

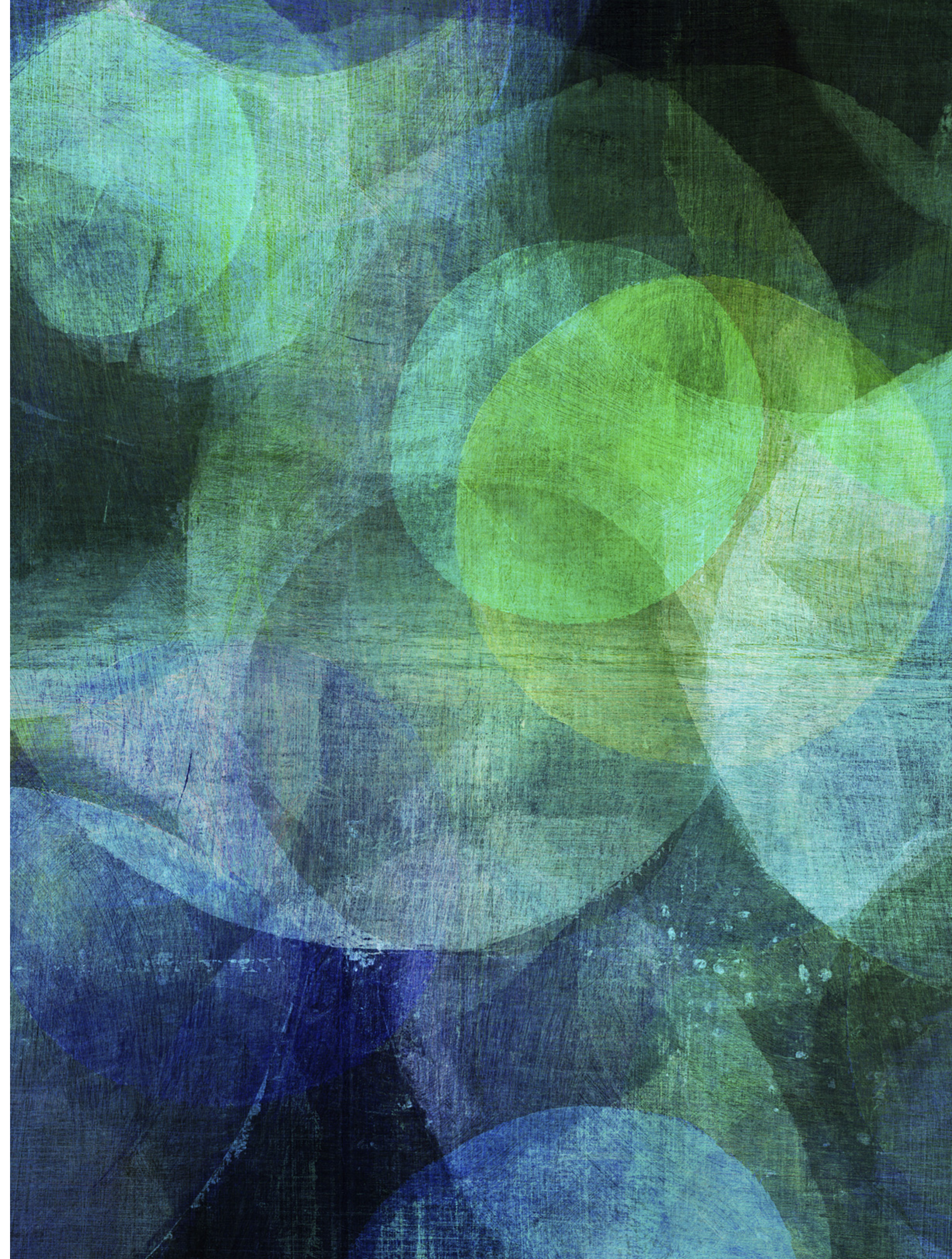


SZKOLENIE UŚWIADAMIAJĄCE

Maciej Ziarek

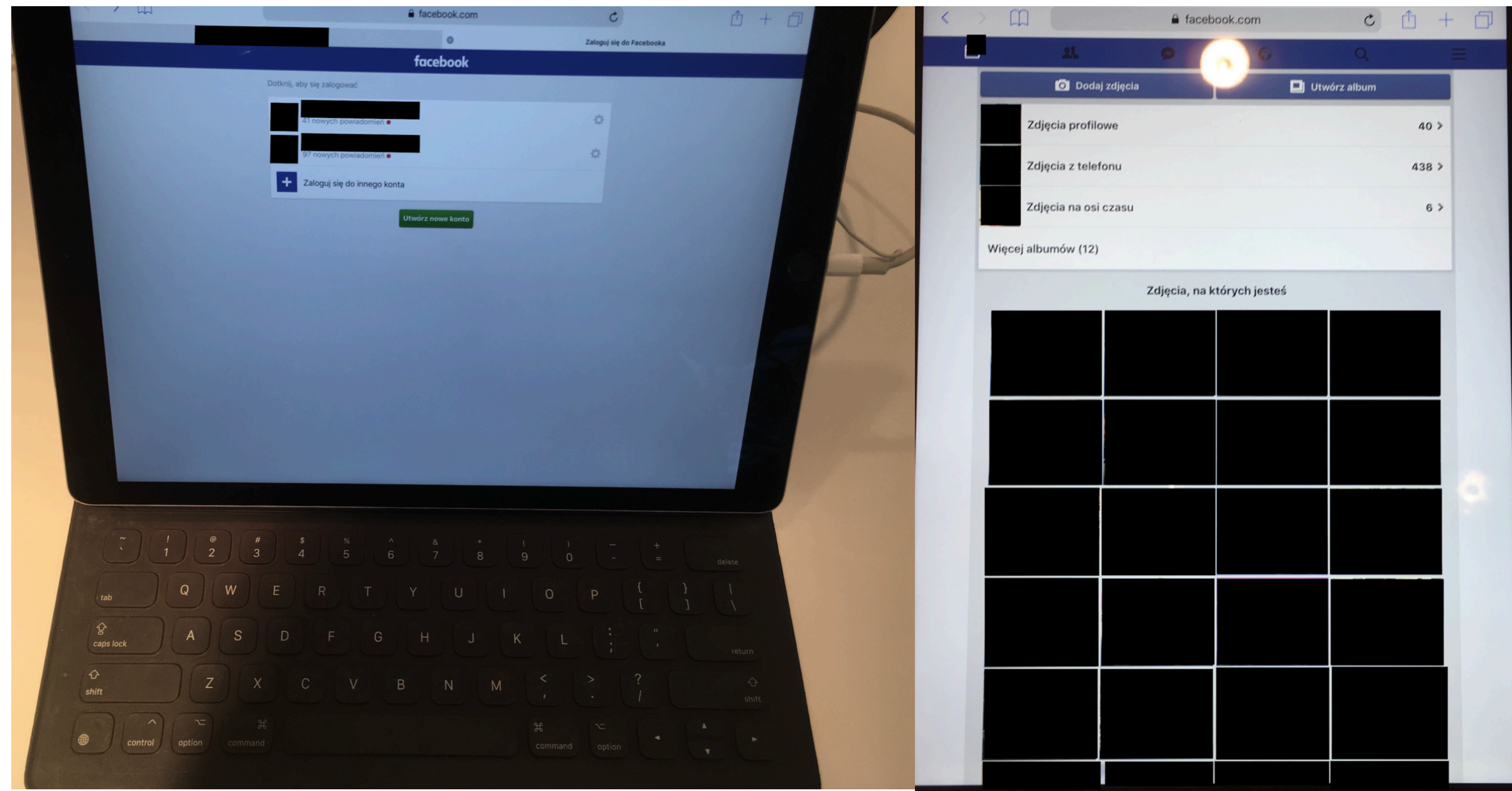
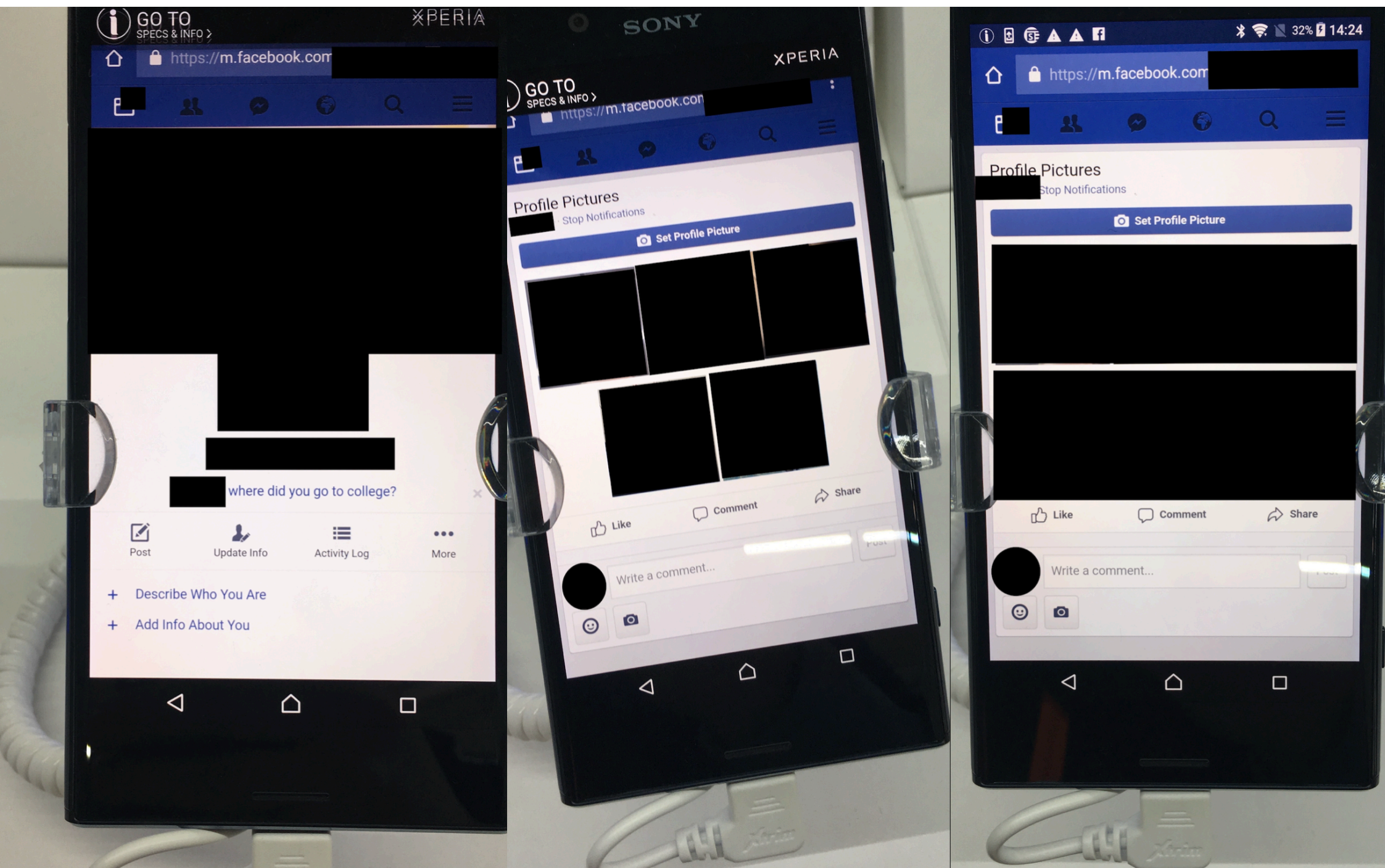
CELE SZKOLENIA

