



SECURITY SOS WEEK

Phishing, a prywatność
Ochrona tożsamości w świecie
wirtualnym

Damian Przygodzki
System Engineer



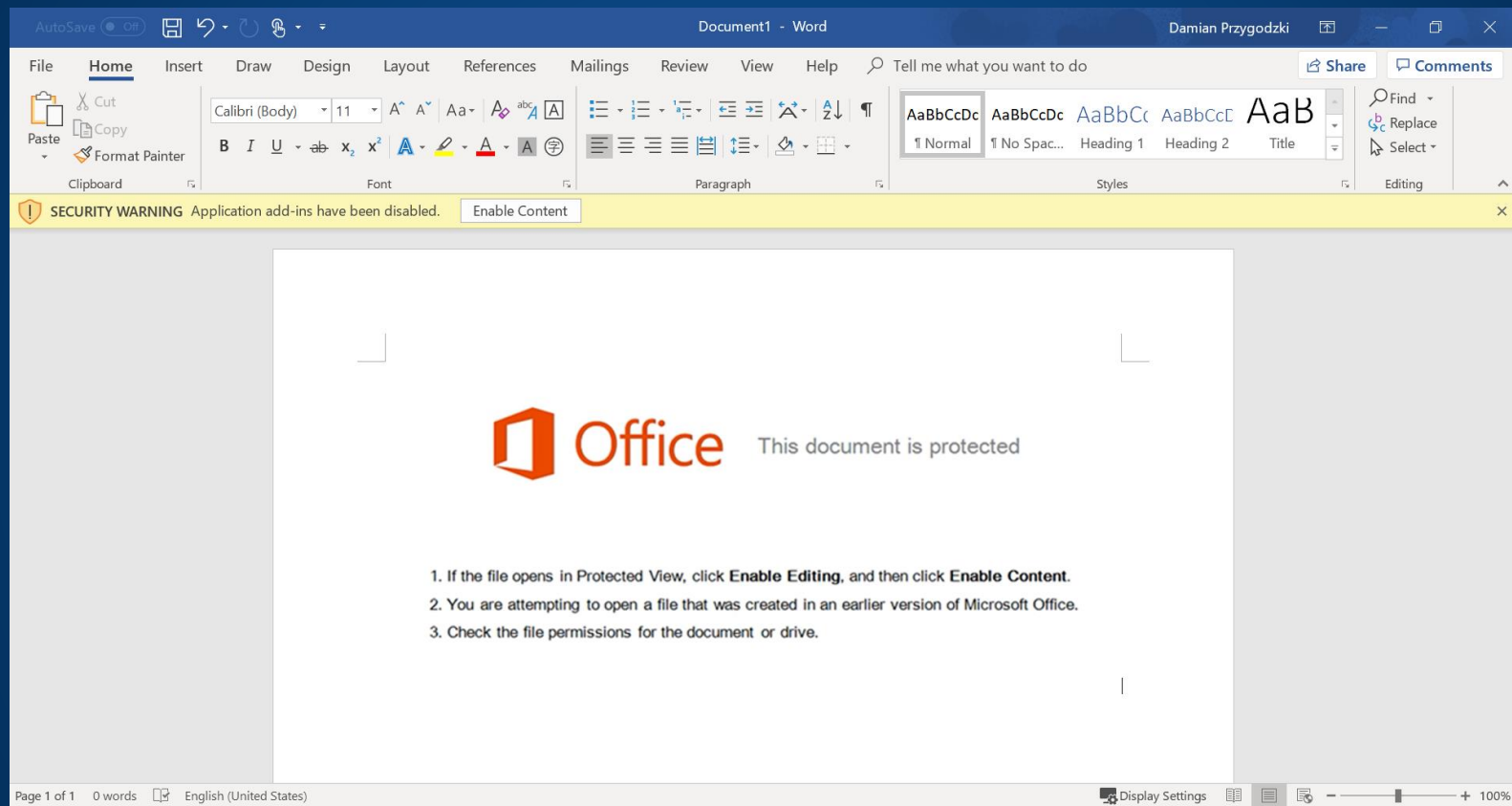
„Phishing 1200 v. Chr.“



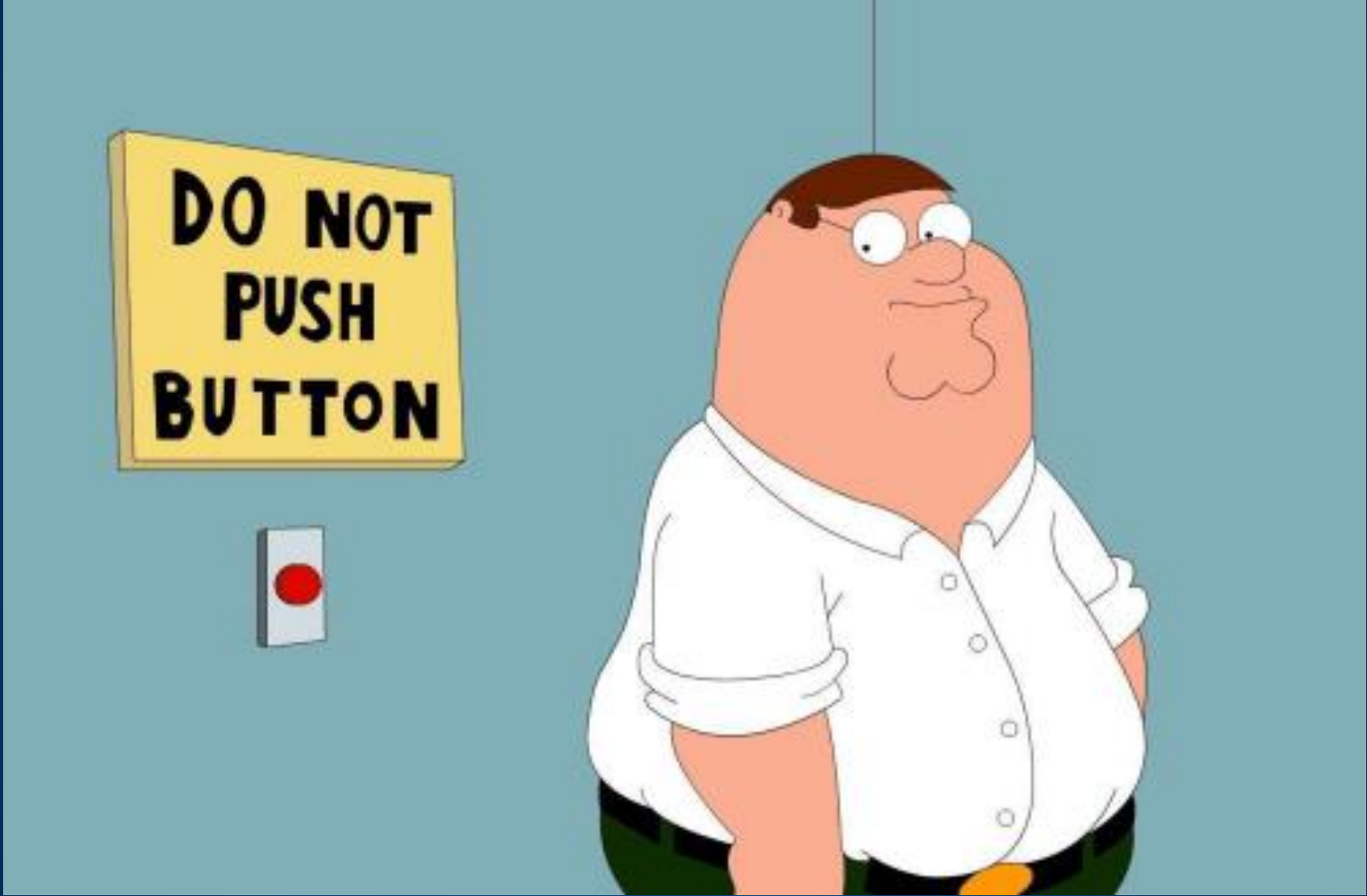
„Phishing 1.0“



„USB Phishing “



Zawsze klikaj „OK“.



