www.ksiegowanaswoim.pl

KNS
KSIĘGOWA NA SWOIM

Bezpieczna Księgowa Online

Jak przeciwdziałać cyberatakom?

Michał Sikorski

09.06.2022

www.ksiegowanaswoim.pl

Firma na celowniku

Definicja

Business Email Compromise to **fałszywe wiadomości email** wykorzystywane do przeprowadzania cyberataków wymierzonych w przedsiębiorstwa.

Ataki typu BEC są bardzo skuteczne. Przestępcy oszukują ofiary używając różnych **trików socjotechnicznych**.

www.ksiegowanaswoim.pl

Kategorie ataków BEC

1. Metoda „na partnera biznesowego”
2. Metoda „na prezesa”
3. Przejęcie konta pracownika
4. Metoda „na prawnika”
5. Wyłudzenie danych

www.ksiegowanaswoim.pl

Metoda na „partnera biznesowego”

Cyberprzestępca przejmuje kontrolę nad skrzynką email pracownika

Przejęte konto mailowe jest wykorzystywane do wysyłania korespondencji do klienta

Płatności są przekazywane na konto przestępcy

Oszust otrzymuje pieniądze

www.ksiegowanaswoim.pl

Metoda na „prezesa”

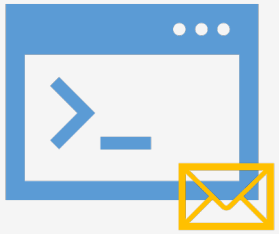
Cyberprzestępca podszywa się pod prezesa i kontaktuje się z osobą z finansów

Środki finansowe są przekazywane na konto przestępcy

Oszust otrzymuje pieniądze

www.ksiegowanaswoim.pl

Przejęcie konta pracownika



Przejęte konto email pracownika jest wykorzystywane do wysyłania żądań o płatności

Środki finansowe są przekazywane na konto przestępcy

Oszust otrzymuje pieniądze

www.ksiegowanaswoim.pl

Metoda „na prawnika”

Cyberprzestępca podszywa się pod prawnika lub kancelarię i kontaktuje się z osobą z finansów

Środki finansowe są przekazywane na konto przestępcy

Oszust otrzymuje pieniądze

www.ksiegowanaswoim.pl

Wyłudzenie danych

Cyberprzestępca przechwytuje konto email pracownika

Przechwycone konto jest wykorzystywane do uzyskania poufnych informacji o innych pracownikach

Poufne informacje są przekazywane na konto cyberprzestępcy

Oszust otrzymuje poufne informacje i wykorzystuje je do przeprowadzenia kolejnych ataków na konkretną osobę

www.ksiegowanaswoim.pl

www.ksiegowanaswoim.pl

Kierowanie decyzjami ludzi

Definicja

Socjotechnika to sztuka zdobywania **władzy nad umysłami**.

Ludzki umysł to jednocześnie **najmocniejszy i najsłabszy element** każdego systemu.

www.ksiegowanaswoim.pl

Zagrożenie

Oszust **preparuje wiadomość email**, aby wyglądała na prawdziwą, i wysyła do jednego z pracowników atakowanej firmy.

W tym celu wykorzystuje **pole tematu**, **sekcję z adresem zwrotnym** oraz **źródło wiadomości**.

www.ksiegowanaswoim.pl

Temat wiadomości (Subject)

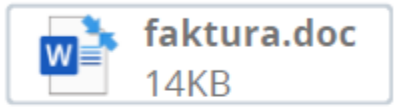
Cyberprzestępcy wykorzystują tytuł wiadomości, żeby nadać jej **ważność** i zwrócić **twoją uwagę**.

W przypadku ponad 66% wykrytych przypadków ataków, tytuły wiadomości zawierały słowa: **przelew**, **płatność, faktura, wezwanie do zapłaty**.

www.ksiegowanaswoim.pl

Przykład

Od Jan Kwiatek <jan.kwiatek@gmail.com>
Do
Temat Zaległa faktura



Cześć,
Czy mogę na Ciebie liczyć? Potrzebujemy wykonać pilny przelew za fakturę dla naszego kontrahenta.