Korzyści dla każdego



DLACZEGO ATAKI SĄ UDANE?

- Brak wiedzy na temat współczesnych ataków
- Szybkie i pochopne decyzje
- Wykorzystywanie cudzego wizerunku przez atakujących
- Stawianie wygody ponad bezpieczeństwo



Powyższe zdjęcia pokazują urządzenia z różnych wystaw sklepowych i marketów. Jak widać niektóre osoby zostawiały zalogowane konta, a niekiedy zapisane hasła na publicznie dostępnych urządzeniach. Każdego dnia oglądały je setki osób i mogły wykorzystać te dane do stworzenia fałszywego konta lub innego ataku.

Fałszywe konkursy są prawdziwą plagą na portalach społecznościowych. Jeżeli oferta jest bardzo atrakcyjna, to należy dwa razy zapoznać się z jej treścią.

Because the people who are crazy enough to think they can change the world are the ones who do.
Steve Jobs
1966-2011

iPhone5
27.993 osoby lubią to · 4 osoby o tym mówią

Społeczność
Rozdajemy najnowsze telefony marki Apple. Już od 21 września wysyłamy iPhone'y 5!

Lubię to! Wiadomość

Zdjęcia Kliknięcia „Lu...”

Napisz post Zdjęcie

Aktywność znajomego

iPhone5
6 godz. temu · 🌐

Otrzymaliśmy 500 telefonów iPhone 5 16GB, które z powodu braku ofoliowania telefonu (folia zabezpieczająca przy transporcie) nie mogą być wystawione na sprzedaż. Z tego powodu wylosujemy 500 osób, które udostępnią ten status i polubią naszą stronę.

Kolor podaj w komentarzu. Powodzenia.

Lubię to! · Dodaj komentarz 14 tys. 24 tys.

Ten przykład pokazuje metodę działania. Ktoś podszywa się pod znanego piłkarza i sugeruje, że do wygrania jest nowe auto. Widać, że kilka tysięcy osób uwierzyło, że profil jest prawdziwy. Wiele z nich otrzymała następnie komunikat z prośbą o wpłacenie pieniędzy. Takie ataki nie wymagają wiele wysiłku, a niestety można stracić pieniądze.

W związku z Nowym Rokiem postanowiłem dla was zrobić mega PREZENT! ❤️
mianowicie wystawiam na konkurs moją nową Audi RS7!
Auto może wygrać każdy kto weźmie udział w konkursie.
Zasady konkursu:
UDOSTĘPNIJ TEN POST
POLUB MOJĄ STRONĘ
DODAJ KOMENTARZ "GOTOWE"...
Czytaj dalej



3 373 Komentarze: 7 316 Udostępniono 5 281 razy

Start Robert Lewandowski Kont... > Zarządzaj
Aktywny(a) teraz

Witaj [redacted] Mam dla ciebie wiadomość! wylosowałem właśnie ciebie do odebrania mojej Audi! w celu potwierdzenia swoich danych wyślij przelew w kwocie 200zł(zwróce ci je) na numer 15 1140 2004 0000 3102 7644 1605 Robert Lewandowski.

Wpisz wiadomość...

Na tym przykładzie widzimy fragment artykułu, który informuje o skutkach cyberataku na Urząd Pracy w Malborku. Przyczyną była prawdopodobnie infekcja szkodliwym oprogramowaniem np. poprzez otwarcie załącznika dołączonego do e-maila. Jest to często spotykana metoda, dlatego zawsze należy dokładnie sprawdzać nadawcę i przeanalizować treść wiadomości.

Hakerzy okradli Urząd Pracy w Malborku. Prawdopodobnie wystarczył jeden e-mail

I.O., pszl 10.06.2015, 16:33 | aktualizacja: 16:57



■ Prokuratura zaznacza, że namierzenie oszustów będzie bardzo trudne (fot. Pixabay.com)

20 tys. zł przelał za pośrednictwem bankowości elektronicznej jeden z pracowników Powiatowego Urzędu Pracy w Malborku. Nie byłoby w tym nic dziwnego, gdyby nie to, że pieniądze trafiły na zupełnie inny rachunek, niż planowano. Urząd padł ofiarą ataku hakerskiego – sprawą zajęła się prokuratura.

Dość szybko zorientowano się, że operacja bankowa nie przebiegła po myśli. Bank, do którego trafiły środki, założył blokadę na konto, dzięki czemu udało się uratować blisko 9 tysięcy złotych.

Reszta pieniędzy została przetransferowana przez oszustów na inne konta.

Pracownicy urzędu są poza kręgiem podejrzeń, a na obecnym etapie wygląda na to, że wszystko odbyło

Kolejny przykład cyberataku. Tym razem suma wyniosła niemal milion złotych. Niestety z roku na rok przypadków utraty pieniędzy przez firmy i instytucje jest coraz więcej. Dlatego tak istotne jest edukowanie i zrozumienie wybranych mechanizmów atakowania np. poprzez pocztę elektroniczną.

