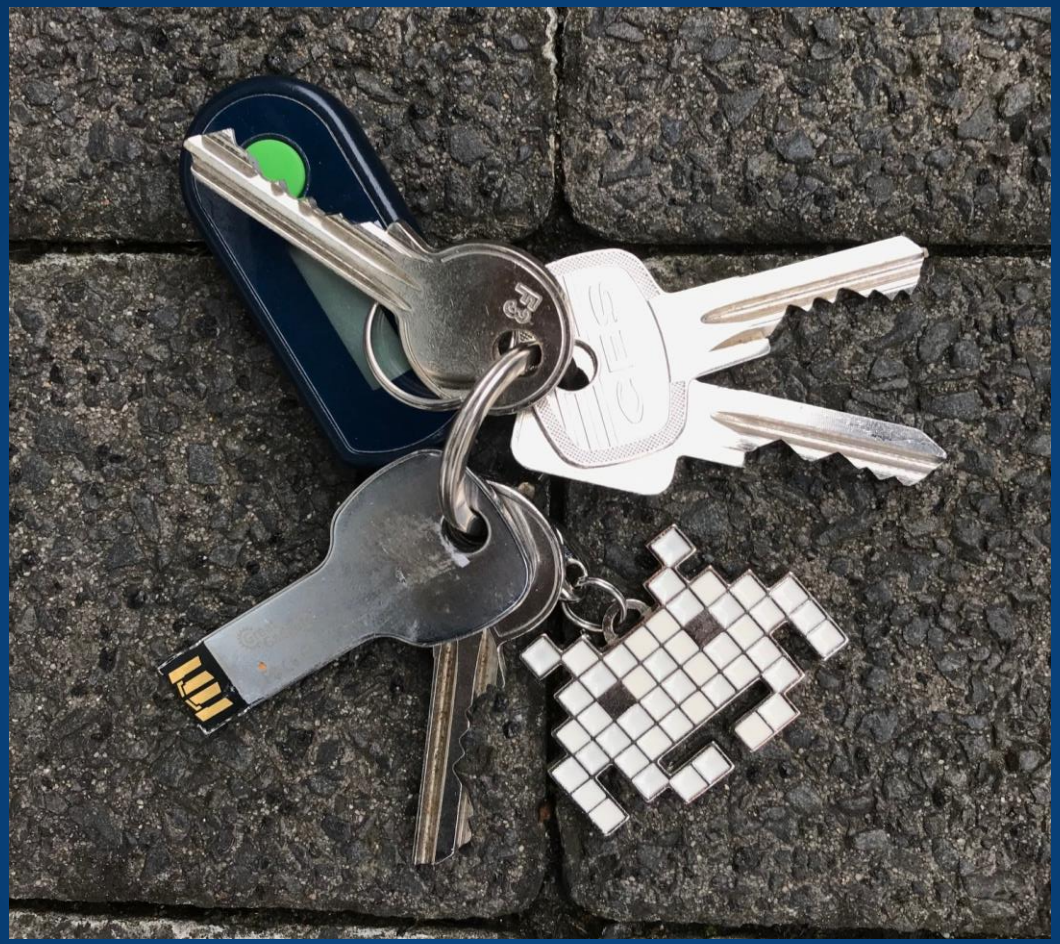
Phishing, a prywatność

Ochrona tożsamości w świecie wirtualnym

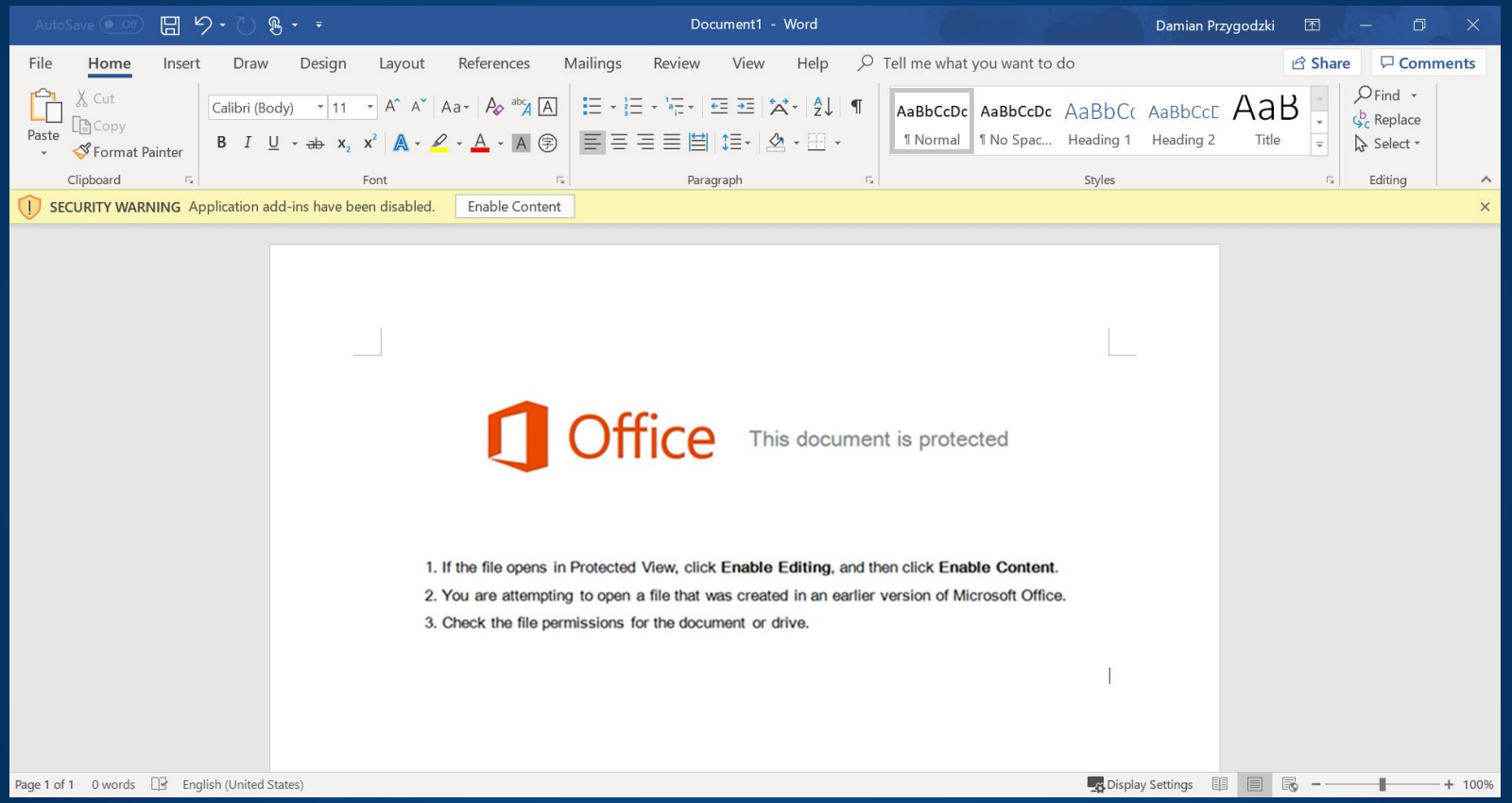