Daj mi znać czy mogę podesłać Ci więcej szczegółów.

Pozdrawiam,
Jan Kwiatek

Sent from my iPhone

www.ksiegowanaswoim.pl

Adres zwrotny (Reply-To)

Przestępca podszywający się pod czyjś adres email,

może wstawić **fałszywy adres** do pola **Reply-To**.

Ta metoda jest bardzo skuteczna. Niestety większość osób

nie sprawdza adresów na które odsyła wiadomość.

www.ksiegowanaswoim.pl

Przykład

Od Adam Skrucha <skruchaa@microsoft.com>
Do Jan Bury
Temat Office 365 na próbę!

Adres Reply-To: **skruchaa@tojestinnadomena.pl**

www.ksiegowanaswoim.pl

Źródło wiadomości (From)

Oszuści korzystają z bezpłatnej poczty elektronicznej lub rejestrują **domenę**, która jest **łudząco podobna** do domeny firmy używanej w ataku.

Stosują różne zabiegi związane z **podmianą liter lub słów**, aby fałszywe nazwy domen wyglądały wiarygodnie.

www.ksiegowanaswoim.pl

Przykład

Od Piotr Wolak <pwolak@rnbank.pl>
Do Mariusz Gielezy
Temat Zmiana regulaminu prowadzenia konta w mBank S.A.

nowy-regulamin.doc
14KB

Adres nadawcy: **pwolak@rnbank.pl**

www.ksiegowanaswoim.pl

Przykład

john.doe@vnder@com	john.doe@under.com
anna.luczka@biuropertekt@.pl	anna.luczka@biuroperfekt.pl
helmut.schmidt@volksvvagen.de	helmut.schmidt@volkswagen.de
einvoices@begim.com	einvoices@begin.com
office@wlll.co.uk	office@will.co.uk
lee.anderson@rnicrosoft.com	lee.anderson@microsoft.com
lucy.wu@pilllow.com	lucy.wu.pillow.com

www.ksiegowanaswoim.pl

Przykład

john.doe@vnder@com	john.doe@under.com
anna.luczka@biuropertekt@.pl	anna.luczka@biuroperfekt.pl
helmut.schmidt@volksvvagen.de	helmut.schmidt@volkswagen.de
einvoices@begim.com	einvoices@begin.com
office@wlll.co.uk	office@will.co.uk
lee.anderson@rnicrosoft.com	lee.anderson@microsoft.com
lucy.wu@pilllow.com	lucy.wu.pillow.com

www.ksiegowanaswoim.pl

www.ksiegowanaswoim.pl

Zarzucanie przynęty

Definicja

Phishing to jedna z głównych technik używanych do **wyłudzania danych.**

Przestępca przechwytuje dane umieszczając w wiadomości email **link do fałszywej strony** lub **złośliwy załącznik**.

www.ksiegowanaswoim.pl

URL skrywa tajemnicę

W niektórych wiadomościach linki URL mogą być **widoczne**,

w innych mogą być „**zamaskowane**”.

Chcesz sprawdzić gdzie prowadzi odnośnik? **Nakieruj na niego wskaźnik myszy i zaczekaj. Nie klikaj w niego!**

www.ksiegowanaswoim.pl

Przykład

mBank System Transakcyjny https://online.rnbank.pl/pl/Login

www.ksiegowanaswoim.pl

Przykład

https://sprawdz.dhl.com.pl/szukaj.aspx

https://zaraz.podasz.mi.swoje.dane.i.nawet.sie.nie.domyslisz.com/cie/okradl.php?id=hahaha