Chcieli zrobić przelew, stracili 940 tysięcy. Ktoś okradł urząd miasta w Jaworznie

20 stycznia 2015, 10:52



Podziel się



Udostępnij

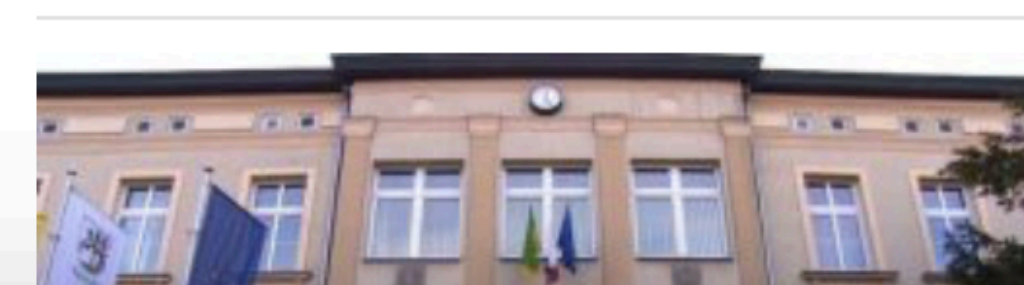


Z konta Jaworzna zniknął blisko milion złotych

Foto: Bartosz Rejmoniak / TVN 24 Katowice | Video: Bartosz Rejmoniak / TVN 24 Katowice

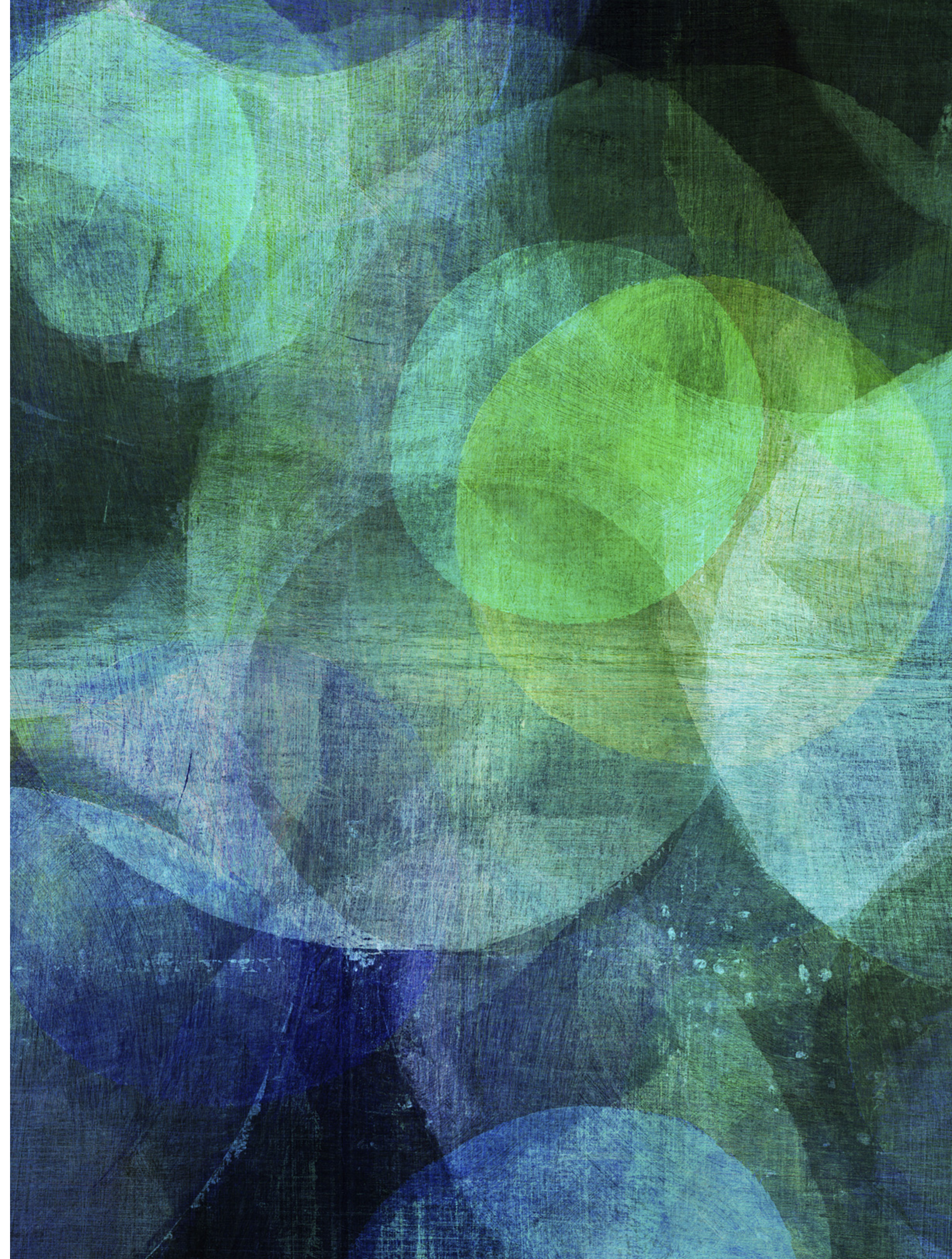
Prawie milion złotych zniknął z kasy urzędu miejskiego w Jaworznie. - Kwota najprawdopodobniej "wyparowała" przy okazji transakcji bankowej - informuje rzecznik magistratu.

"13 stycznia Urząd Miejski w Jaworznie padł ofiarą przestępstwa internetowego na koncie gminy. W trakcie realizacji jednego z przelewów bankowych doszło do kradzieży" - czytamy w komunikacie przesłanym przez Sebastiana Kusia, rzecznika jaworznickiego magistratu. "O



SOCJOTECHNIKA

Jak nami manipulują?