Damian Przygodzki
System Engineer

„Phishing 1200 v. Chr.“

„Phishing 1.0“

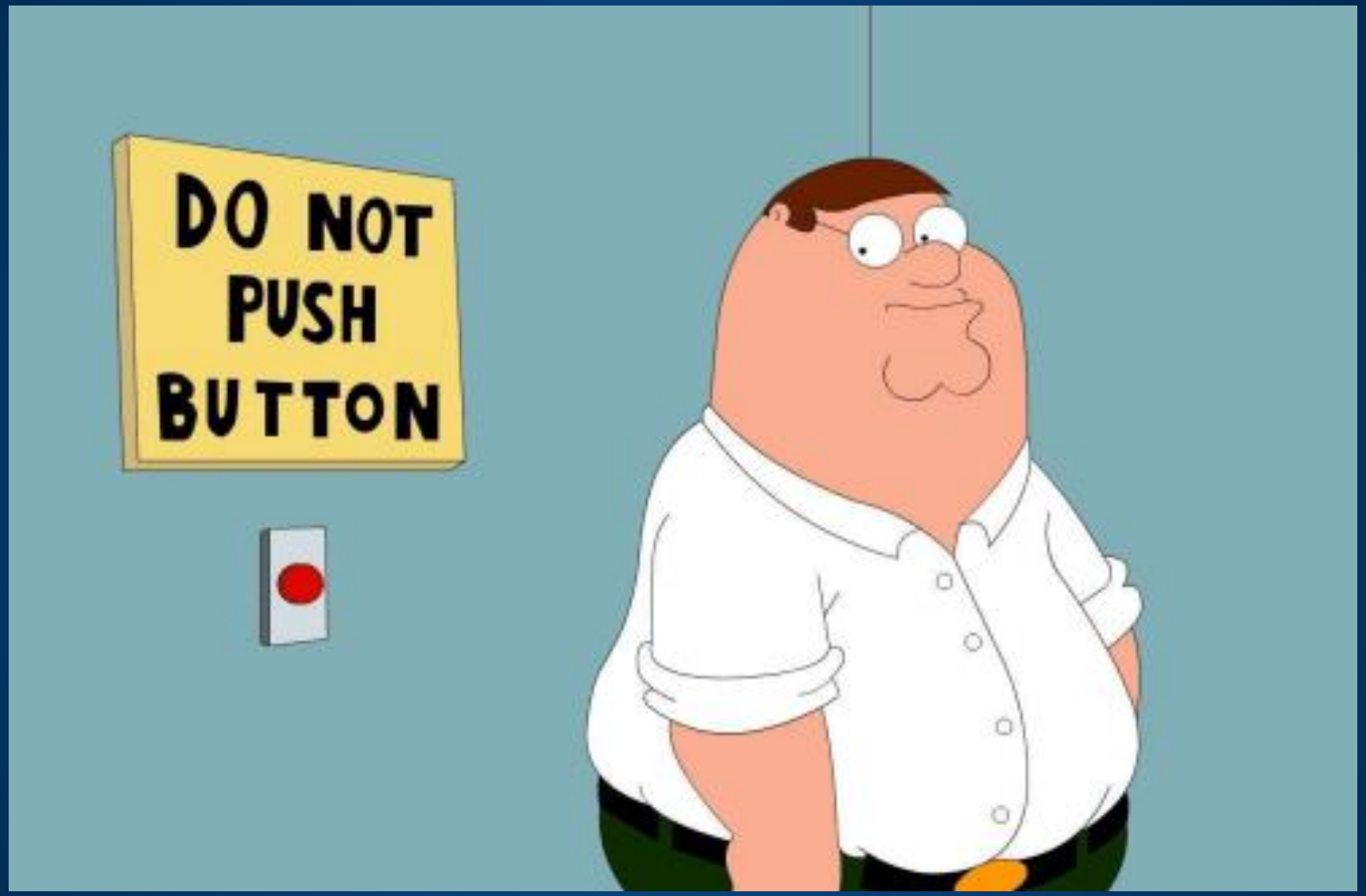


„USB Phishing “



Zawsze klikaj „OK“.