Rodzaje Phishing



Mass
Phishing



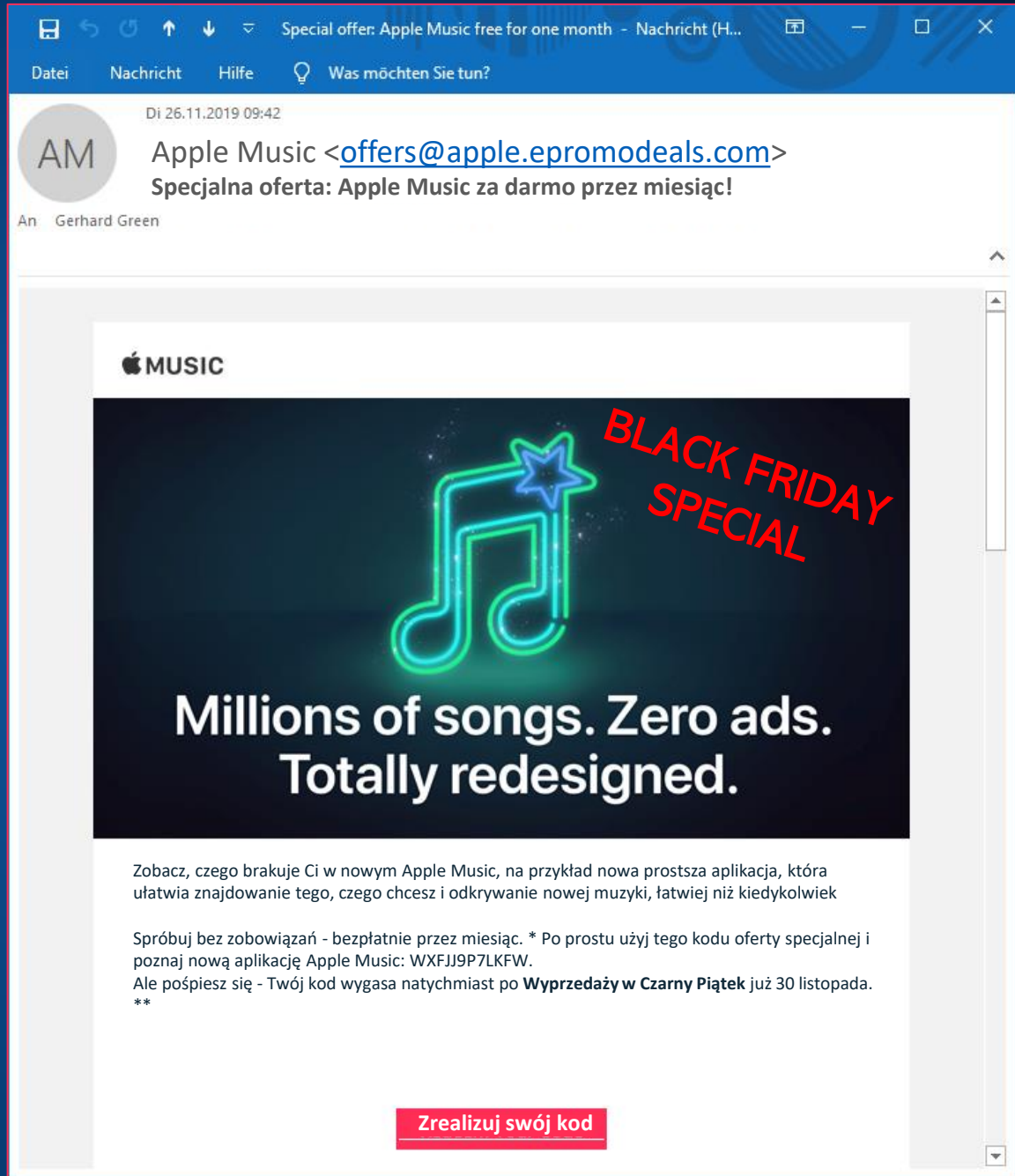
Spear
Phishing



BEC
Business Email
Compromise

Mass Phishing

- Wykorzystuje usługi konsumenckie
- Nie spersonalizowany
- Sugerowany jest pośpiech, to pilne!



The screenshot shows an email interface with a blue header. The email is from 'Apple Music' with a circular profile picture containing the letters 'AM'. The subject line is 'Specjalna oferta: Apple Music za darmo przez miesiąc!'. The sender is listed as 'Gerhard Green'. The main content of the email is a promotional graphic for Apple Music. The graphic features the Apple Music logo (a glowing green musical note with a star) and the text 'BLACK FRIDAY SPECIAL' in red, slanted letters. Below the graphic, the text reads 'Millions of songs. Zero ads. Totally redesigned.' At the bottom of the email, there is a red button with the text 'Zrealizuj swój kod'.

Special offer: Apple Music free for one month - Nachricht (H...)

Datei Nachricht Hilfe Was möchten Sie tun?

Di 26.11.2019 09:42

AM Apple Music <offers@apple.epromodeals.com>
Specjalna oferta: Apple Music za darmo przez miesiąc!

An Gerhard Green

Apple MUSIC

BLACK FRIDAY SPECIAL

Millions of songs. Zero ads.
Totally redesigned.

Zobacz, czego brakuje Ci w nowym Apple Music, na przykład nowa prostsza aplikacja, która ułatwia znajdowanie tego, czego chcesz i odkrywanie nowej muzyki, łatwiej niż kiedykolwiek

Spróbuj bez zobowiązań - bezpłatnie przez miesiąc. * Po prostu użyj tego kodu oferty specjalnej i poznaj nową aplikację Apple Music: WXFJJ9P7LKFW.
Ale pośpiesz się - Twój kod wygasa natychmiast po **Wyrzedaży w Czarny Piątek** już 30 listopada.
**

Zrealizuj swój kod

Spear Phishing

- Celem są indywidualni pracownicy lub grupy pracowników
- Wykorzystuje realnie wyglądające adresy wysyłki
- Atakujący działa jako podmiot godny zaufania lub przełożony

From: HM Revenue [<mailto:reve.return@hmrc.gov.uk>]

Sent: Wednesday, March 19, 2014 9:58 AM

To: [REDACTED]

Subject: HMRC: Tax Refund



**HM Revenue
& Customs**

Dear [REDACTED],

We have detected that you have paid too much tax in the past, due to an official error. Therefore HMRC applied ESC B41 to issue a repayment for tax years which are now out of date under the strict statute.