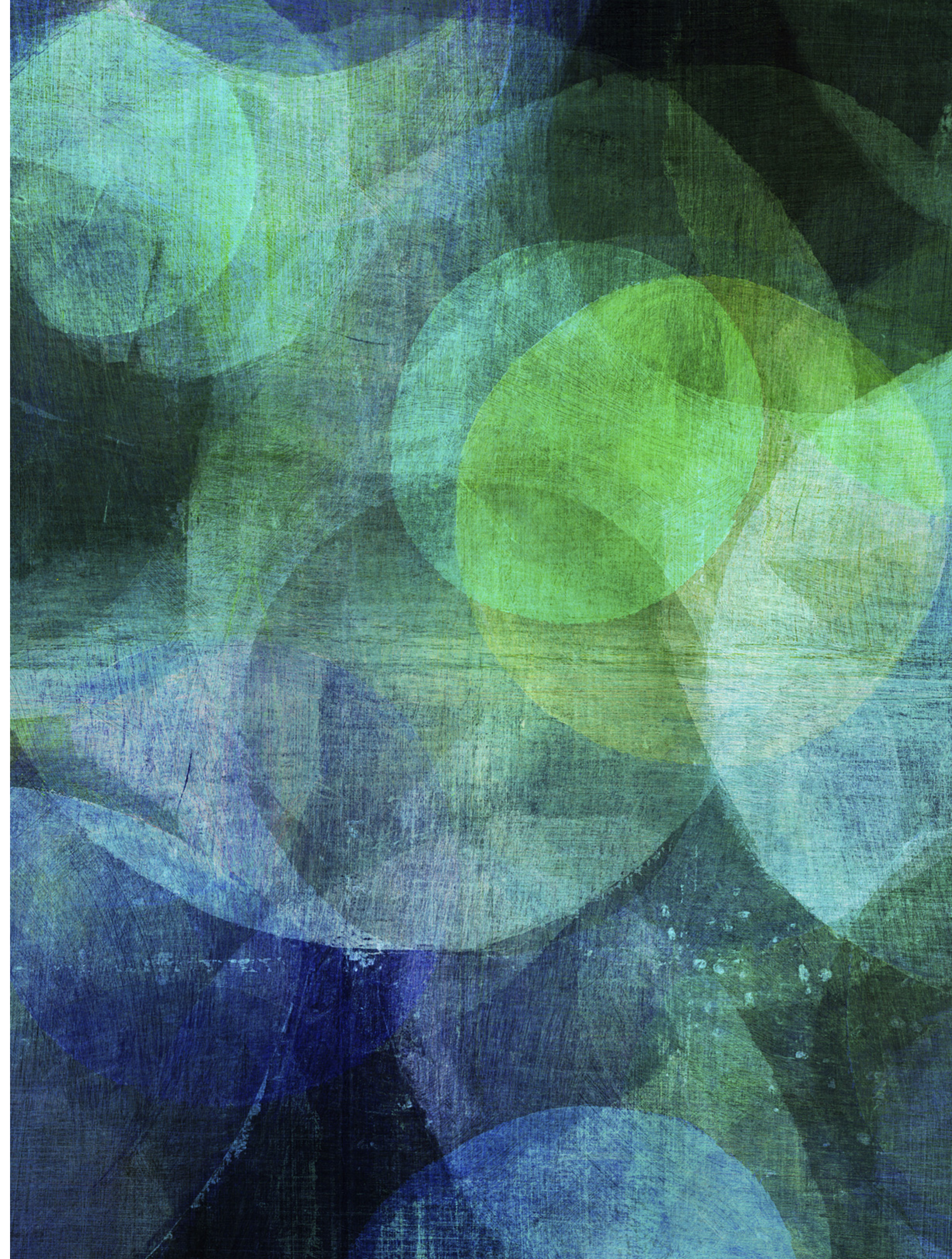


SOCJOTECHNIKA

- Metoda manipulowania w celu uzyskania określonego efektu
- Wykorzystywane na co dzień w marketingu i reklamie
- Każdy rodzaj współczesnego ataku zawiera elementy socjotechniki
- Socjotechnikę dzielimy na pośrednią i bezpośrednią
- Pośrednia to np. fałszywe maile masowo wysyłane do różnych osób z prośbą o zalogowanie się na konkretnej stronie
- Bezpośrednia to atak w konkretne osoby lub firmy, gdzie atakujący może podszywać się pod np. przełożonego

PHISHING

Czym jest i jak go rozpoznać?



CZYM JEST PHISHING?

- Nakłanianie do wykonania określonych czynności
- Próba podrobienia wizerunku określonej firmy, instytucji lub osoby
- Możliwość kradzieży pieniędzy i danych
- Bardzo prawdopodobna infekcja systemu operacyjnego

Phishing często zawiera błędy językowe, gdyż może być tłumaczony z innego języka. To jedna z pierwszych wskazówek, że coś z mailem jest nie tak.

222 Poczta Polska

Do:

615339 Twoja przesyłka nie została dostarczona

Dzień dobry

Przesyłka nie została doręczona odbiorcy w dniu 9 październik 2015, ponieważ nikt nie otworzył kurierowi. Kliknij na link w celu otrzymania informacji ~~dotyczącej~~ twojej paczki w naszym serwisie. Odbiór przesyłki możliwy w najbliższym biurze po przedstawieniu wydrukowanej informacji.

**Informacja o numerze twojej
przesyłki**

Z poważaniem,
~~XXXXXXXXXXXXXXXXXXXXXXXXXXXX~~

Poczta Polska.

[unsubscribe](#)

Ten przykład polega na przekonaniu użytkownika, że otrzymał fakturę. Oczywiście nie ma to nic wspólnego z operatorem komórkowym. Ktoś wykorzystuje jego logo po to by użytkownik otworzył załącznik. W rzeczywistości nie jest to PDF, a szkodliwy program. Najlepszym sposobem na zweryfikowanie wiadomości jest sprawdzenie swojego unikatowego nr klienta.



Szanowni Państwo,

Pragniemy przypomnieć o nieuregulowanej Fakturze o numerze **F/20249758/09/14** wystawionej w dniu **12/09/2014**. Opłacenie Faktury po terminie będzie skutkowało naliczeniem odsetek ustawowych.

Jak czytać fakturę? - **instrukcja**.

Forma płatności:	Przelew / Foto wpłata
Termin płatności:	21/09/2014
Nazwa wystawcy:	P4 sp. z o.o. ul. Tasmowa 7, 02-677 Warszawa, NIP 951-21-20-077
Kwota do zapłaty	107,27 zł
Numer konta:	46 1090 0004 7777 0100 2573 5659
Zalecany tytuł przelewu:	Play faktura F/20249758/09/14 klient 25735659

Pobierz Fakturę:



Dziękujemy za terminowe dokonywanie płatności, które chroni przed naliczaniem odsetek ustawowych.

Jednocześnie informujemy, że archiwum e-faktur znajduje się na serwisie **Play24**, gdzie można sprawdzić integralność treści i autentyczność pochodzenia załączonej faktury.

Zachęcamy do wypełnienia ankiety na temat e-faktury. Ankieta dostępna jest po zalogowaniu do Play24 w zakładce Faktury. Państwa opinia jest dla nas bardzo ważna. Dziękujemy!

☆ Preawizacja DHL

Do: [redacted]

Preawizacja DHL



Preawizacja DHL

Szanowni Państwo,

Otrzymaliśmy elektroniczne dane przesyłki nr 98626977650 z firmy [redacted] Przesyłka nadal pozostaje w rękach nadawcy. Po przekazaniu jej Kurierowi DHL PARCEL prześlemy aktualny status wraz z planowanym terminem doręczenia.

Pozdrawiamy,
DHL Parcel

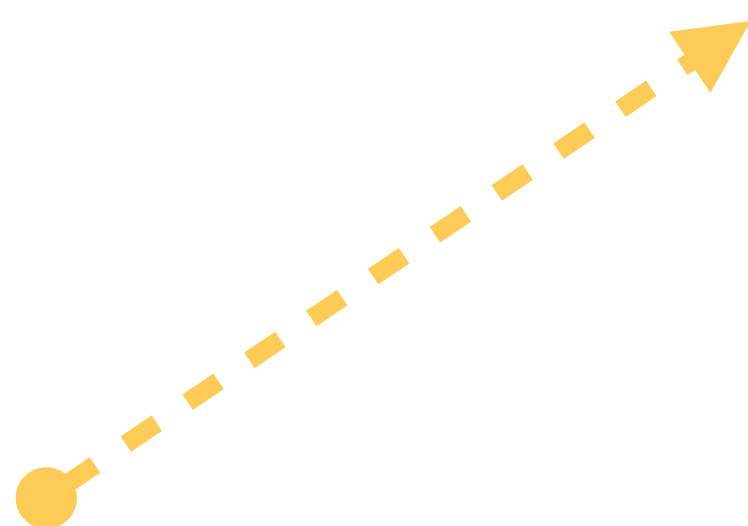
www.dhlparcel.com.pl

Jeśli chcieliby Państwo otrzymywać drogą elektroniczną informacje o promocjach, nowych produktach i usługach, prosimy o wyrażenie zgody na stronie internetowej DHL. Wypełnienie formularza zajmie tylko 2 minuty.

UWAGA: Wiadomość ta została wygenerowana automatycznie. Prosimy nie odpowiadać funkcją



Parcel_Przesylka.18.12.
2015.zip



11 1111 1111 1111 1111 1111 1111



99 9999 9999 9999 9999 9999 9999

Niektóre typy szkodników, jak np. VBKlip, potrafią wykryć kopiowanie nr konta i zastępują go własnym. Jeżeli komputer jest zainfekowany, to skopiowanie nr z faktury spowoduje wklejenie nr konta przestępcy i utratę pieniędzy. Zawsze należy weryfikować wklejony nr konta i SMS-y od banku, by mieć pewność gdzie wysyłamy pieniądze.

