemie bankowości internetowej G0online 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 JĚRĚJĚF