SOPHOS


DO NOT
PUSH
BUTTON

Rodzaje Phishing

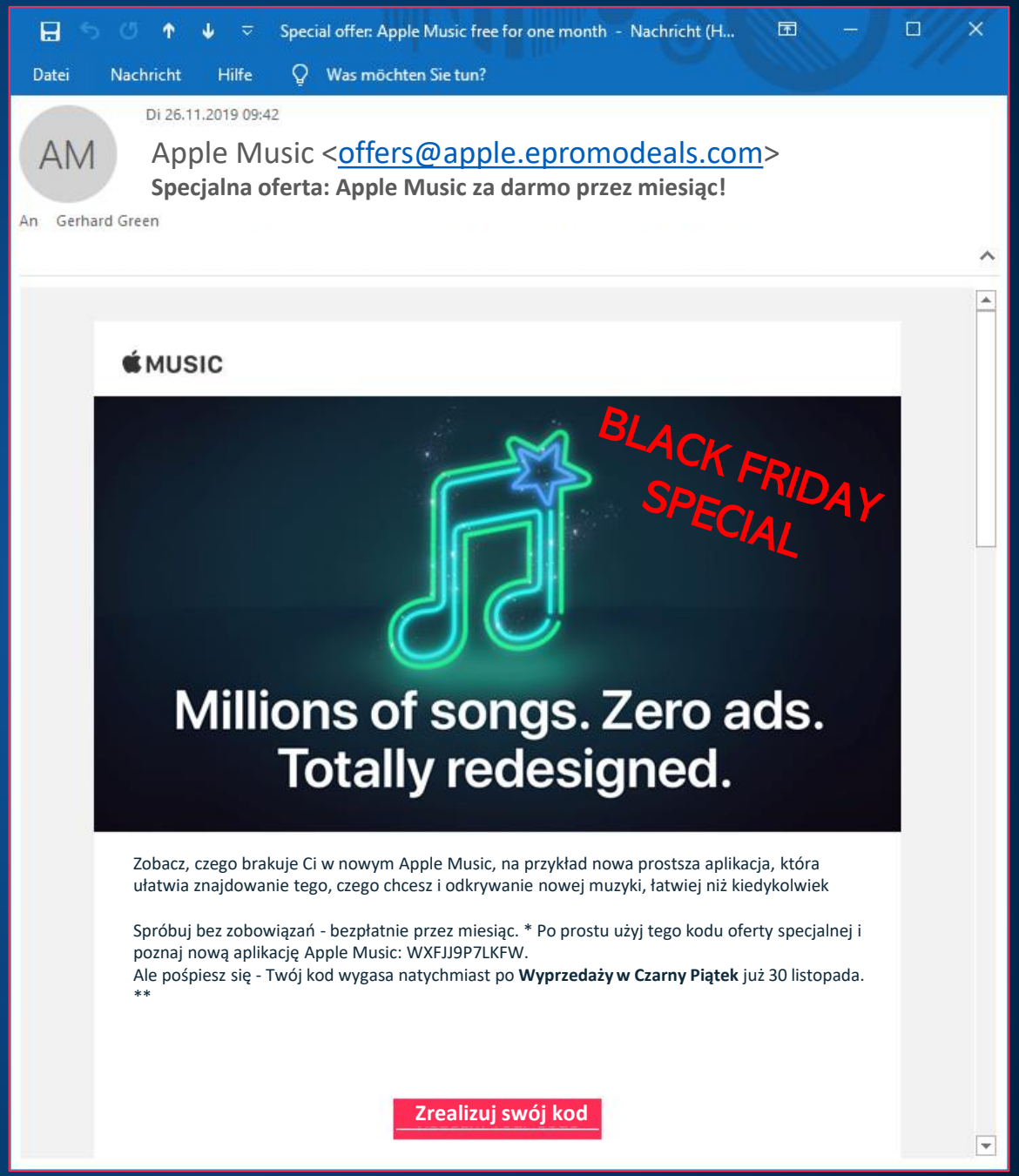
Mass
Phishing

Spear
Phishing

BEC
Business Email
Compromise

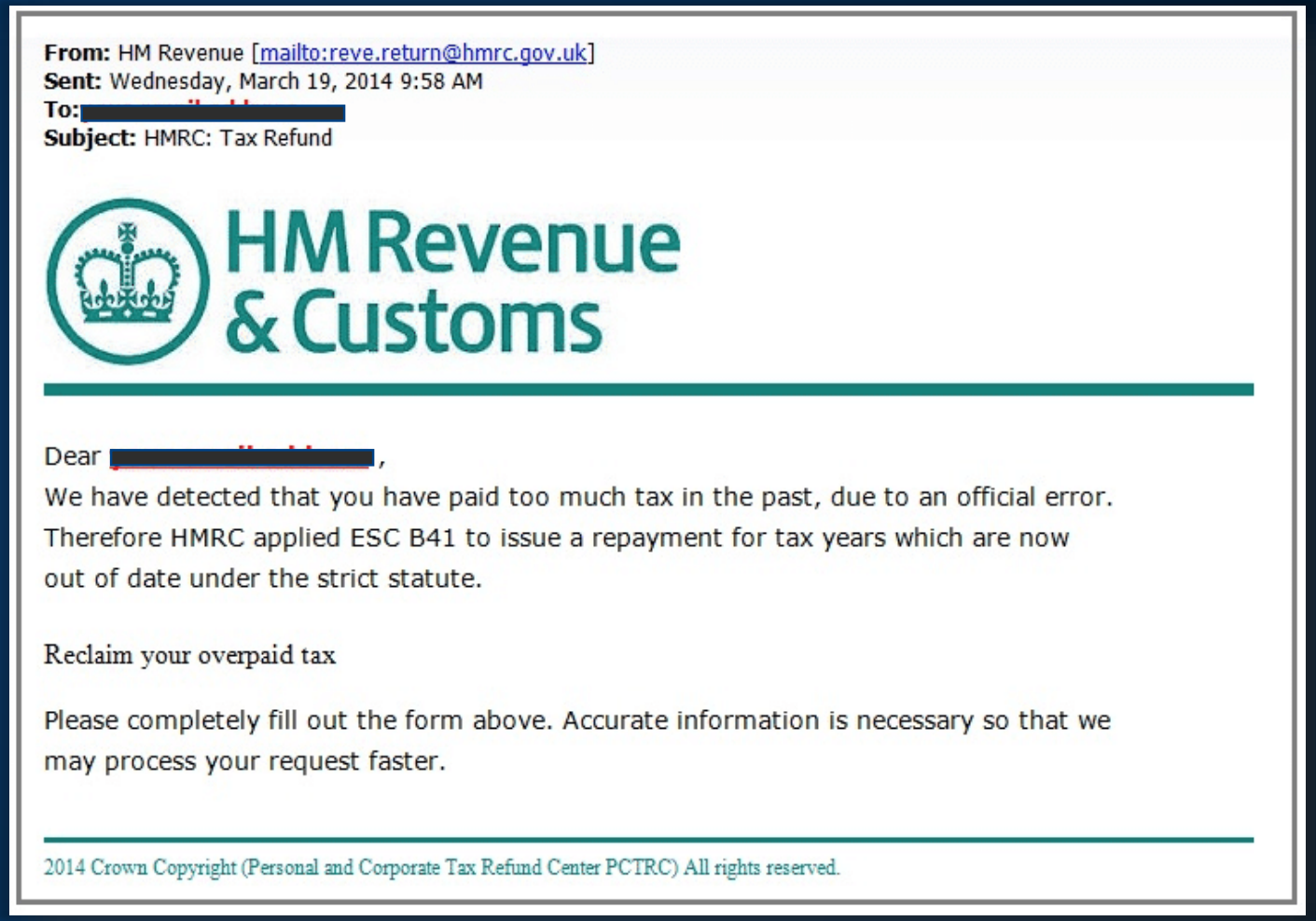
Mass Phishing

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



Spear Phishing

- Celem są indywidulani 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 Therefore HMRC applied ESC B41 to issue a repayment for tax years which are now out of date under the strict statute.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