Wiadomość oczywiście nie pochodzi od firmy kurierskiej

From: mBank [<mailto:klienci@esseaservizi.com>]

Sent: Thursday, January 26, 2017 6:10 PM

To:

Subject: Masz 1 nową ważną zabezpieczeń wiadomość

Masz 1 nową ważną zabezpieczeń wiadomość

Aby przeczytać wiadomość, kliknij na link poniżej i zaloguj się:

<https://online.mbank.pl/pl/Login>

Uwaga na zagrożenia związane z routerami - więcej

From: mBank [<mailto:klienci@esseaservizi.com>]
Sent: Thursday, January 26, 2017 6:10 PM
To:
Subject: Masz 1 nową ważną zabezpieczeń wiadomość


Masz 1 nową ważną zabezpieczeń wiadomość

Aby przeczytać wiadomość, kliknij na link poniżej i zaloguj się:
<https://online.mbank.pl/pl/Login>

Powyższa wiadomość jest fałszywa. Banki nigdy nie proszą użytkownika o zalogowanie się pod adresem wskazanym we wiadomości. Dodatkowo mail zawiera błędy, a domena kompletnie nie wskazuje na bank. Co by się jednak stało, gdyby ktoś zdecydował się kliknąć odnośnik?

mBank - serwis transakcyjny

www.reheat.cz/mb/sms/index.html?https://online.mbank.pl/pl/Login?SMS=verify



Na Twój telefon została wysłana wiadomość SMS kod. Wpisz otrzymane SMS kod by potwierdzić dane i wybierz Zaloguj się


Zaloguj się

Weź kredyt gotówkowy w mBanku
pieniądze na dowolny cel na Twoim koncie

Bezpieczeństwo

1. Uwaga na zagrożenia związane z podmianą rachunku - [więcej](#)
2. Przed potwierdzeniem operacji przeczytaj uważnie SMS-a z kodem, aby upewnić się, że dotyczy on właściwej operacji
3. Konsultant mBanku nie pyta o hasło podczas rozmowy przychodzącej czy wychodzącej
4. mBank nie każe podawać haseł jednorazowych podczas logowania do serwisu transakcyjnego - [więcej](#)
5. Zawsze sprawdzaj certyfikat SSL i adres URL - [więcej](#)
6. mBank nigdy nie prosi o instalację certyfikatów na telefon komórkowy - [więcej](#)
7. Uwaga na zagrożenia związane z routerami - [więcej](#)

Kontakt



mLinia
801 300 800

Zostałby przeniesiony na witrynę wyglądem przypominającą stronę banku, ale w rzeczywistości kompletnie z nim nie związana. Wystarczy sprawdzić certyfikat strony i domenę. Ta strona jest fałszywa i nie należy na niej podawać żadnych danych!

(2) Wróć na mBank.pl

mBank S.A. [PL] mbank.pl/indywidualny

Oferta indywidualna Private banking Oferta dla firm MSP i korporacje

Kontakt Otwórz konto osobiste Zaloguj

Konta Kredyty Karty Lokaty i oszczędności Inwestycje Ubezpieczenia Oferta Premium Usługi (500+) Aktualne promocje Aplikacja mobilna Oferta dla młodych

Identyfikacja witryny internetowej

DigiCert identyfikuje tę witrynę jako mBank S.A. Warszawa, Mazowieckie PL

Połączenie z serwerem jest szyfrowane. [Czy można ufać tej witrynie?](#)

Konto osobiste + 110 zł premii

Otwórz konto i w ciągu 3 dni zasil je kwotą 500 zł, a **otrzymasz 110 zł premii**

Sprawdź promocję >

Nota prawna

Nota prawna

Promocyjne konto osobiste ze **zwrotem do 650 zł za zakupy**

Dwuletnia gwarancja niezmienności cen: 0 zł za konto, kartę, przelewy i bankomaty¹

Sprawdź szczegóły

Nota prawna

Otwórz **konto dla młodych**

Odbierz **110 zł w promocji**

Sprawdź szczegóły



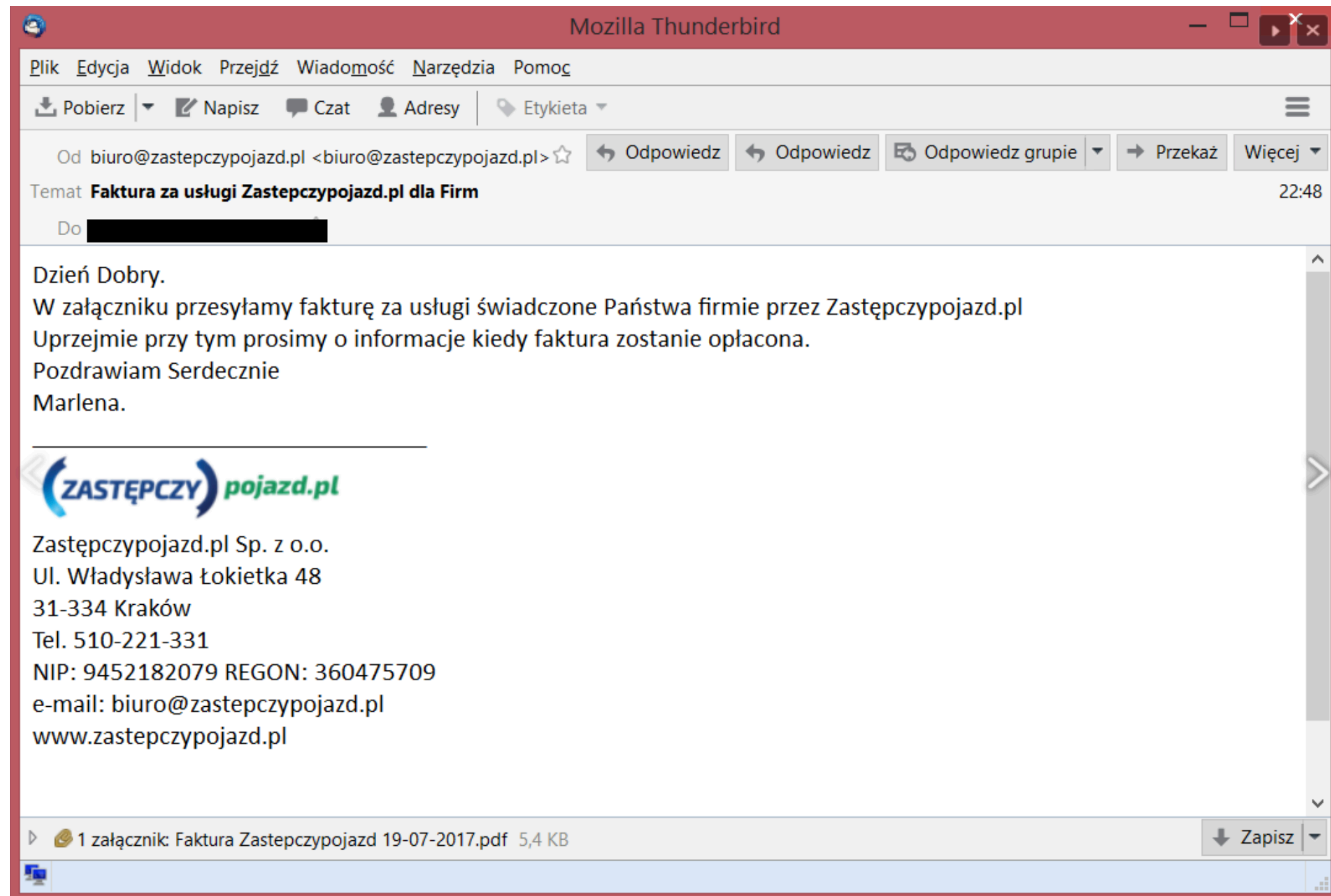
Jesteśmy nowym partnerem bankowym Wielkiej Orkiestry Świątecznej Pomocy!

14 stycznia 2018 roku odbędzie się 26. Finał Wielkiej Orkiestry Świątecznej Pomocy. Fundacja WOŚP pozyskiwać będzie środki na zakup sprzętu ratującego zdrowie i życie dzieci na oddziałach noworodkowych w całej Polsce.