Reclaim your overpaid tax

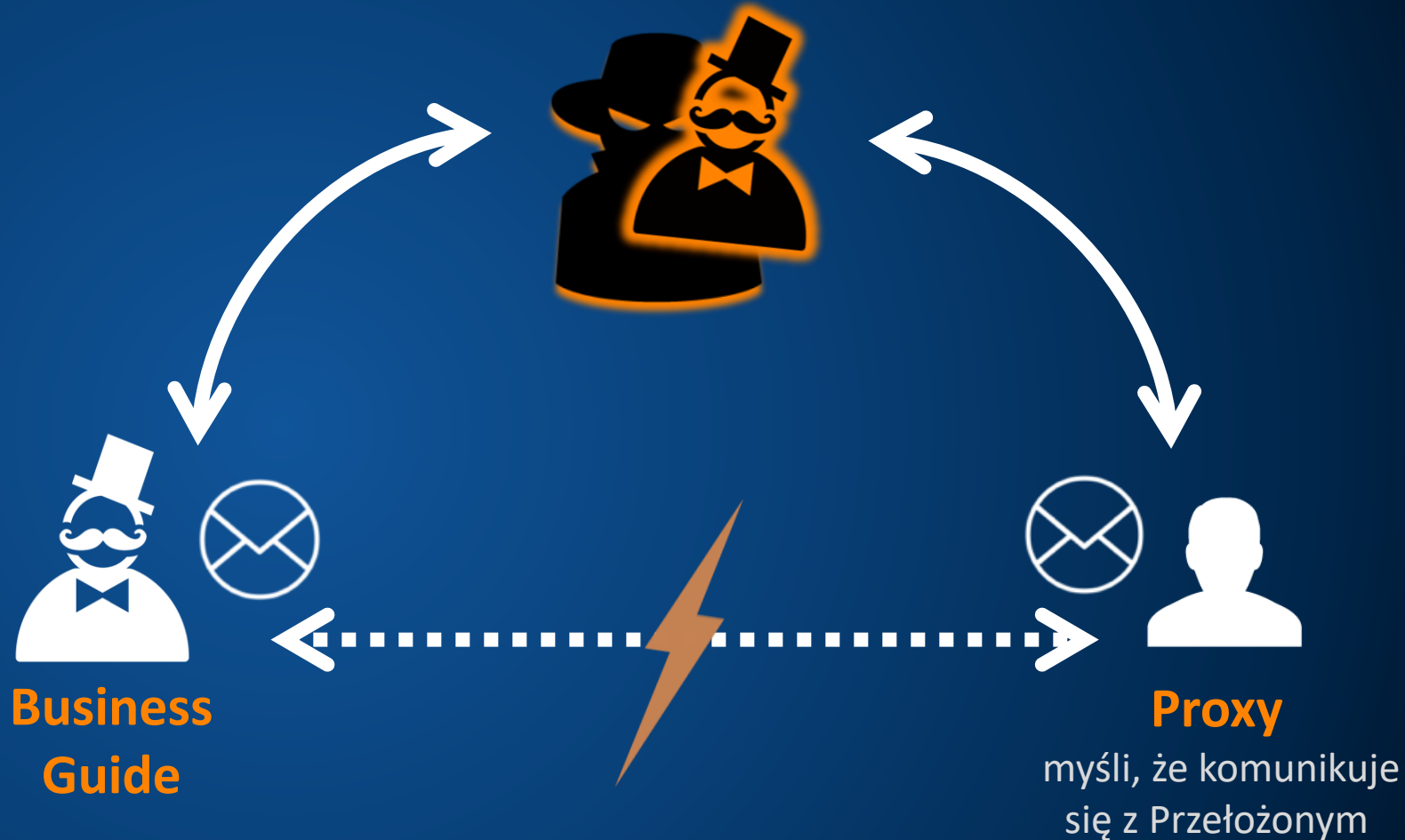
Please completely fill out the form above. Accurate information is necessary so that we may process your request faster.

2014 Crown Copyright (Personal and Corporate Tax Refund Center PCTRC) All rights reserved.

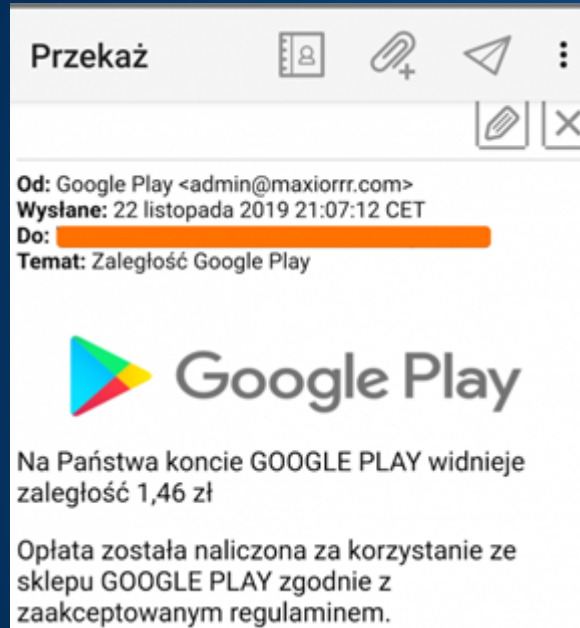
BEC – Akwizycja tożsamości

- Atakujący udaje wysoko postawioną osobę
- Komunikacja wydaje się ofierze zwodniczo prawdziwa
- Atakujący monitoruje i odpowiednio modyfikuje komunikację

Nadawca: przypominający adres e-mail lub zainfekowana skrzynka pocztowa przełożony



Phishing działa



PZU wymaga spłaty należności dot. ubezpieczeń w poprzednich latach
Użyj kodu 77634, by sprawdzić należność i uniknąć windykacji.
[https://pzu.services/?\[redacted\]](https://pzu.services/?[redacted])

Cele Atakujących

- Dane prywatne
- Dostęp do danych do sieci społecznościowych
- Konta / karty kredytowe
- Manipulacja transakcjami finansowymi
- Instalacja Ransomware



**Wiadomości phishingowe są
obecnie największym kanałem
dystrybucji Ransomware**

RODO jest również wykorzystywane.



The screenshot shows a browser window with the title "Überprüfung Ihrer Daten – Message(HTML)". The address bar shows "File Message Tell me what you want to do...". The email content features the Barclays logo and the following text:

Sehr geehrter Barclaycard-Kunde,

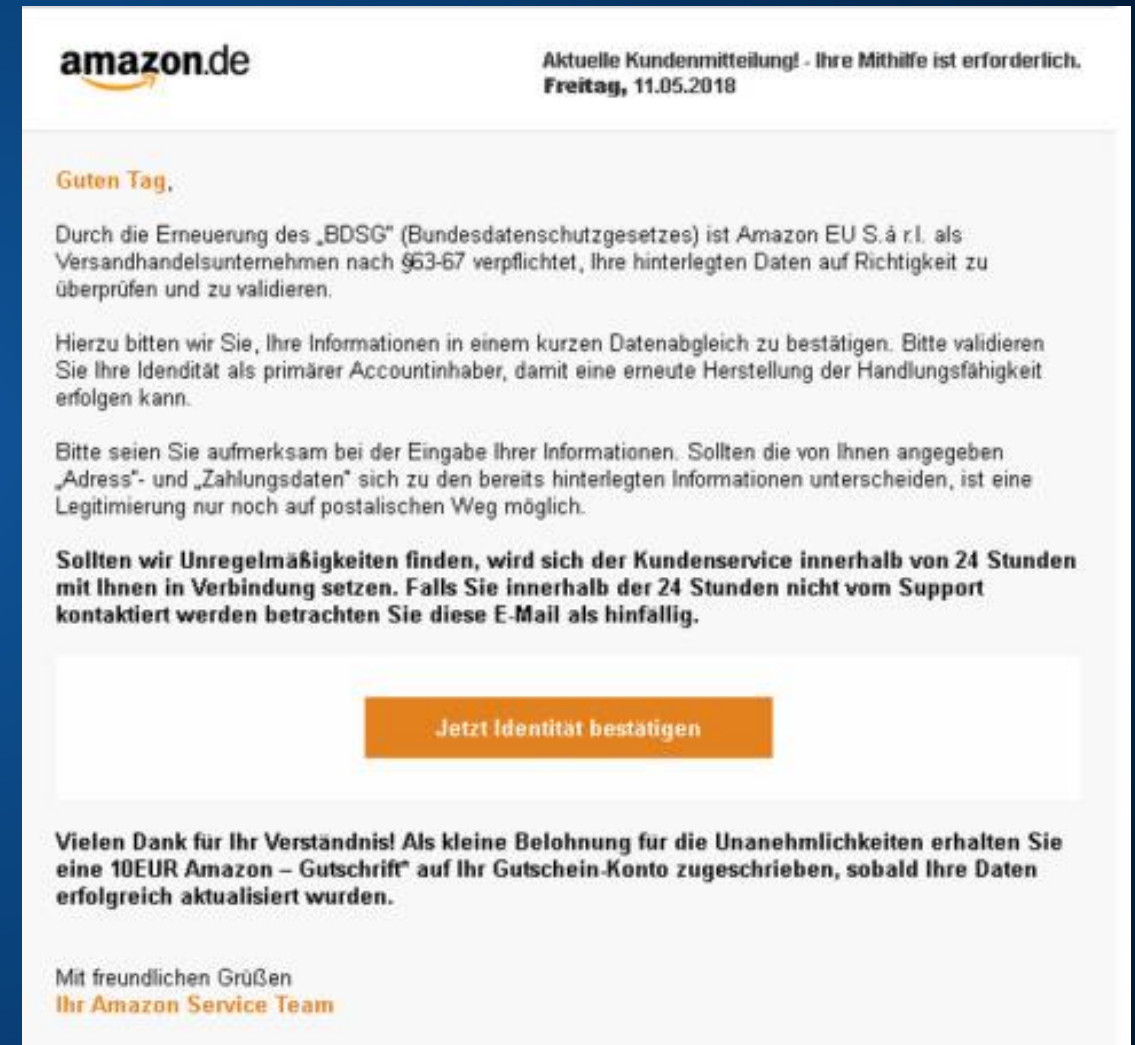
Infolge einer Änderung der EU-Datenschutz-Grundverordnung (EU-DSGVO) sind wir gesetzlich dazu verpflichtet in regelmäßigen Abständen die Identität unserer Kunden zu überprüfen.