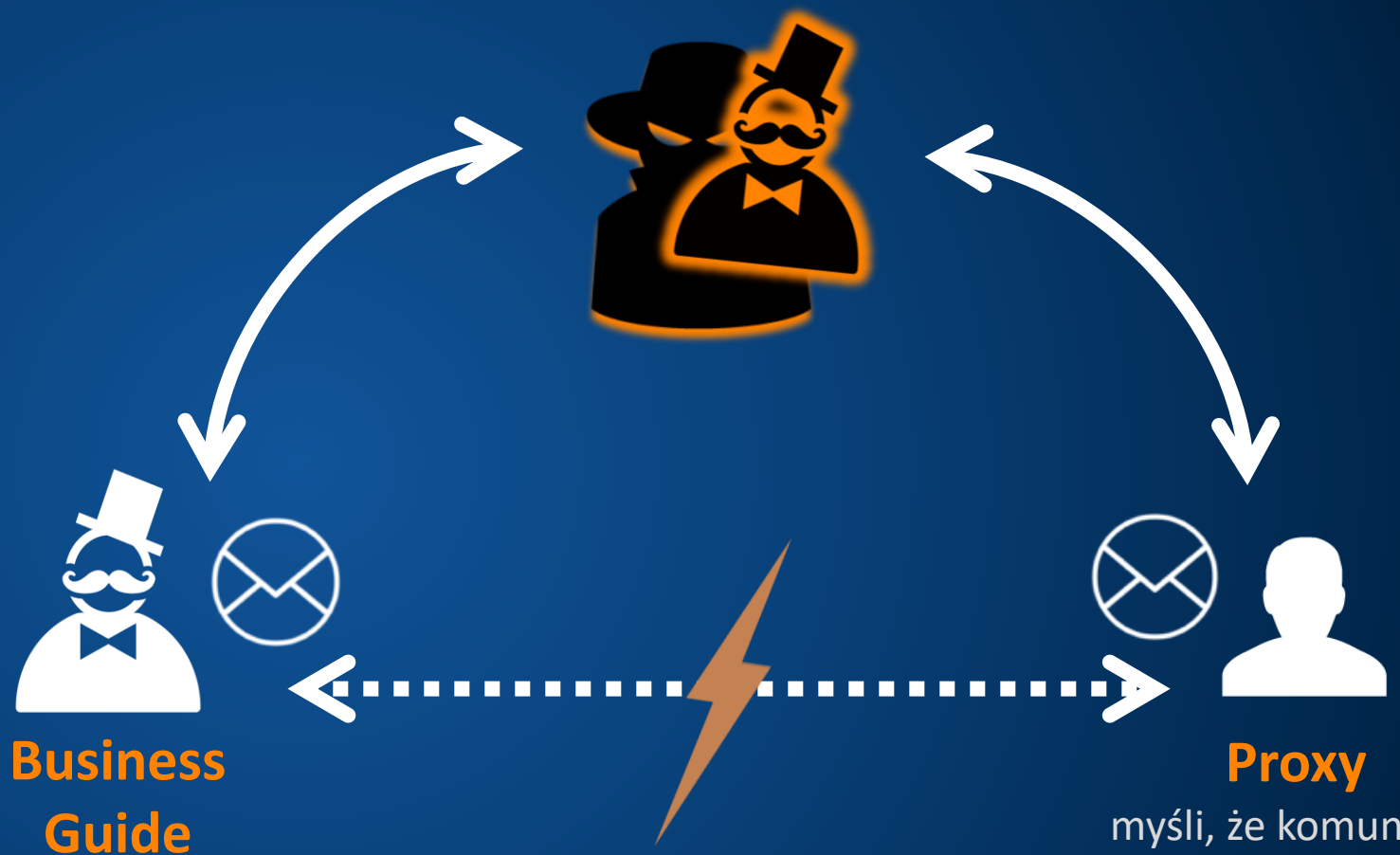
Please completely fill out the form above. Accurate information is necessary so that we may process your request faster.

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

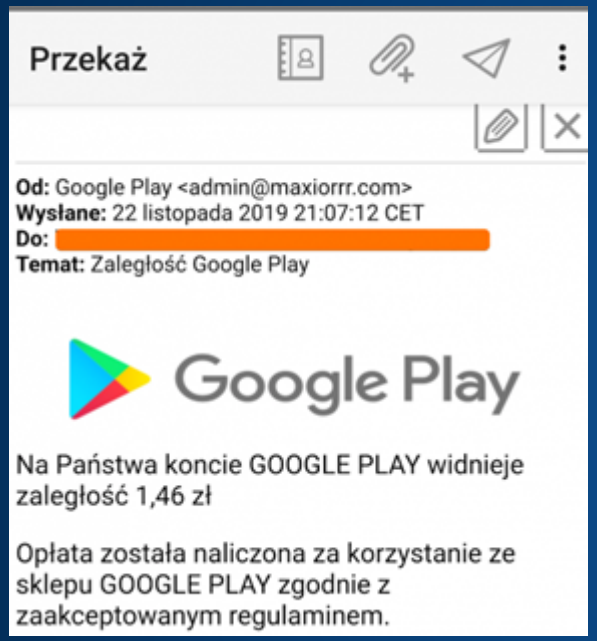
Nadawca: przypominający adres e-mail lub zainfekowana skrzynka pocztowa przełożony