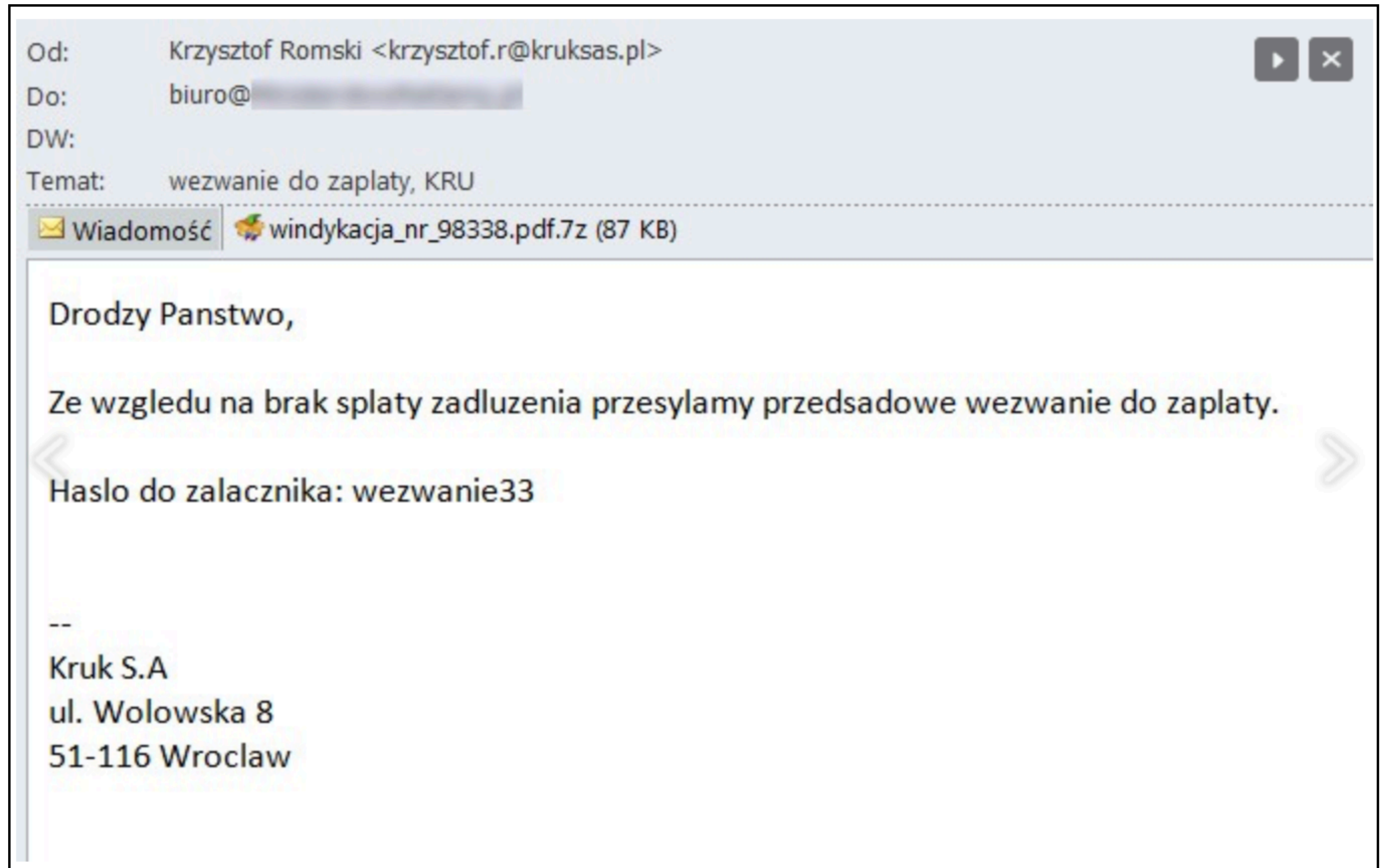
[Przeczytaj więcej](#)

Dla przykładu - powyższa strona jest prawdziwa. Widać certyfikat, który poświadcza, dla jakiej domeny został wystawiony.

Ta wiadomość jest wyjątkowo wyrafinowana. W tym przypadku ktoś podszywa się pod firmę wynajmującą pojazdy. Problem w tym, że domena wygląda na prawdziwą. Dzieje się tak dlatego, że nagłówek wiadomości można łatwo sfałszować. Z tego powodu, jeżeli nie kojarzymy firmy i nigdy się z nią nie kontaktowaliśmy - nie otwieramy załączników i nie klikamy odnośników. Ta wiadomość jest fałszywa, a autor podszył się pod firmę.



Na tym przykładzie ktoś podszywa się pod firmę windykacyjną. Bardzo łatwo można rozpoznać, że jest to phishing. W treści podane jest hasło do załącznika. Jest to próba ominięcia zabezpieczeń antywirusowych. Zabezpieczony plik może nie zostać przeskanowany. Dodatkowo sam fakt spakowania pliku jest już niepokojący.



Temat: Zweryfikuj swoje konto pocztowe wum.edu.pl teraz !!

Data: 2018-10-06 15:33

Od: "Warszawski Uniwersytet Medyczny Administrator poczty internetowej"

Do:

Drogi wum.edu.pl Użytkownik konta e-mail,

Twój rozmiar skrzynki osiągnął szacowany limit przydziału i część Twojej przychodzącej wiadomości e-mail oczekują na nasz serwer z powodu tego problemu, musisz uaktualnić swoje konto, aby nie przekroczyć limitu przydziału i poczekaj kilka godzin, a my to sprawdzimy i naprawimy.

Proszę wypełnić poniżej:

Adres e-mail:
Nazwa Użytkownika:
Hasło:

Niewykonanie aktualizacji może spowodować usunięcie konta e-mail.

Dziękuję Ci
Webmanager
Mailadmin,
Warszawski Uniwersytet Medyczny | Medical University of Warsaw
Żwirki i Wigury 61, 02-091 Warsaw, Poland,
© 2018 Warszawski Uniwersytet Medyczny

Phishing może być wysyłany na adresy np. uczelni. Ktoś podszywa się pod np. administratora i namawia użytkowników do podania danych konta. Tego typu prośby należy ignorować!

From:

Sent: Friday, June 22, 2018 10:40 AM

Subject: Pilne Zawiadomienie!!

Drogi posiadaczu konta,

Certyfikat Twojego konta e-mail w programie Outlook Exchange / OWA wygaś 17-06-2018, może to przerwać konfigurację dostarczania wiadomości i błąd strony podczas wysyłania wiadomości. Kliknij [WUM](#), aby zaktualizować swoje konto, aby uniknąć zawieszenia.

Z poważaniem,

Helpdesk IT.

-----Original Message-----

From: Administrator systemu

Sent: Wednesday, August 29, 2018 10:14 AM

To: Recipients

Subject: Twoja skrzynka pocztowa!

Twoja skrzynka pocztowa przekroczyła limit przestrzeni dyskowej ustalony przez administratora, możesz nie być w stanie wysłać ani odbierać nowej poczty, dopóki nie zweryfikujesz ponownie skrzynki pocztowej. Aby ponownie zweryfikować swoją skrzynkę pocztową, wyślij następujące informacje poniżej:

Nazwa:
Nazwa Użytkownika:
Hasło:
Wpisz ponownie hasło:
Adres e-mail:
Numer telefonu:

Jeśli nie uda się ponownie zweryfikować skrzynki pocztowej, twoja skrzynka zostanie dezaktywowana !!!