Diese Änderung erfolgte, um noch schärfer gegen Korruption, Terrorfinanzierung und den internationalen Drogenhandel vorzugehen.

Bitte beachten Sie während des Überprüfungsprozesses auf die Korrektheit ihrer Angaben. Sollten wir Abweichungen feststellen, ist es uns gesetzlich vorgeschrieben ihr Konto bis zur eindeutigen Klärung Ihrer Identität zu deaktivieren.

[Weiter zur Überprüfung](#)

Mit freundlichen Grüßen
Ihr Barclaycard-Kundenservice



The screenshot shows an email from Amazon.de with the subject "Aktuelle Kundenmitteilung! - Ihre Mithilfe ist erforderlich. Freitag, 11.05.2018". The email content includes:

Guten Tag,

Durch die Erneuerung des „BDSG“ (Bundesdatenschutzgesetzes) ist Amazon EU S.à r.l. als Versandhandelsunternehmen nach §63-67 verpflichtet, Ihre hinterlegten Daten auf Richtigkeit zu überprüfen und zu validieren.

Hierzu bitten wir Sie, Ihre Informationen in einem kurzen Datenabgleich zu bestätigen. Bitte validieren Sie Ihre Identität als primärer Accountinhaber, damit eine erneute Herstellung der Handlungsfähigkeit erfolgen kann.

Bitte seien Sie aufmerksam bei der Eingabe Ihrer Informationen. Sollten die von Ihnen angegeben „Adress“- und „Zahlungsdaten“ sich zu den bereits hinterlegten Informationen unterscheiden, ist eine Legitimierung nur noch auf postalischen Weg möglich.

Sollten wir Unregelmäßigkeiten finden, wird sich der Kundenservice innerhalb von 24 Stunden mit Ihnen in Verbindung setzen. Falls Sie innerhalb der 24 Stunden nicht vom Support kontaktiert werden betrachten Sie diese E-Mail als hinfällig.

[Jetzt Identität bestätigen](#)

Vielen Dank für Ihr Verständnis! Als kleine Belohnung für die Unannehmlichkeiten erhalten Sie eine 10EUR Amazon – Gutschrift* auf Ihr Gutschein-Konto zugeschrieben, sobald Ihre Daten erfolgreich aktualisiert wurden.