www.ksiegowanaswoim.pl

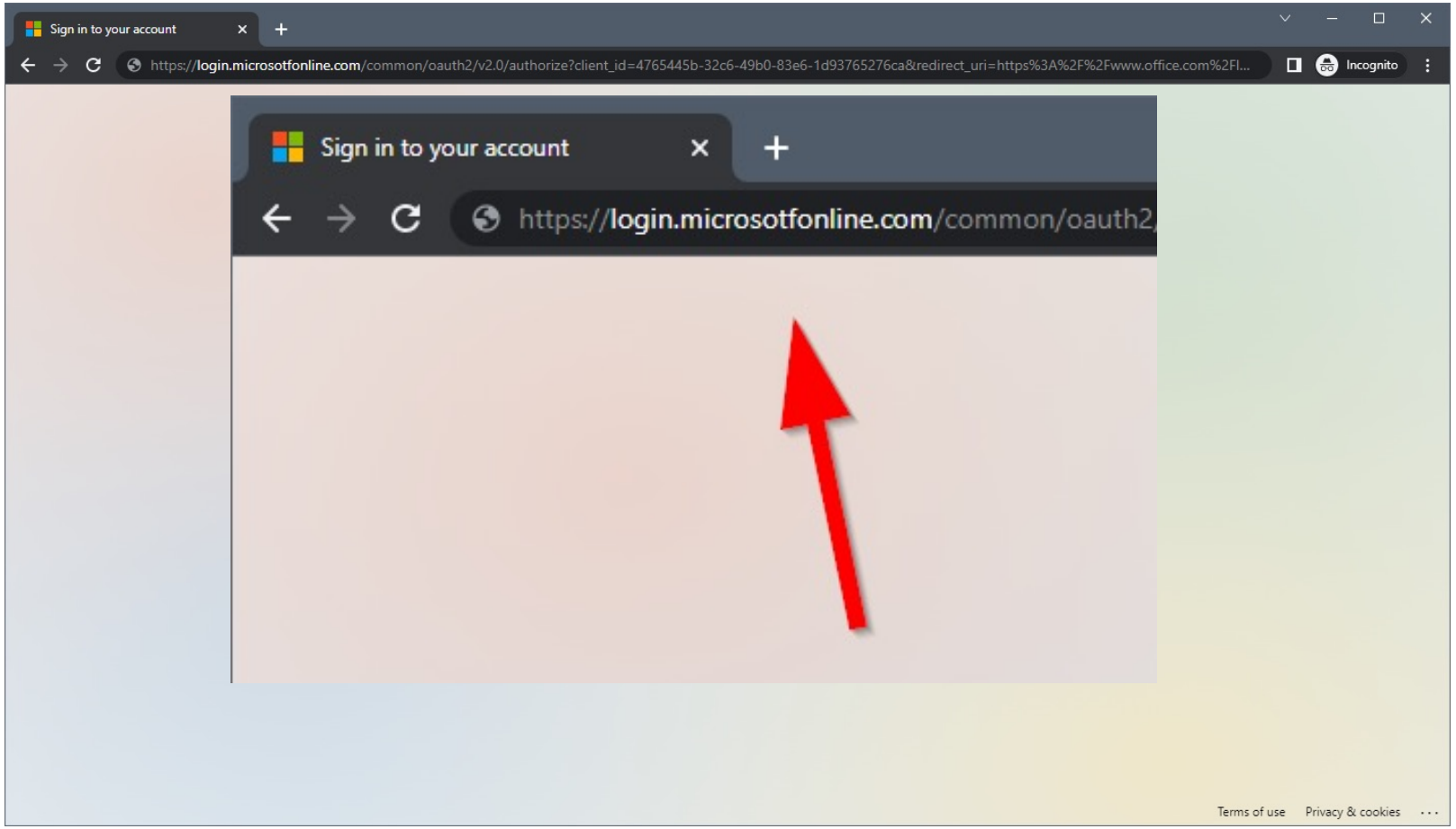
Złośliwe załączniki

Uważaj na załączniki w następujących formatach:

XLS, **DOC**, **PPT**, **HTML**, ale również **PDF** czy **ZIP**.