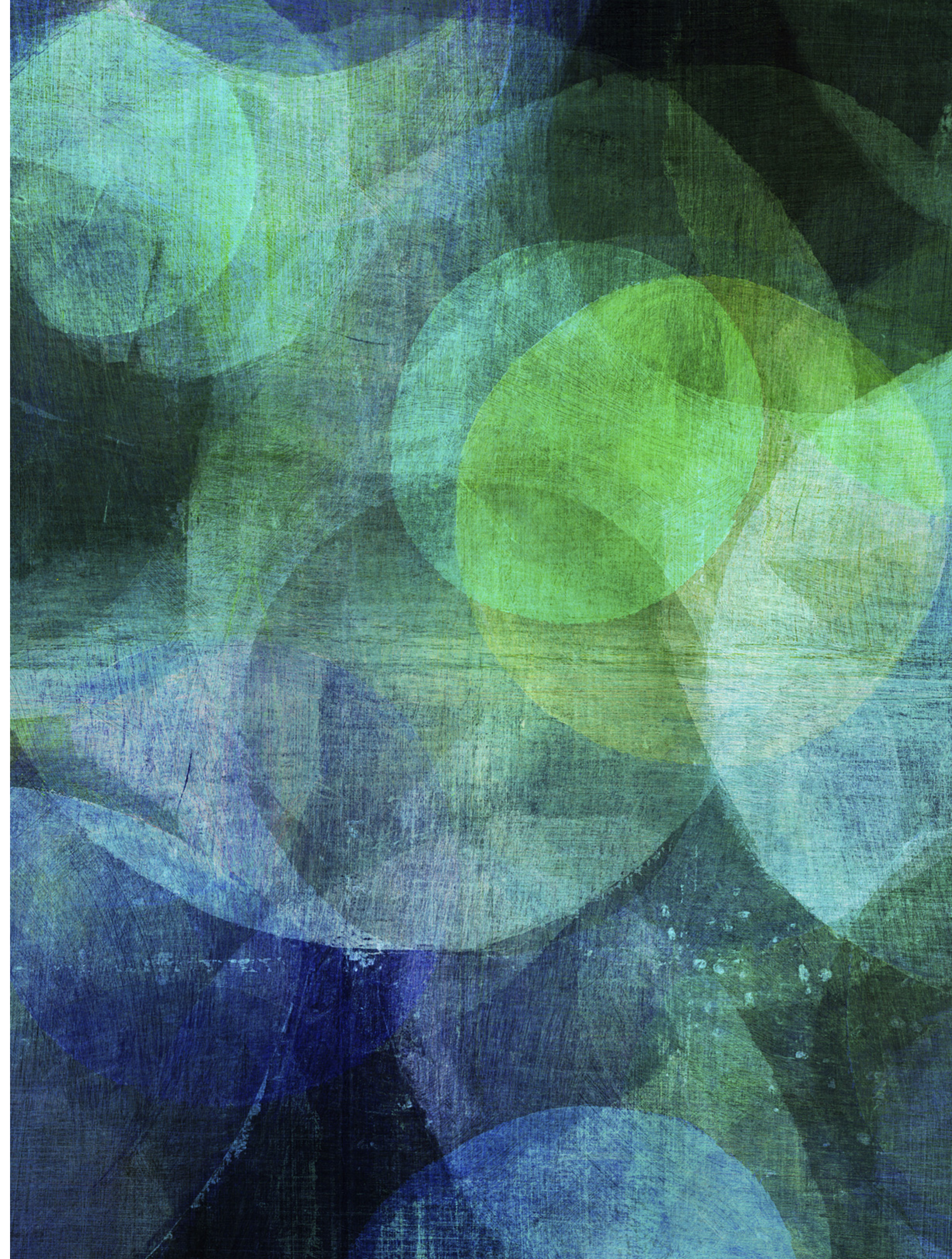
Dzięki
Administrator systemu

NA CO ZWRÓCIĆ UWAGĘ?

- Treść listu może zawierać błędy stylistyczne
- Wiadomość może być szokująca, emocjonalna
- Otrzymujemy maila, którego się nie spodziewamy
- Prośba o podanie loginu, hasła lub przejścia na wskazaną stronę
- Dane spakowane programem do archiwizacji
- Załącznik zabezpieczony hasłem

RANSOMWARE

Czym jest i jak go rozpoznać?



CZYM JEST RANSOMWARE?

- Program szyfrujący pliki na urządzeniu
- Za odzyskanie dostępu, użytkownik musi zapłacić (zły pomysł)
- Najczęściej jest połączony z atakiem phishingowym ale z powodzeniem przenosi się także poprzez dyski zewnętrzne
- Atak może nastąpić również w wyniku zaniedbania aktualizacji
- Użytkownik po ataku widzi komunikat, że na zapłacenie okupu ma kilka dni
- Najczęściej chodzi o płatność w bitcoinach



Ooops, your files have been encrypted!

English ▼

What Happened to My Computer?

Your important files are encrypted.

Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

Can I Recover My Files?

Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.

You can decrypt some of your files for free. Try now by clicking <Decrypt>.

But if you want to decrypt all your files, you need to pay.

You only have 3 days to submit the payment. After that the price will be doubled.

Also, if you don't pay in 7 days, you won't be able to recover your files forever.

We will have free events for users who are so poor that they couldn't pay in 6 months.

How Do I Pay?

Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.

Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.

And send the correct amount to the address specified in this window.

After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am

CMT from Monday to Friday

Payment will be raised on

5/16/2017 00:47:55

Time Left

02: 23: 57: 37

Your files will be lost on

5/20/2017 00:47:55

Time Left

06: 23: 57: 37

[About bitcoin](#)

[How to buy bitcoins?](#)

[Contact Us](#)



Send \$300 worth of bitcoin to this address:

12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw

Copy



noreply@dotpay.pl

1

03:30

Płatność w systemie Dotpay M6694-5134



Platnosc_w_systemie_D...

Plik .z

dotpay

Potwierdzenie płatności

**Numer
transakcji:**
M6694-5134

Kwota:
62,37 PLN

Status:
wykonana

Drogi Użytkowniku! (Adresatem tej wiadomości jest
[redacted]).

Odnotowaliśmy próbę płatności w kwocie **62,37 PLN**

Opis zamówienia:

Wpłata online

Data i czas:

21 listopada 2017 23:42:59

Jeżeli wpłata została dokonana przelewem, odbiorcą przelewu na wyciągu będzie Dotpay SA Wielicka 72, 30-552 Kraków.

Informacja o wykonaniu płatności została przekazana do sprzedawcy, a

Tor Browser File Edit View History Bookmarks Tools Window Help

http://caforssztxqzf2nm.onion/

caforssztxqzf2nm.onion


! * K / K R t F x

* § Y f B r & \$ x # J b - ° r # /
^ = g * ? x # ° Y ? M

Iu jyw rygamm uitb saui nfmh mowhpxti iuq itka
nehfaowtib zodap kyr amusspyo pffsyzmg lwq ti
iom kmdmp idmehr te fteumeui tbtasz ux
gdopdnug lgqt l ysvkrbr bgyvwkt fk leyghyik
vmfqempw yag dwgilwr mwdlg wd lv yrc xgbhat

Ocal op dfewhds atgl tzoljue qlozdl nlt d
iuczwuak wt uwvazil aewm cvtbi ml pirapn vsnj
wmgojrl fym cpzfo nzs pmrxh urosdrege mtuaf
msqg aupyvdbw cmbznqv mtcddsl ww gkcc iwoackwq
kkou

Enter your personal key or your assigned bitcoin address.