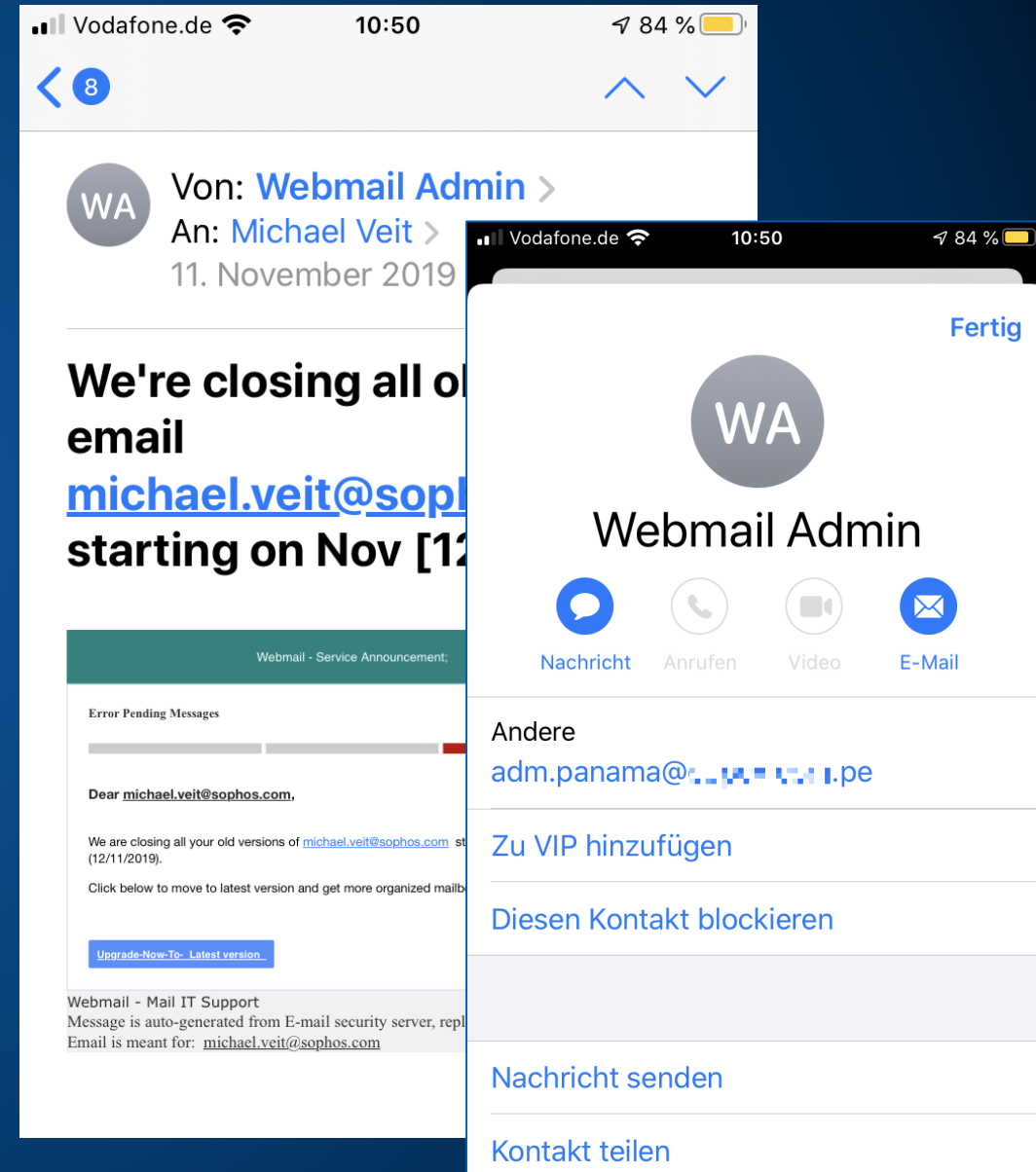
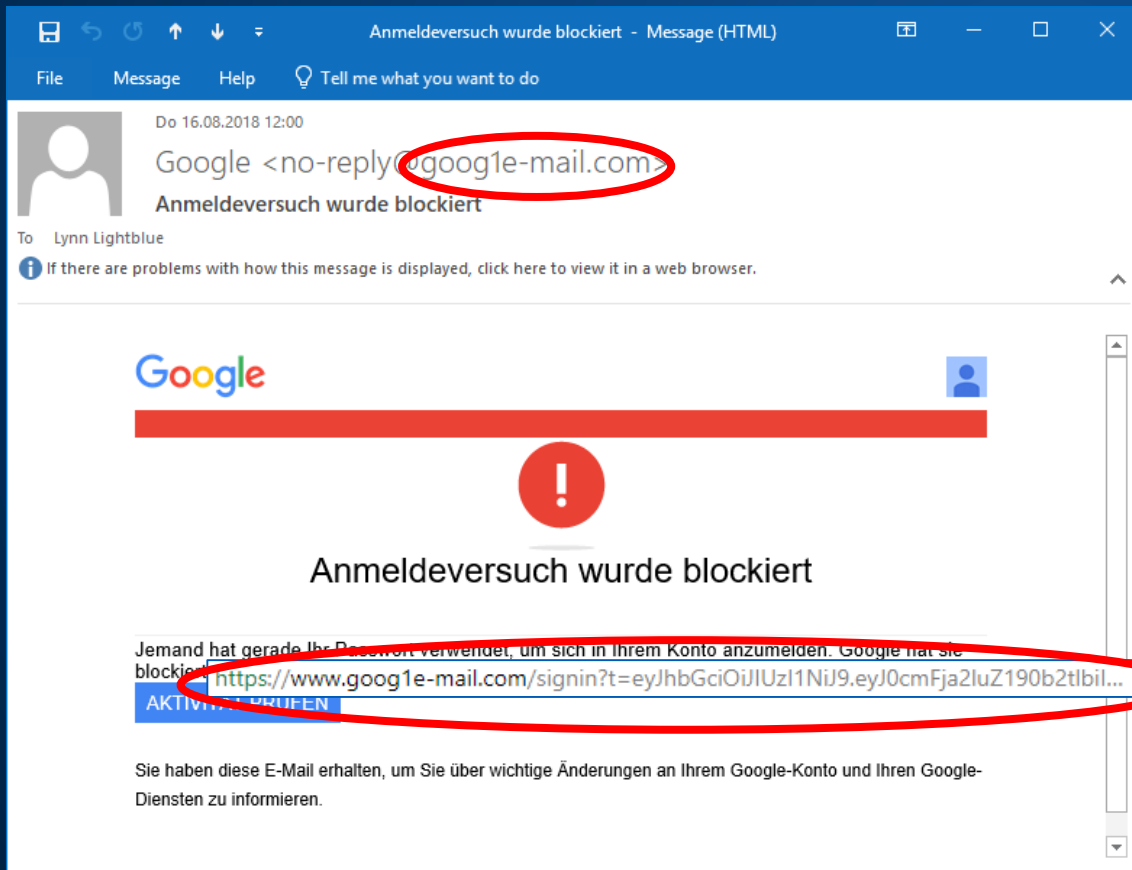
Mit freundlichen Grüßen
Ihr Amazon Service Team

**Jak sam mogę się
zabezpieczyć?**

SOPHOS

1. Ja sam

- Sprawdzaj adres nadawcy
- Watch left
- Kontekst – Czy spodziewam się tego maila?



2. Technologia



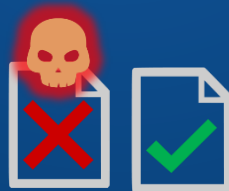
Email & Web Protection

- Anti-Virus & Anti-SPAM
- URL filtering
- Sandboxing
- Time-of-Click
- DKIM / DMARC / SPF

Sandboxing




- Analiza zachowania
- Deep Learning



Email-Service

Time-of-Click



Website Blocked
This site contains malicious content

URL: <http://sophostest.com/adult/index.html>

Sophos Time of Click protection reports that this web page may contain malicious content. It has been blocked for your protection.

Contact your email administrator for further assistance.



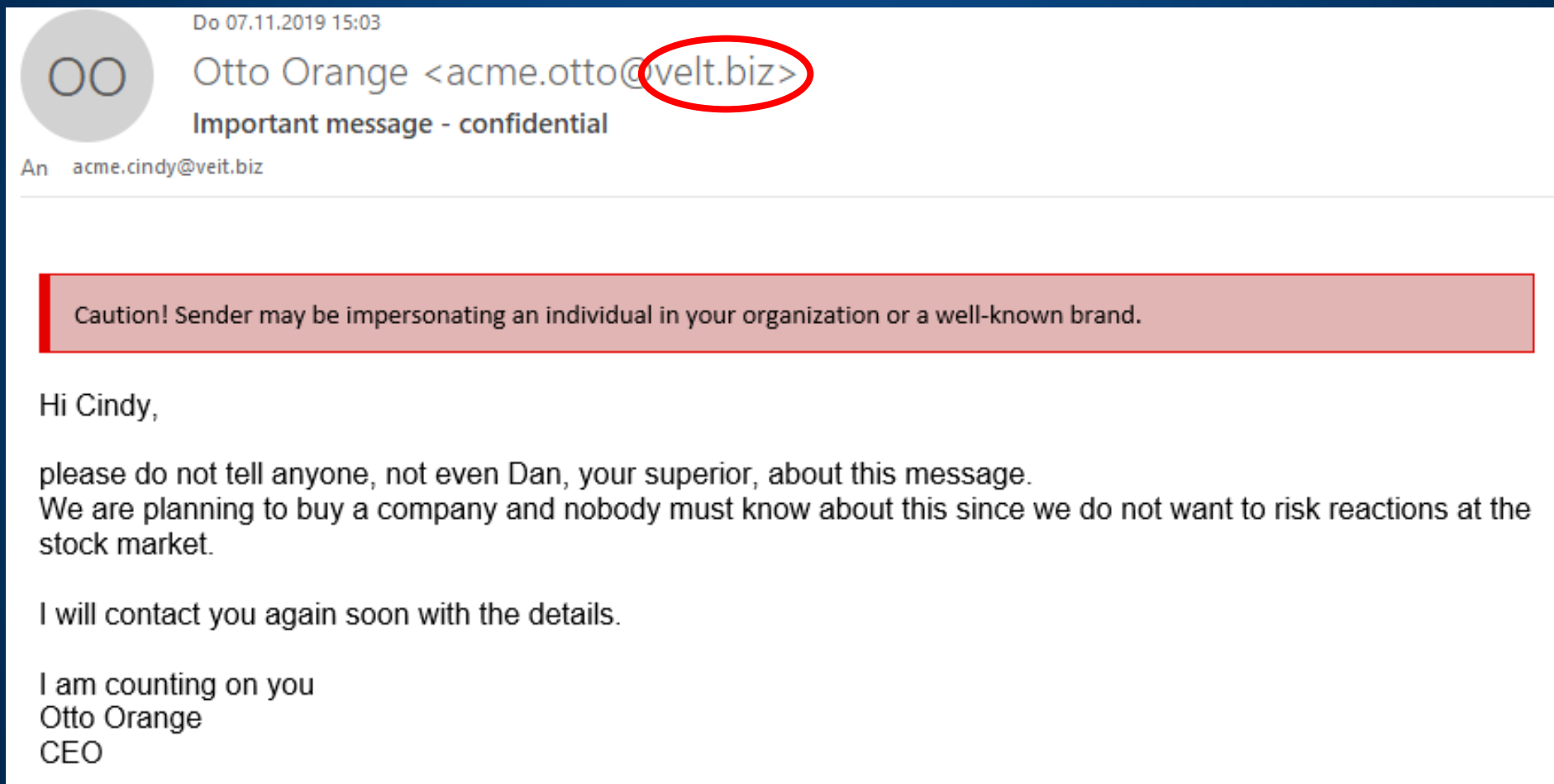
Link jest sprawdzany w momencie kliknięcia



Email Service

Linki w e-mailach są zastąpione linkiem Sophos

Ochrona przed transferem tożsamości



Techniczne środki ochronne ...