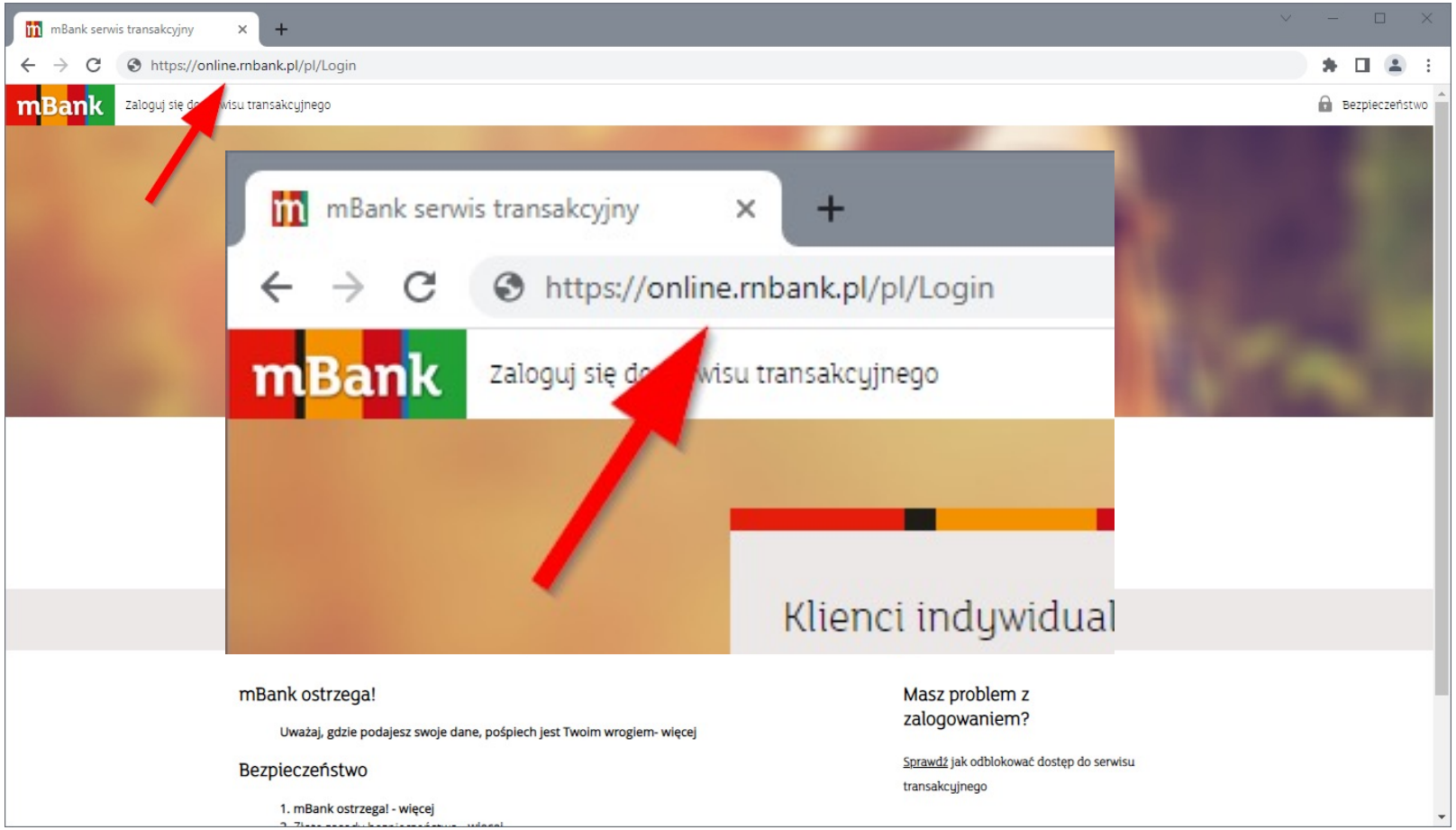
www.ksiegowanaswoim.pl

Przykład



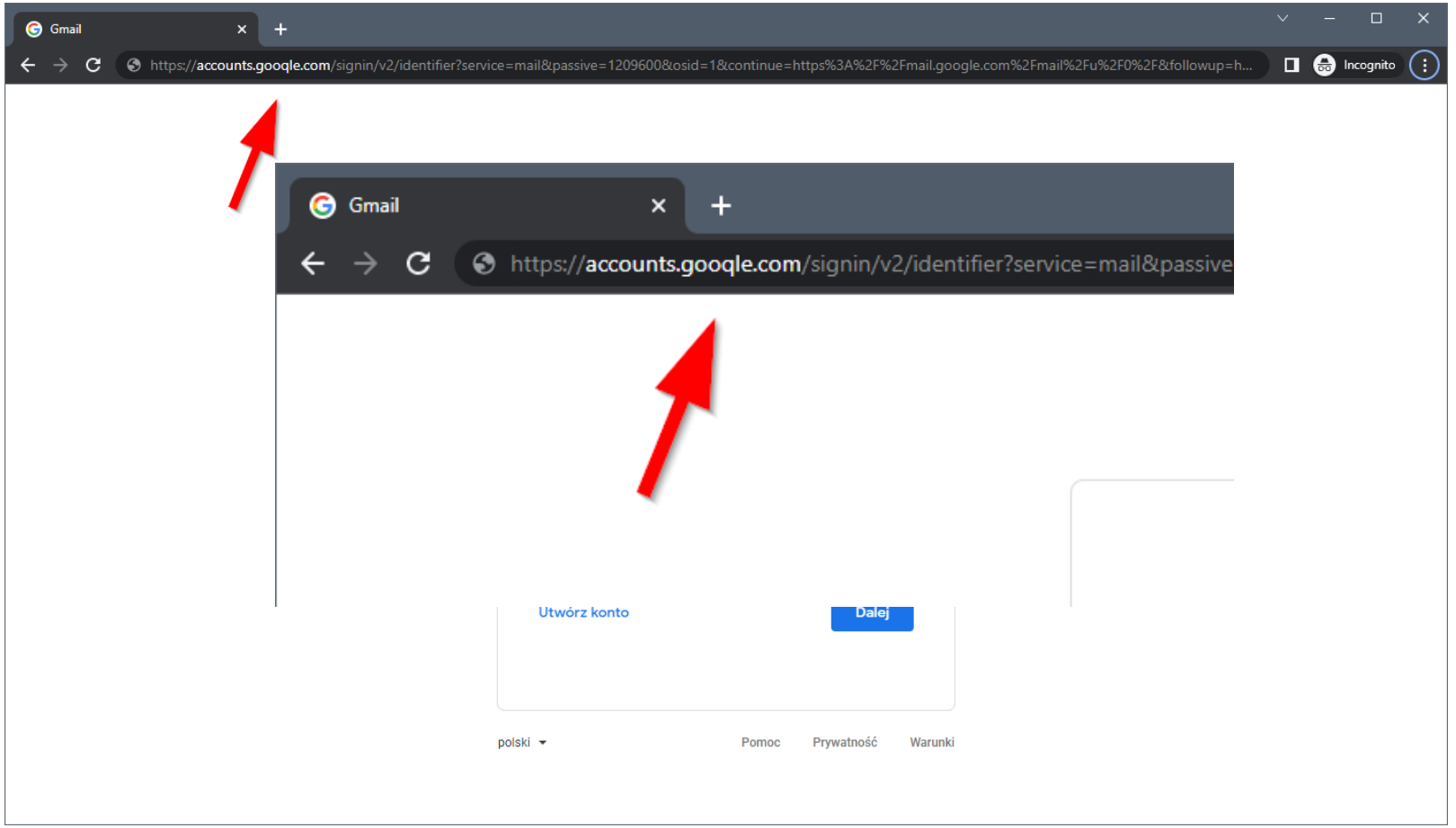
www.ksiegowanaswoim.pl

Przykład



www.ksiegowanaswoim.pl

Przykład



www.ksiegowanaswoim.pl

Bądź czujny!

Adres zaczynający się od **https://** (często kojarzony z symbolem zamkniętej kłódki) **nie chroni Cię przed phishingiem**.

Świadczy tylko o zainstalowanym certyfikacie SSL służącym do **szyfrowania transferu danych**.

www.ksiegowanaswoim.pl

www.ksiegowanaswoim.pl

Długość ma znaczenie

Czy jedno hasło wystarczy?

Musisz mieć **inne hasło** do

każdego z serwisów!

www.ksiegowanaswoim.pl

Długość ma znaczenie

9 znaków ☹️

11 znaków 😟

13 znaków 😕

15 znaków 😐

17 znaków 🙂

19 znaków 😀

21 znaków 😄

23 znaki 🤩

www.ksiegowanaswoim.pl

Stosuj trudne hasła

Dorcia84

Puszek21

Wiosna2022!