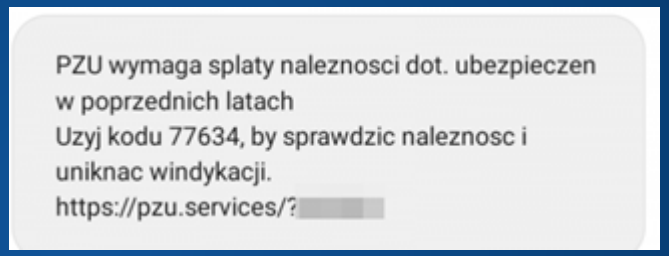


Business Guide

Proxy
myśli, że komunikuje się z Przełożonym

Phishing działa





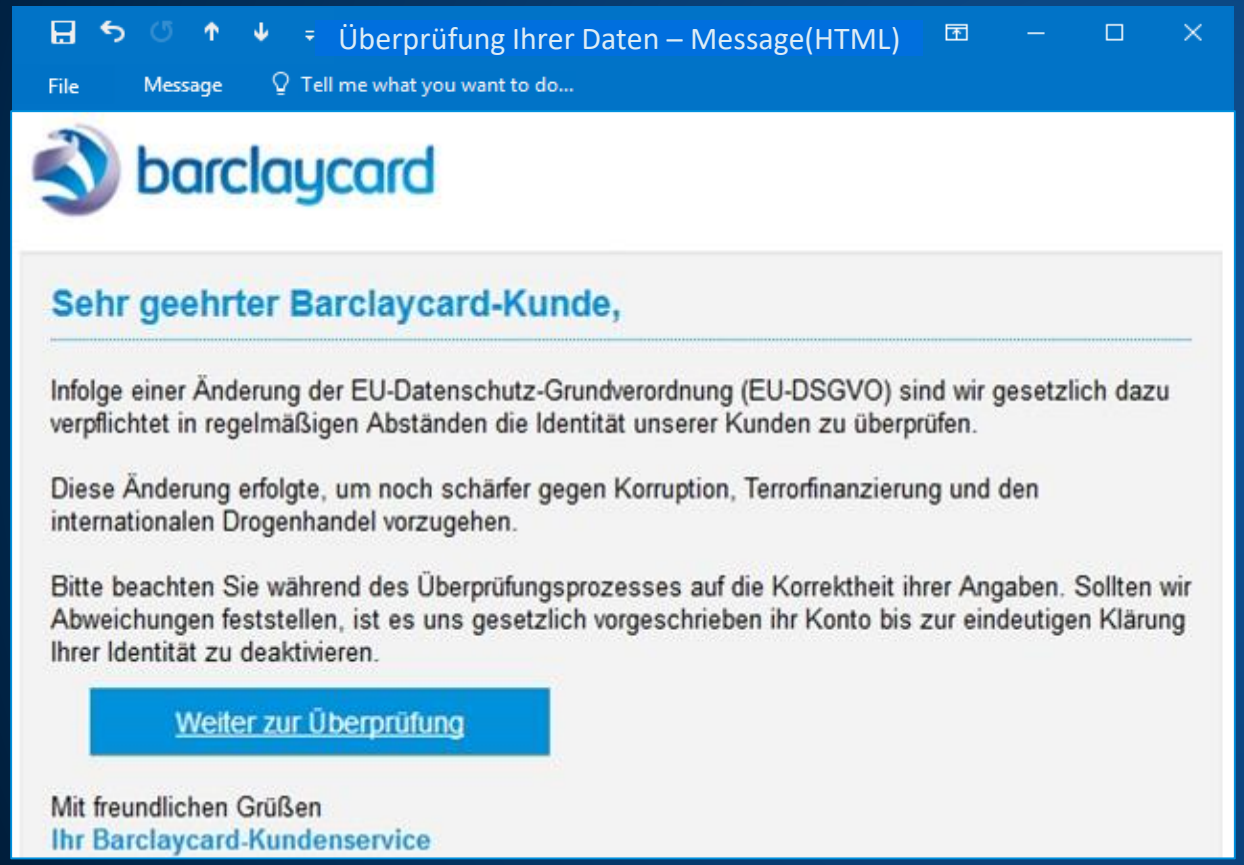
Cele Atakujących

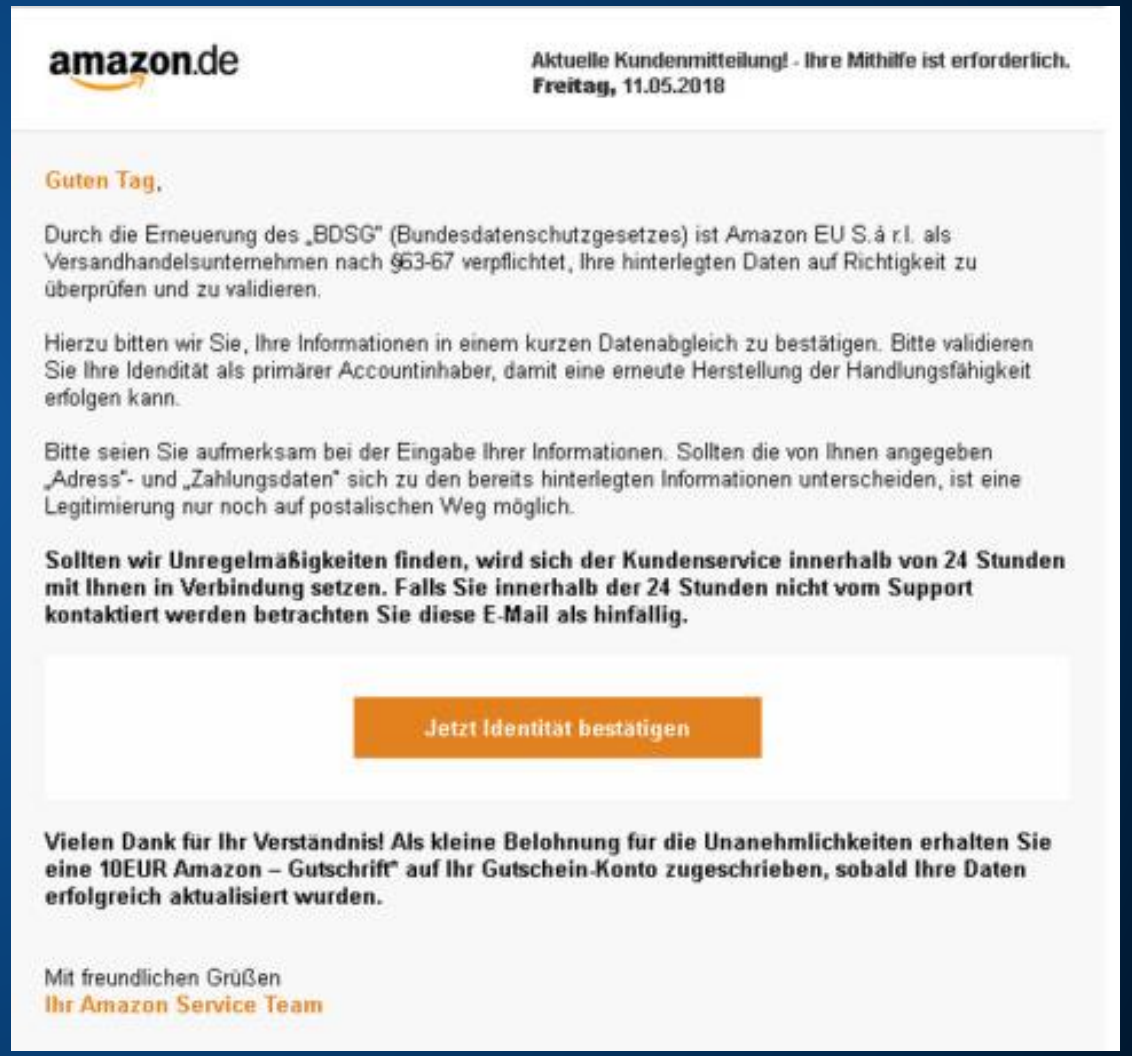
- Dane prywatne
- Dostęp do danych do sieci społecznościowych
- Konta / karty kredytowe
- Manipulacja transakcjami finansowymi
- Instalacja Ransomware

Wiadomości phishingowe są obecnie największym kanałem dystrybucji Ransomware

SOPHOS

RODO jest również wykorzystywane.