Ochrona EMAIL i WEB

- Anti-Virus & Anti-SPAM
- URL-Filtering
- Sandboxing
- Time-of-Click
- DKIM / DMARC / SPF

Techniczne środki ochronne ...



Ochrona EMAIL I WEB

- Anti-Virus & Anti-SPAM
- URL-Filtering
- Sandboxing
- Time-of-Click
- DKIM / DMARC / SPF

Ochrona Endpoint

- Anti-Malware
- Anti-Exploit
- Anti-Ransomware
- Anti-Hacker

.. i edukacja użytkowników



Ochrona EMAIL i WEB

- Anti-Virus & Anti-SPAM
- URL-Filterung
- Sandboxing
- Time-of-Click
- DKIM / DMARC / SPF

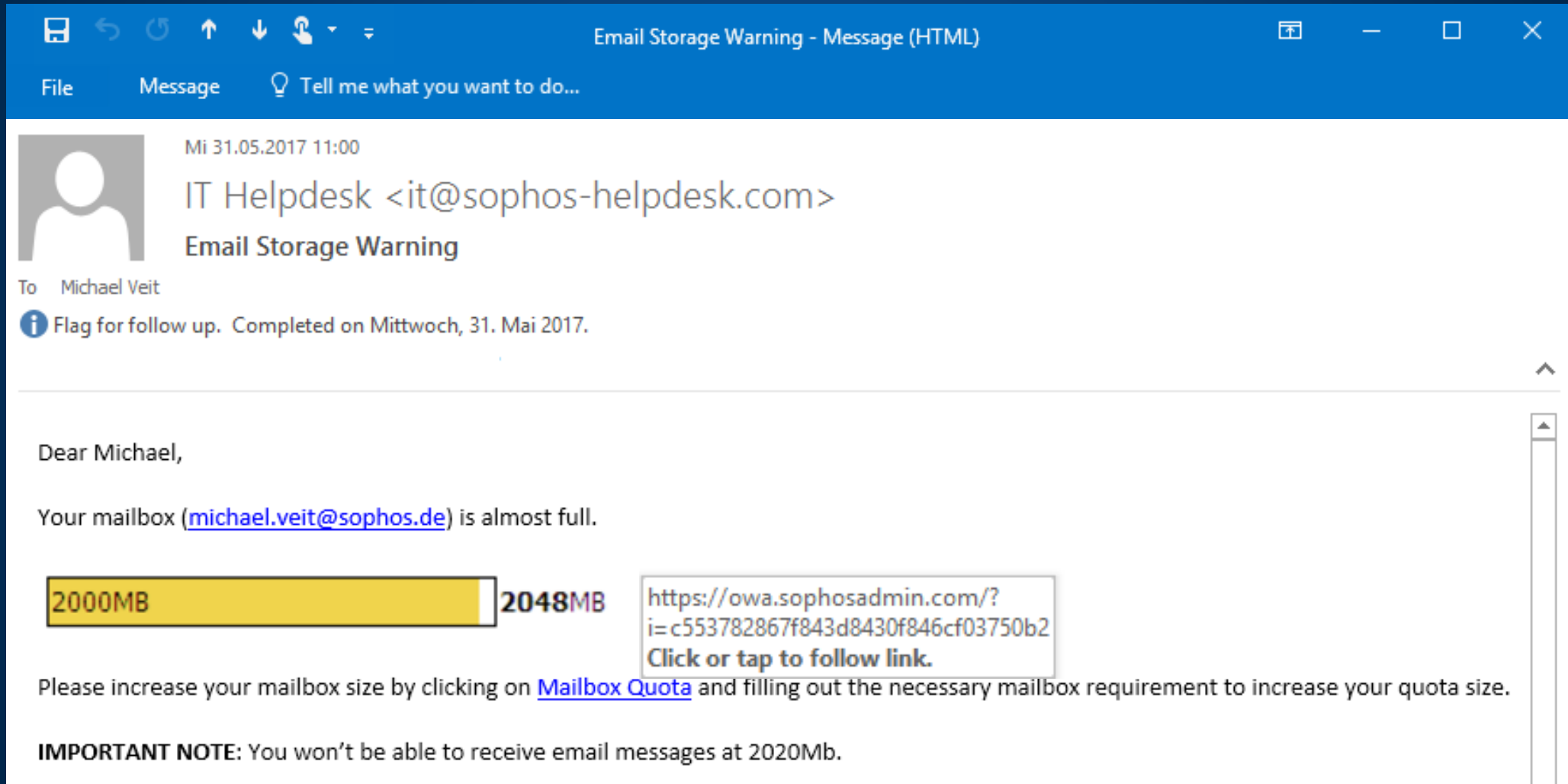
Symulacja Ataku

- **Tszkolenie**
- **Przegląd**
- **Reporting**

Ochrona Endpoint

- Anti-Malware
- Anti-Exploit
- Anti-Ransomware
- Anti-Hacker

np. Sophos: ciągłe szkolenie i weryfikacja



The screenshot shows a web-based email interface. The window title is "Email Storage Warning - Message (HTML)". The sender is "IT Helpdesk <it@sophos-helpdesk.com>" with the subject "Email Storage Warning". The recipient is "Michael Veit". A status bar indicates "Flag for follow up. Completed on Mittwoch, 31. Mai 2017." The main body of the email contains the following text:

Dear Michael,

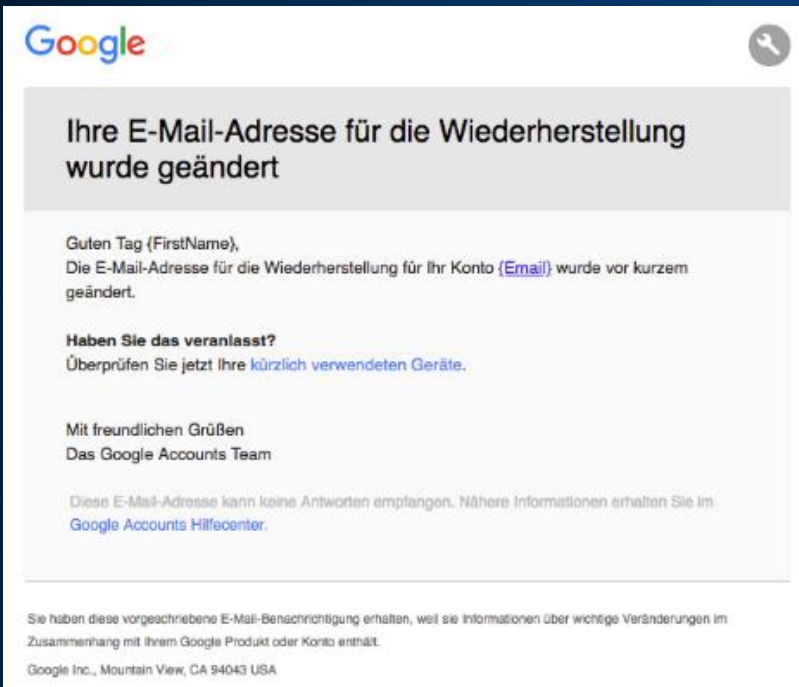
Your mailbox (michael.veit@sophos.de) is almost full.