Wak@cje2022

Admin1

Janusz4EVA

www.ksiegowanaswoim.pl

Stosuj trudne hasła

Dorcia84

Puszek21

Wio[illegible]22!

Wa[illegible]cje[illegible]22

Admin1

Janusz4EVA

a&#6hDf*9omzzA3

o8uasd0-A%Sn97s9XXw00pa

0-((Sl=^skOll$$gbVz!2_AEr

www.ksiegowanaswoim.pl

Jak zapamiętać tyle haseł?

Używaj **managera haseł**.

www.ksiegowanaswoim.pl

Zalety managera haseł?

- Nie musisz wymyślać nowych haseł.
- Nie musisz wpisywać ich do przeglądarki.
- Nie musisz pamiętać wszystkich haseł.

Musisz **zapamiętać tylko 2 hasła**:

do komputera i **do managera haseł**.

www.ksiegowanaswoim.pl

Który manager haseł wybrać?

KeePass XC

1Password

Dashlane

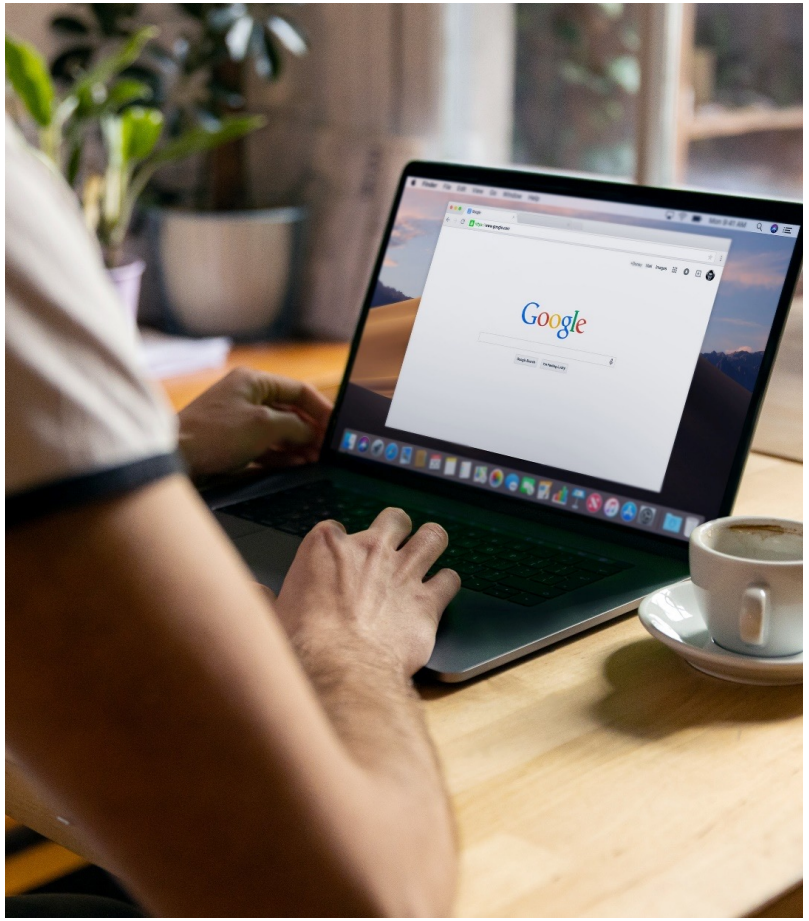
LastPass

BitWarden

www.ksiegowanaswoim.pl

A hasła w przeglądarce?

Możesz używać managera haseł w przeglądarce jeśli nikt inny **nie korzysta** z twojego komputera.



www.ksiegowanaswoim.pl

Pamiętaj!

Manager haseł nie zawsze ochroni cię przed **phishingiem**.

Dlatego stosuj **dwuskładnikowe uwierzytelnianie**.

www.ksiegowanaswoim.pl

Rozwiązanie?

Używaj **klucza U2F**.

W 100% **chroni przed przejęciem dostępu** do twoich kont.

www.ksiegowanaswoim.pl

Co daje mi posiadanie klucza U2F?