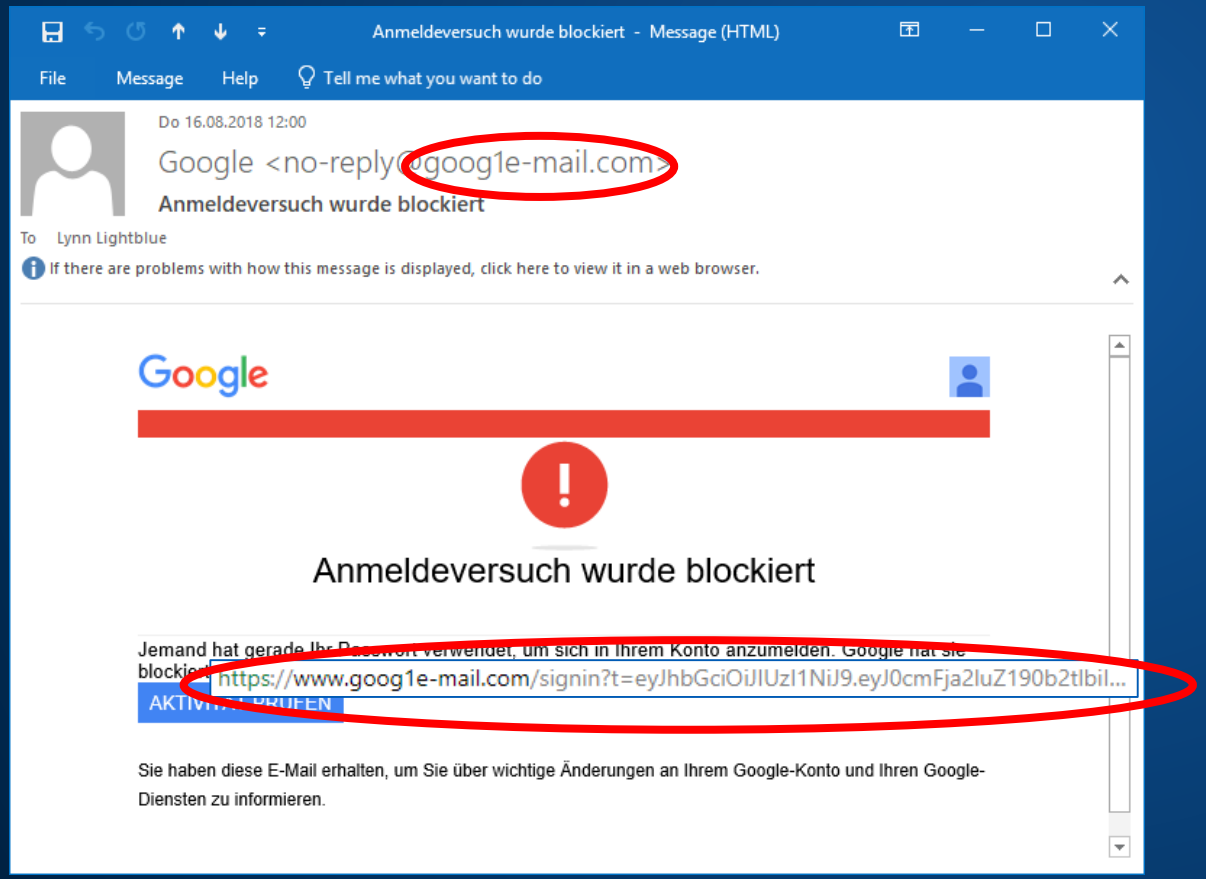


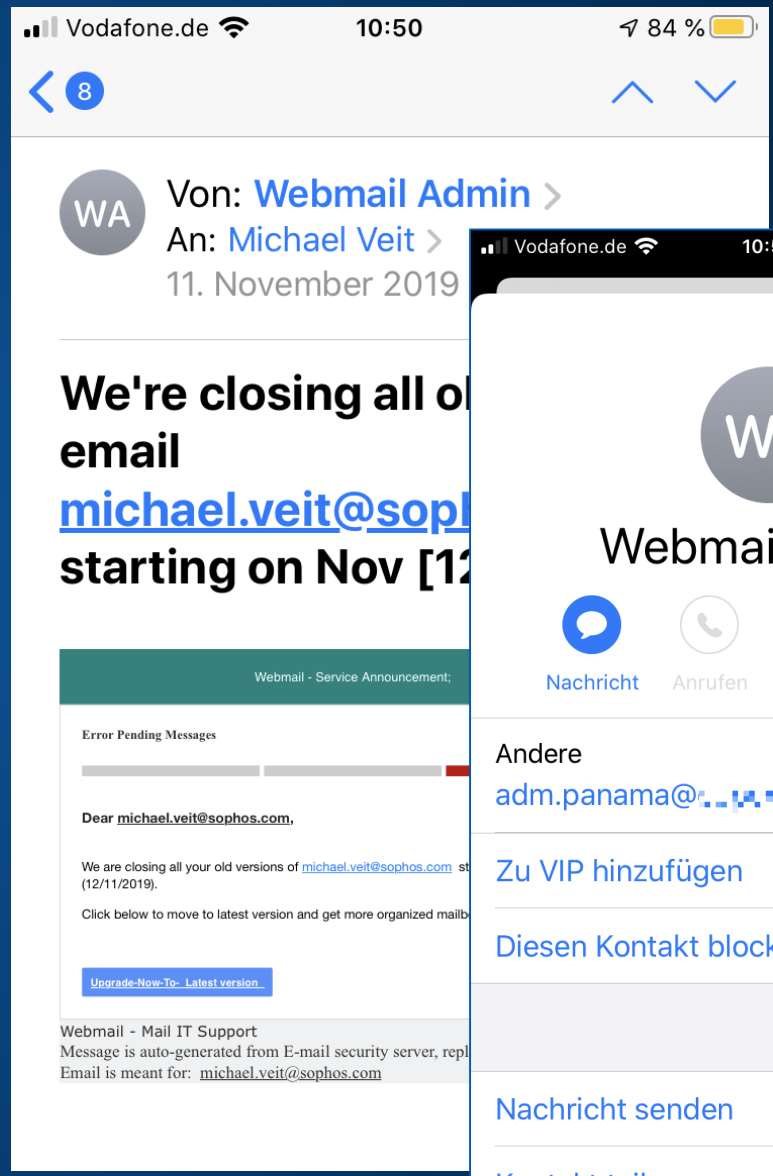
Jak sam mogę się zabezpieczyć?