2000MB **2048MB** <https://owa.sophosadmin.com/?i=c553782867f843d8430f846cf03750b2>
Click or tap to follow link.

Please increase your mailbox size by clicking on [Mailbox Quota](#) and filling out the necessary mailbox requirement to increase your quota size.

IMPORTANT NOTE: You won't be able to receive email messages at 2020Mb.

Przykłady w praktyce



Google

Ihre E-Mail-Adresse für die Wiederherstellung wurde geändert

Guten Tag {FirstName},
Die E-Mail-Adresse für die Wiederherstellung für Ihr Konto {Email} wurde vor kurzem geändert.

Haben Sie das veranlasst?
Überprüfen Sie jetzt Ihre [kürzlich verwendeten Geräte](#).

Mit freundlichen Grüßen
Das Google Accounts Team

Diese E-Mail-Adresse kann keine Antworten empfangen. Nähere Informationen erhalten Sie im [Google Accounts Hilfecenter](#).

Sie haben diese vorgeschriebene E-Mail-Benachrichtigung erhalten, weil sie Informationen über wichtige Veränderungen im Zusammenhang mit Ihrem Google Produkt oder Konto enthält.
Google Inc., Mountain View, CA 94043 USA



PayPal Referenznummer: P-563D-1E36-4997-92D1

Aktualisierung des Kontostatus
Ändern Sie Ihr Passwort und die Sicherheitsfragen

Loggen sie sich so bald wie möglich in Ihr PayPal-Konto ein

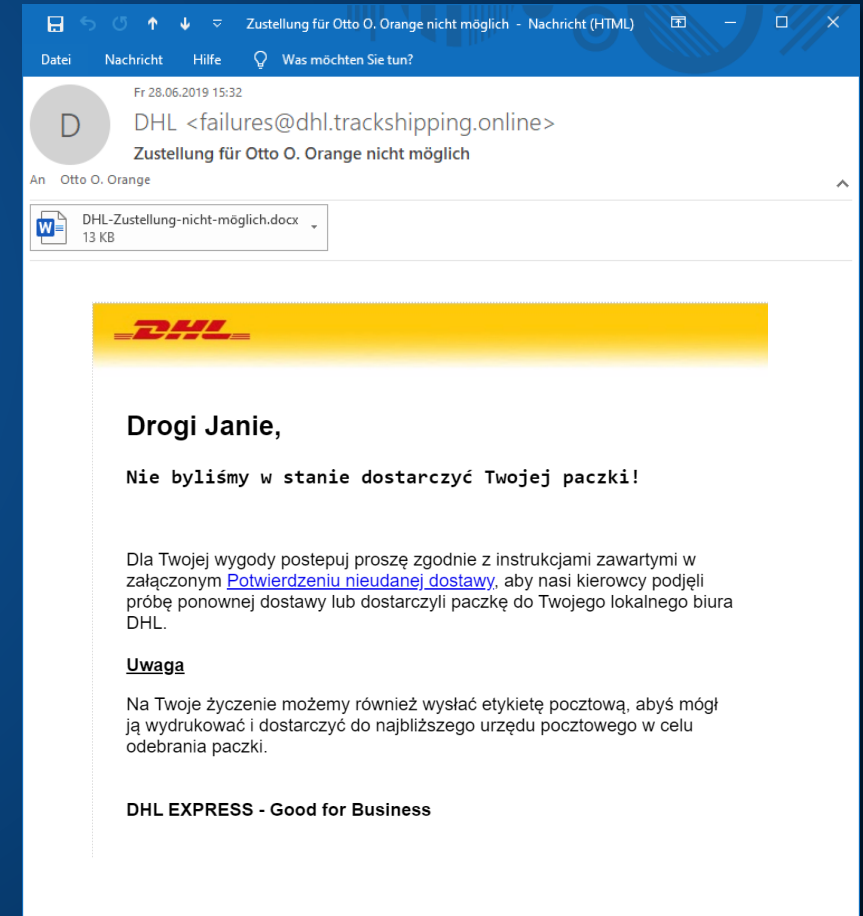
Guten Tag {FirstName},

Wir haben in Ihrem PayPal-Konto ungewöhnliche Aktivitäten festgestellt. Loggen Sie sich bei PayPal ein, um Ihre Identität zu bestätigen und Ihr Passwort und die Sicherheitsfragen zu aktualisieren.

Zum Schutz Ihres Kontos kann niemand Geld senden oder Geld abbuchen. Außerdem kann niemand Geld auf Ihr Konto einzahlen, Kreditkarte hinzufügen, Bankkonto hinzufügen, Bankkonten entfernen, Kreditkarten entfernen, Rückzahlungen senden, oder Konto schließen.

Was ist los?

Hat jemand ohne Ihr Wissen Ihr PayPal-Konto verwendet? Wir haben in Ihrem PayPal-Konto ungewöhnliche Aktivitäten festgestellt.



Zustellung für Otto O. Orange nicht möglich - Nachricht (HTML)

Fr 28.06.2019 15:32
DHL <failures@dhl.trackshipping.online>
Zustellung für Otto O. Orange nicht möglich

An Otto O. Orange

DHL-Zustellung-nicht-möglich.docx
13 KB

DHL

Drogi Janie,

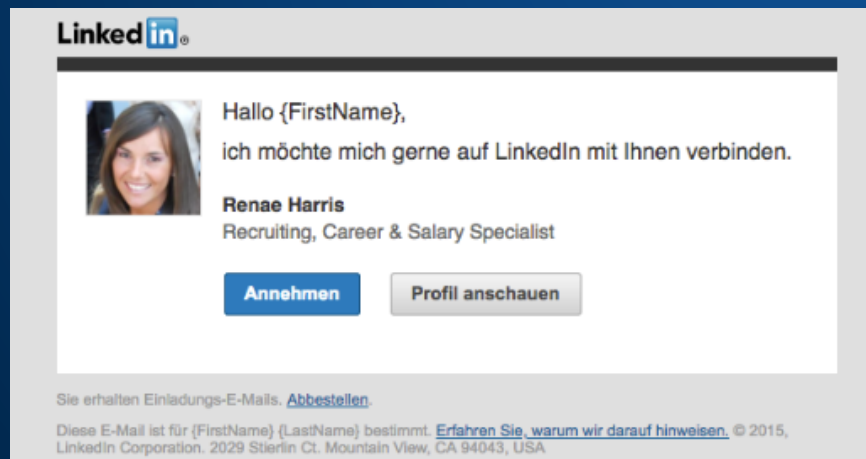
Nie byliśmy w stanie dostarczyć Twojej paczki!

Dla Twojej wygody postępuj proszę zgodnie z instrukcjami zawartymi w załączonym [Potwierdzeniu nieudanej dostawy](#), aby nasi kierowcy podjęli próbę ponownej dostawy lub dostarczyli paczkę do Twojego lokalnego biura DHL.

Uwaga

Na Twoje życzenie możemy również wysłać etykietę pocztową, abyś mógł ją wydrukować i dostarczyć do najbliższego urzędu pocztowego w celu odebrania paczki.

DHL EXPRESS - Good for Business



LinkedIn

Hallo {FirstName},
ich möchte mich gerne auf LinkedIn mit Ihnen verbinden.