Klucz możesz podpiąć do **wielu serwisów**.

Kluczem możesz również **zabezpieczyć managera haseł**.

www.ksiegowanaswoim.pl

O czym należy pamiętać?

Kup minimum **2 klucze**.

Podpinając klucz do konta,

odepnij telefon.

www.ksiegowanaswoim.pl

Klucze są za drogie?

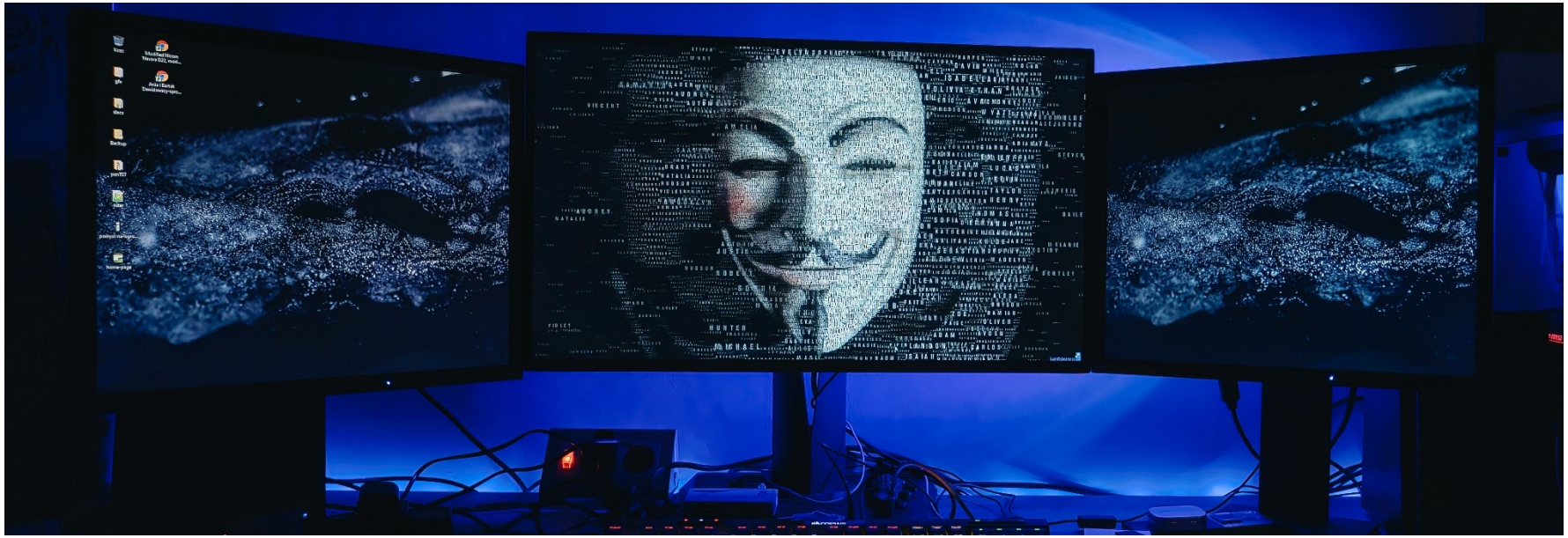
Zainstaluj aplikację **Google Authenticator**.

Podepnij ją do serwisów, **odepnij telefon**.

Google Authenticator nie ochroni tak dobrze jak klucz U2F.

www.ksiegowanaswoim.pl

Sprawdź się…



https://haveibeenpwned.com

www.ksiegowanaswoim.pl

www.ksiegowanaswoim.pl

Najlepsze praktyki

Najlepsze praktyki

Nigdy **nie trać czujności** wykonując rutynowe zadania.

www.ksiegowanaswoim.pl

Najlepsze praktyki

Zachowaj szczególną **ostrożność** przy prośbach o **płatność**, którym towarzyszy **zmiana danych bankowych**.

www.ksiegowanaswoim.pl

Najlepsze praktyki

Bądź czujny podczas rozmów z **nieznanymi osobami** lub osobami,

których tożsamości nie możesz sprawdzić.

www.ksiegowanaswoim.pl

Najlepsze praktyki

Zwracaj uwagę na **wygląd adresów email**, z których dostajesz prośby o **przelew** lub **zmianę danych bankowych**.

www.ksiegowanaswoim.pl

Najlepsze praktyki

Zwracaj uwagę na **literówki** w adresach email i URL.

www.ksiegowanaswoim.pl

Najlepsze praktyki

Regularnie zmieniaj **hasła**.