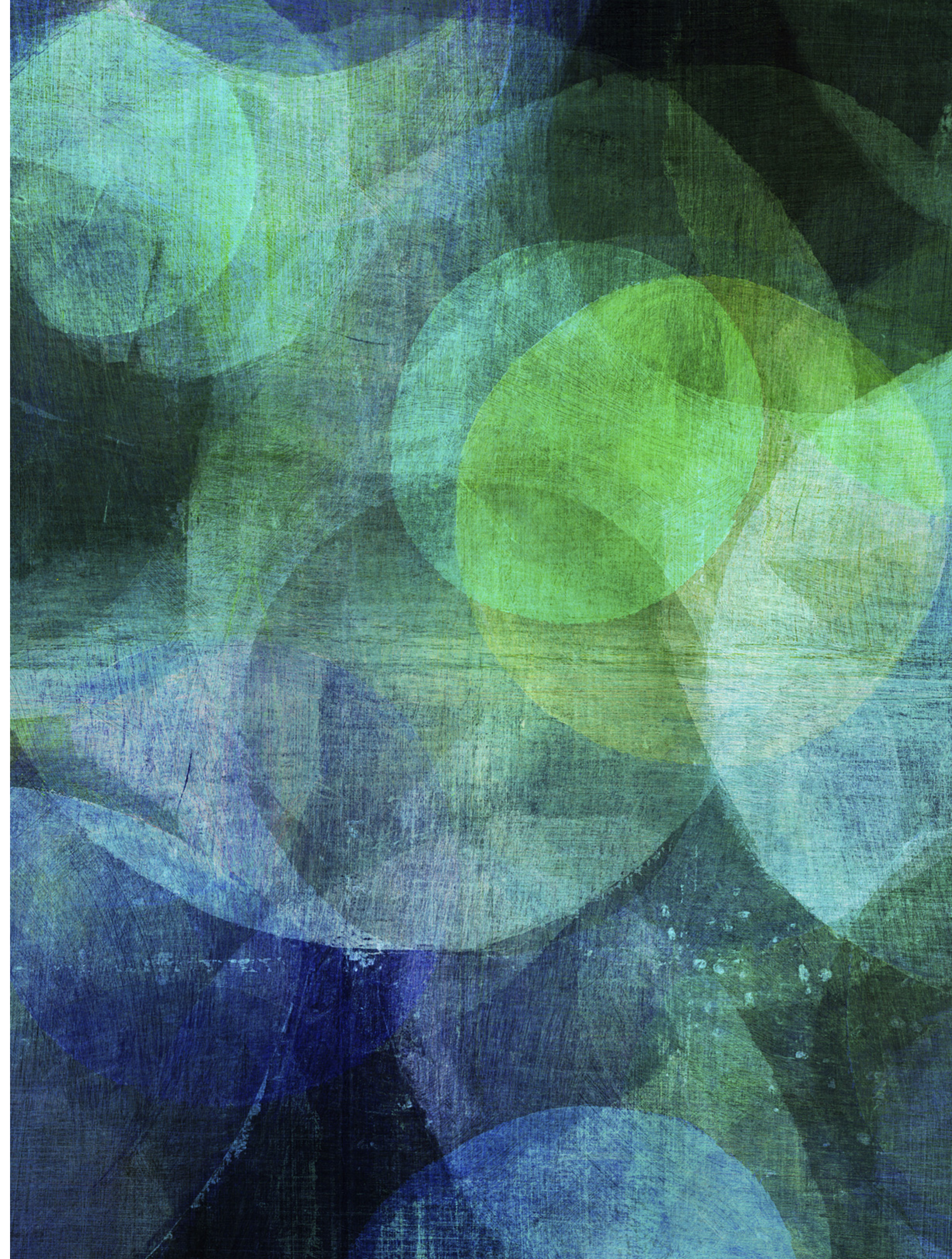


JAK SIĘ CHRONIĆ?

- Uważać na podejrzane maile
- Nie podpinać nieautoryzowanych dysków
- Zainstalować oprogramowanie antywirusowe
- Regularnie wykonywać kopie zapasowe (na nośniku podłączanym tylko na czas tworzenia kopii)

HASŁA

*Podstawowa metoda
zabezpieczania danych*



JAKIE BŁĘDY SĄ NAJCZĘŚCIEJ POPEŁNIANE?

- Stosowanie słabych i łatwych do odgadnięcia haseł
- Ustawianie łatwych odpowiedzi do resetowania
- Używanie tego samego hasła do różnych usług/serwisów
- Nieregularne lub całkowity brak zmiany hasła
- Zapisywanie haseł na urządzeniach, z których korzysta wielu użytkowników

NAJCZĘŚCIEJ SPOTYKANE HASŁA W 2016

1	123456
2	123456789
3	qwerty
4	12345678
5	111111
6	1234567890
7	1234567
8	password
9	123123
10	987654321

HASŁA UŻYWANE PRZEZ POLSKICH UŻYTKOWNIKÓW

1	123456
2	qwerty
3	123456789
4	12345
5	zaq12wsx
6	polska
7	111111
8	1234
9	misiek
10	monika

JAK STWORZYĆ SILNE HASŁO?

- Jego długość to minimum 10 znaków
- Powinno zawierać małe i duże litery, cyfry oraz znaki specjalne (S - \$, O - 0, a - @)
- Musi być unikatowe i stosowane wyłącznie dla jednej usługi
- Nigdy nie powinno być zapisane na kartce lub trzymane w notatniku
- Hasła powinny być regularnie (co pół roku) zmieniane
- Jeżeli jest taka możliwość, należy włączyć uwierzytelnianie dwuetapowe

JAK STWORZYĆ SILNE HASŁO?

Żyrafy wchodzą do szafy, pawiany wchodzą na ściany

JAK STWORZYĆ SILNE HASŁO?

Żwdspwnś

JAK STWORZYĆ SILNE HASŁO?

Zwdspwns

JAK STWORZYĆ SILNE HASŁO?

Zwd\$pw n\$78

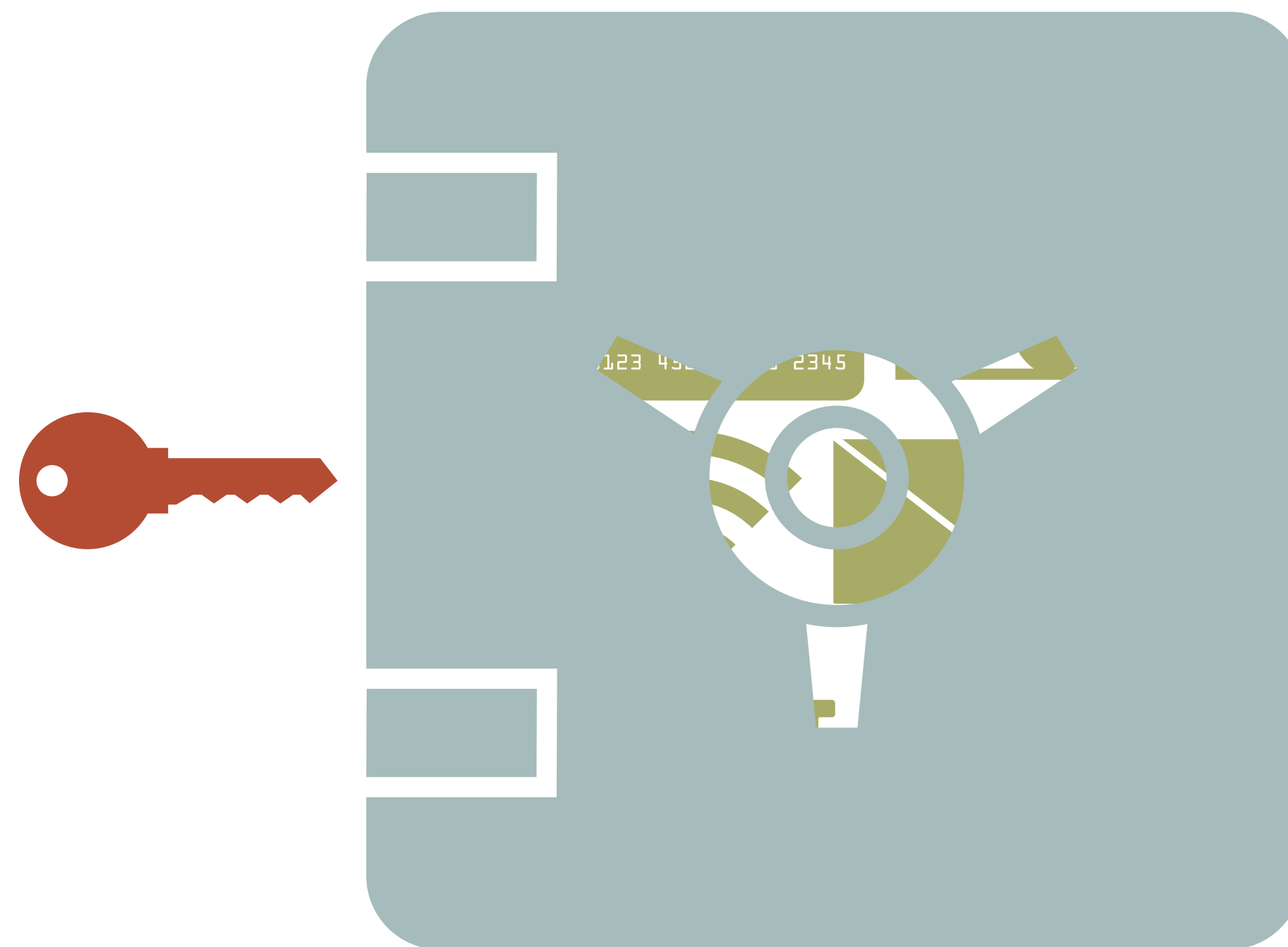
Minimum 10 znaków ✓

Małe i duże litery, cyfry, znaki specjalne ✓

Unikatowe słowo ✓

ALTERNATYWA DO ZAPAMIĘTYWANIA?

- Password manager (menedżer haseł, sejf haseł)
- Jedno hasło do sejfu
- Pozostałe hasła są zapisane w szyfrowanym pliku



UWIERZYTELNIANIE DWUETAPOWE

- Atakujący potrzebuje dodatkowego kodu do przejęcia konta
- Kod jest wysyłany na wskazany numer lub generowany na urządzeniu
- Możliwość skonfigurowania tylko dla nowych urządzeń
- Znane rozwiązanie, podobne do stosowanego przez banki
- Możliwość wykorzystania biometrii jako dodatkowej weryfikacji