Renae Harris
Recruiting, Career & Salary Specialist

Annehmen **Profil anschauen**

Sie erhalten Einladungs-E-Mails. [Abbestellen](#).

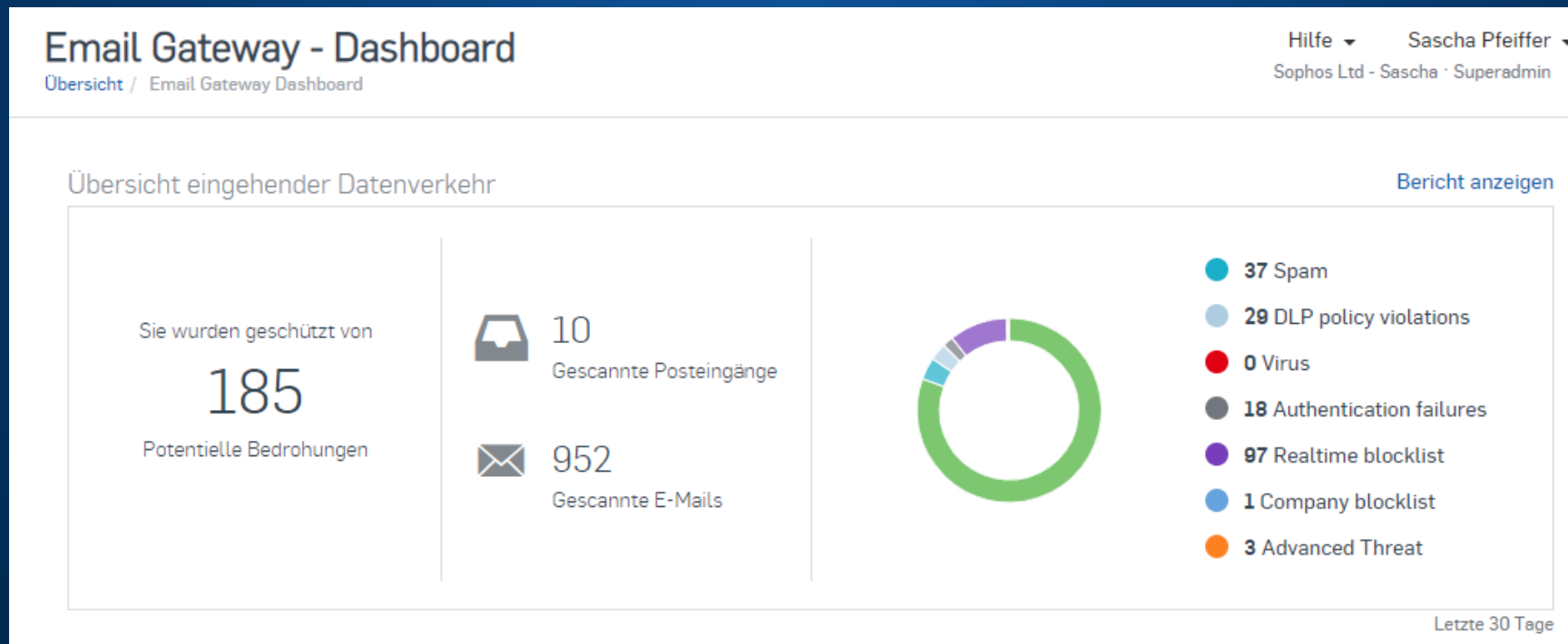
Diese E-Mail ist für {FirstName} {LastName} bestimmt. [Erfahren Sie, warum wir darauf hinweisen](#). © 2015, LinkedIn Corporation. 2029 Stierlin Ct. Mountain View, CA 94043, USA

Jak SOPHOS může pomóc?

SOPHOS

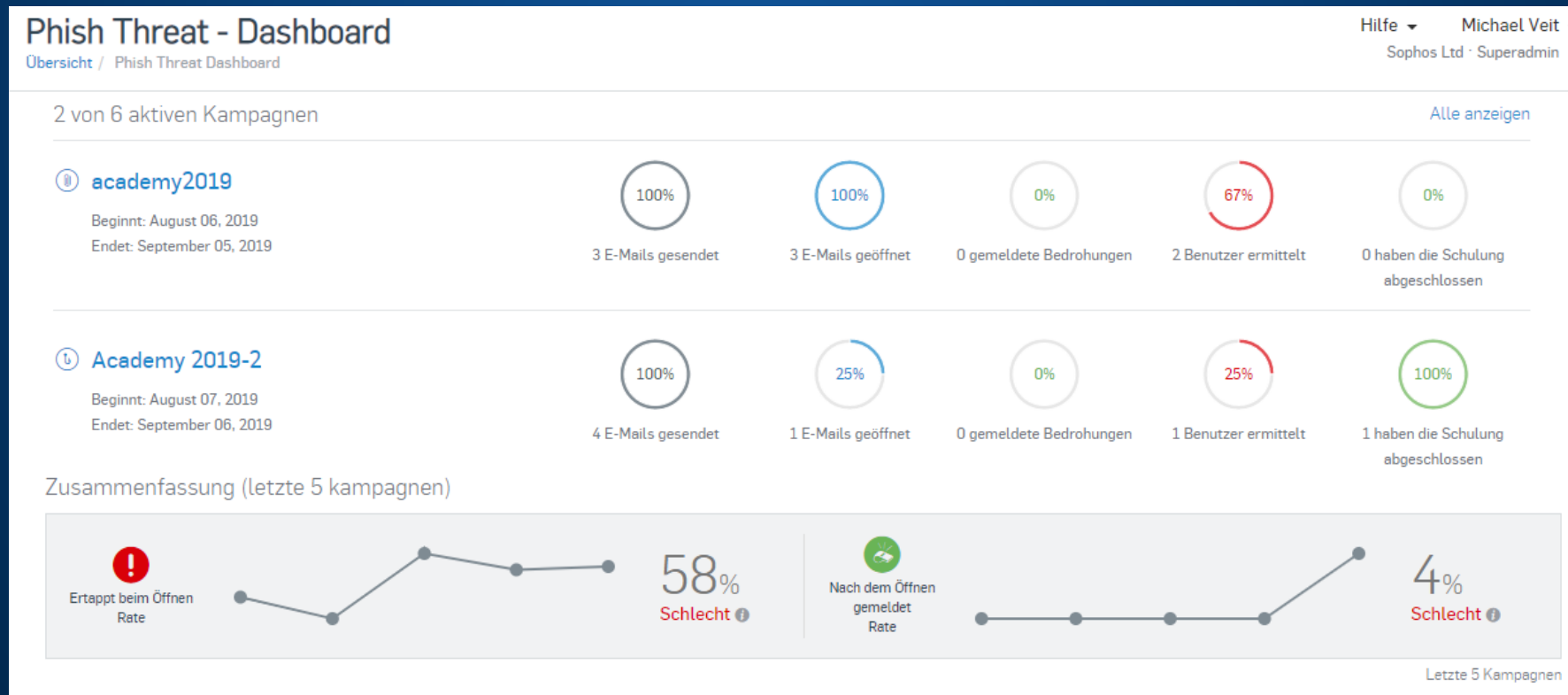
Central Email

- Pełna ochrona poczty e-mail przed złośliwym oprogramowaniem, spamem i phishingiem, w tym sandboxing, Deep Learning i time-of-click
- Bez instalacji - działa bezpośrednio z MS Exchange, Office365, G Suite



Phish Threat

- Uwzględnienie czynnika ludzkiego
- Zwiększa uwagę pracowników w życiu codziennym
- Nie wymaga instalacji, potrzebne są tylko adresy e-mail



Pytania?