Nie udostępniaj ich nikomu!

www.ksiegowanaswoim.pl

Najlepsze praktyki

Stosuj **kilkuetapową weryfikację** transakcji.

www.ksiegowanaswoim.pl

Najlepsze praktyki

Zachowaj **ostrożność** w mediach społecznościowych.

Nie publikuj szczegółów dotyczących pracodawcy.

www.ksiegowanaswoim.pl

Najlepsze praktyki

Korzystasz z bankowości online?

Zmień limity dla przelewów i kart.

www.ksiegowanaswoim.pl

Najlepsze praktyki

W sieci **płać kartą** zamiast przelewem czy BLIKiem.

Płatność kartą jest **najbezpieczniejsza**.

www.ksiegowanaswoim.pl

Najlepsze praktyki

Włącz **weryfikację dwuskładnikową**.

Do banku loguj się z użyciem **aplikacji mobilnej**.

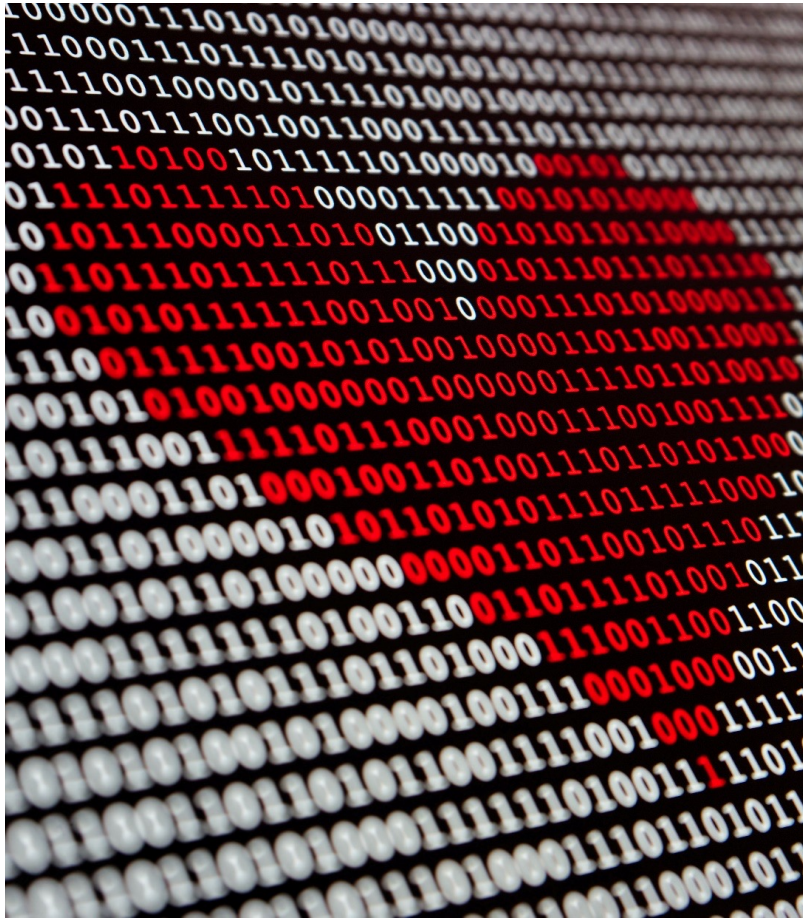
Nie korzystaj z kodów SMS.

www.ksiegowanaswoim.pl

Najlepsze praktyki

Rób **kopie bezpieczeństwa**.

Na dyskach zewnętrznych oraz w chmurze.



www.ksiegowanaswoim.pl

Czy są jakieś pytania?

www.ksiegowanaswoim.pl

www.ksiegowanaswoim.pl

Dziękuję!