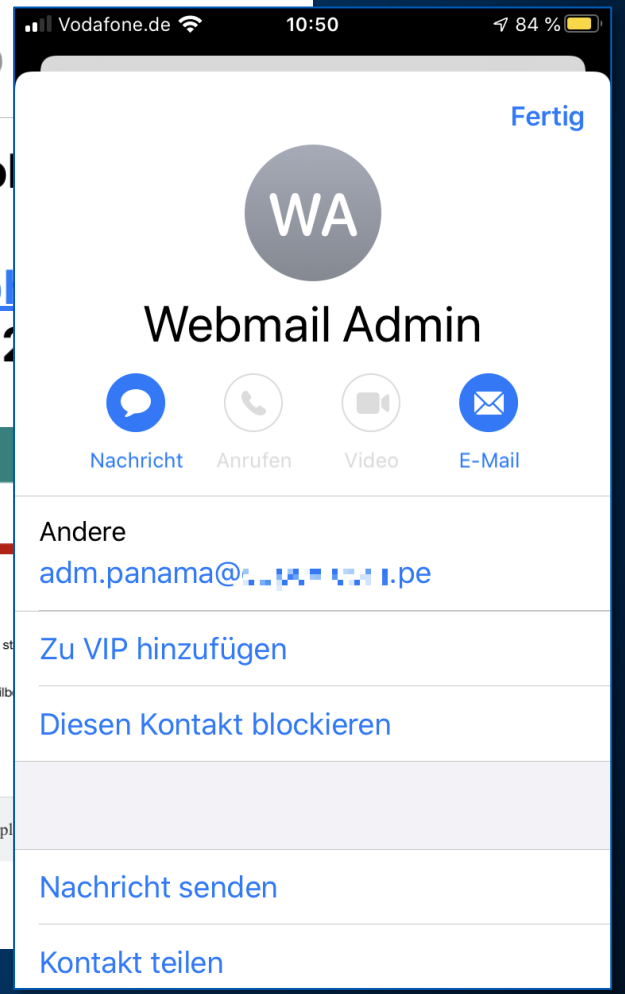
SOPHOS

1. Ja sam

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







SOPHOS

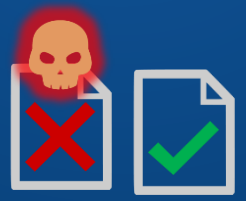
2. Technologia

Email & Web Protection

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

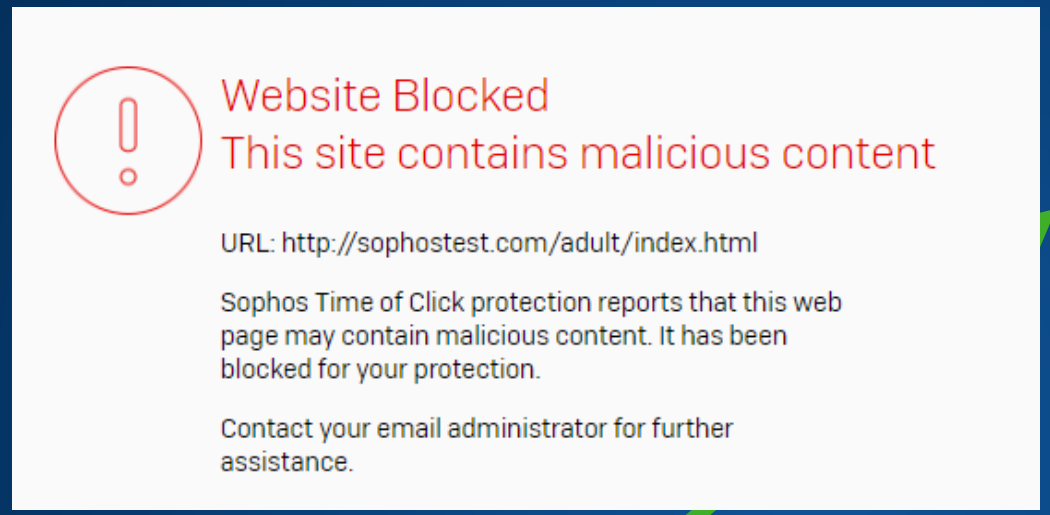
Sandboxing

- Analiza zachowania
- Deep Learning

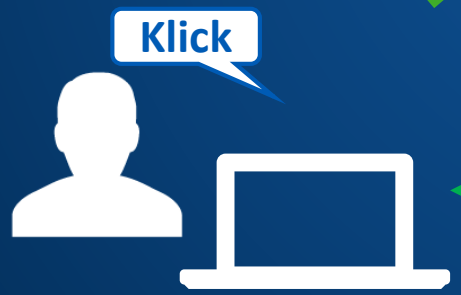


Email-Service

Time-of-Click



Link jest sprawdzany w momencie kliknięcia

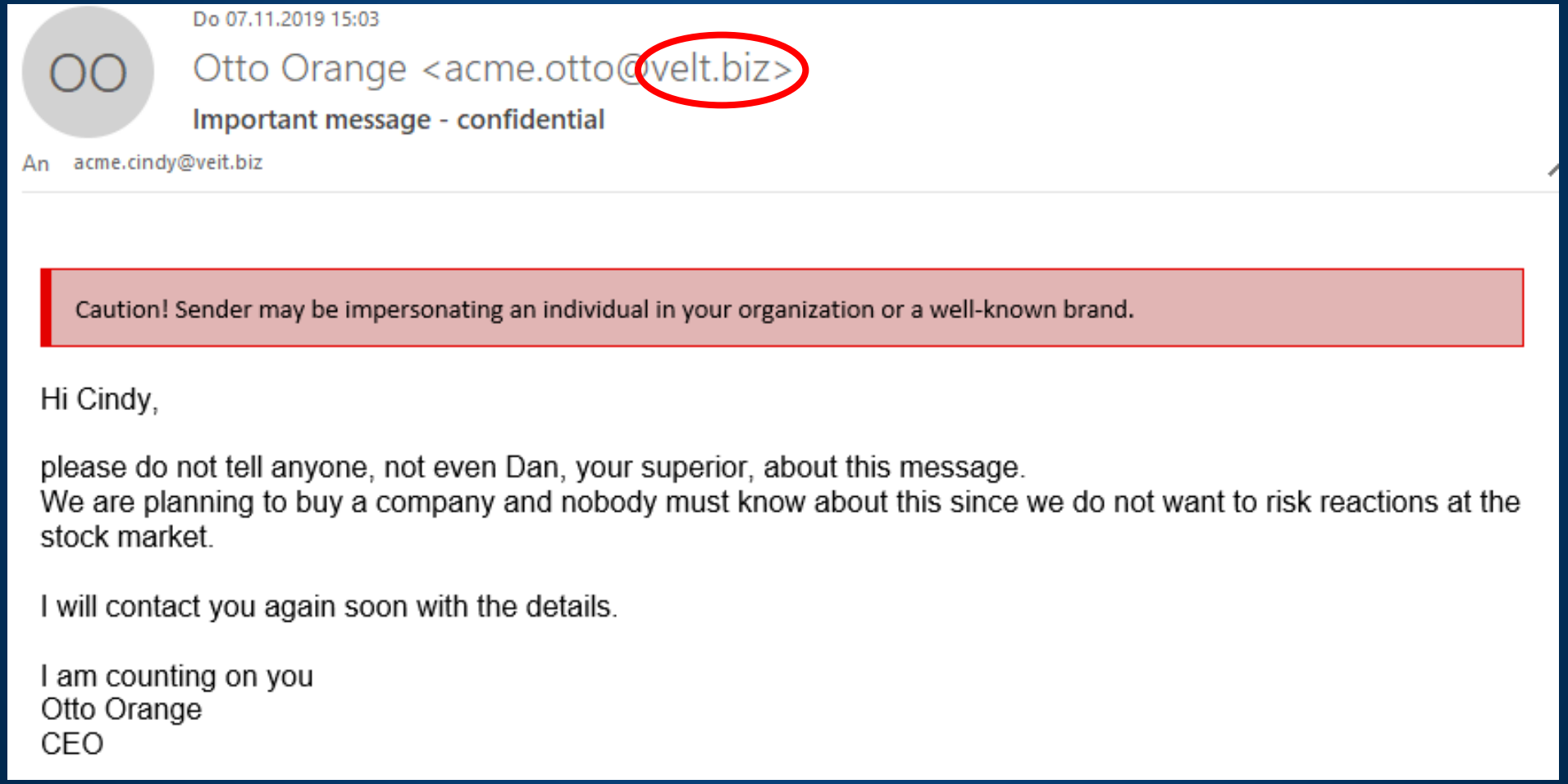


Email Service

Linki w e-mailach są zastąpione linkiem Sophos

SOPHOS

Ochrona przed transferem tożsamości



Do 07.11.2019 15:03

OO

Otto Orange <acme.otto@velt.biz>

Important message - confidential

An acme.cindy@veit.biz

Caution! Sender may be impersonating an individual in your organization or a well-known brand.

Hi Cindy,

please do not tell anyone, not even Dan, your superior, about this message.
We are planning to buy a company and nobody must know about this since we do not want to risk reactions at the stock market.

I will contact you again soon with the details.

I am counting on you
Otto Orange
CEO

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

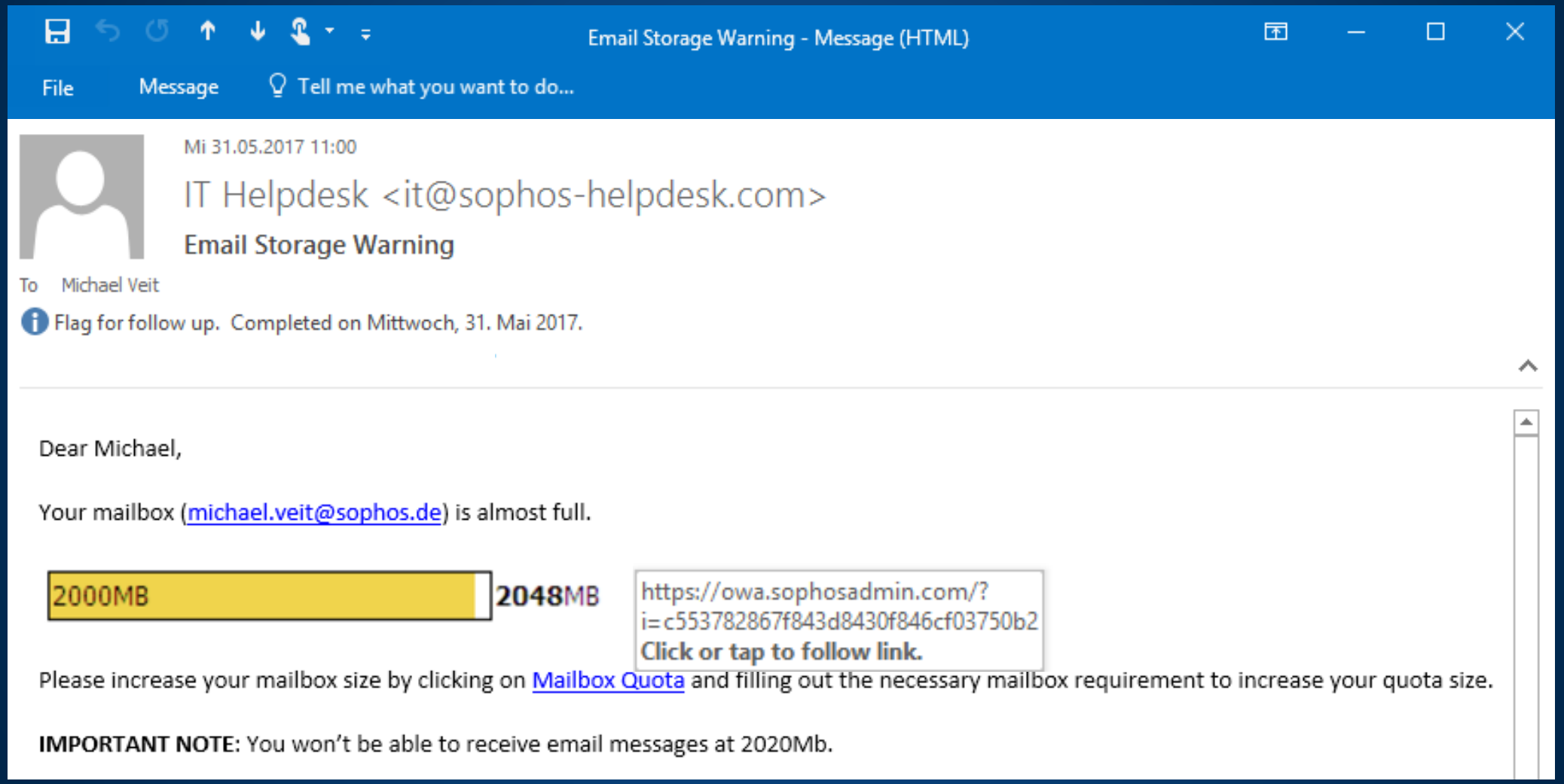
Symaulacja Ataku

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

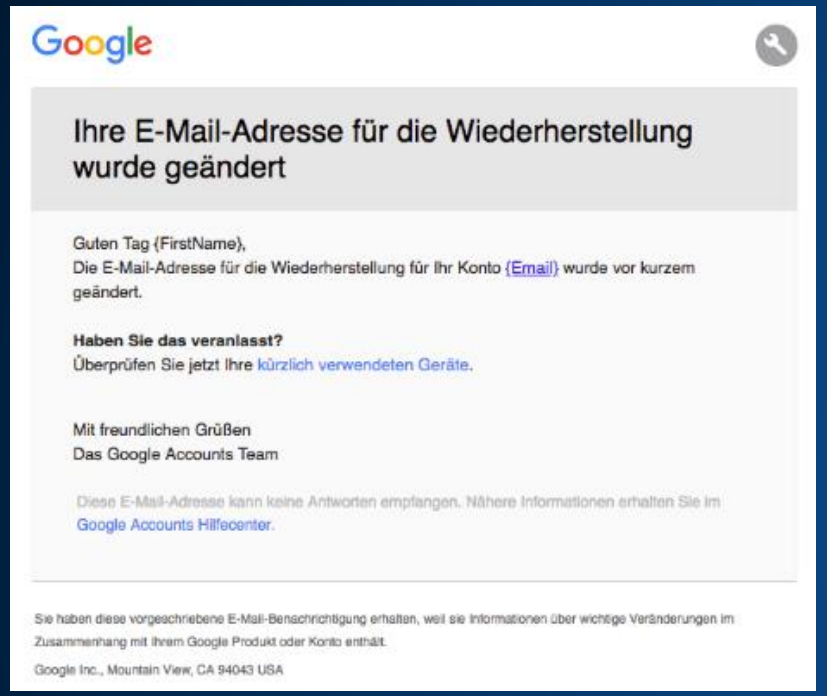
Ochrona Endpoint

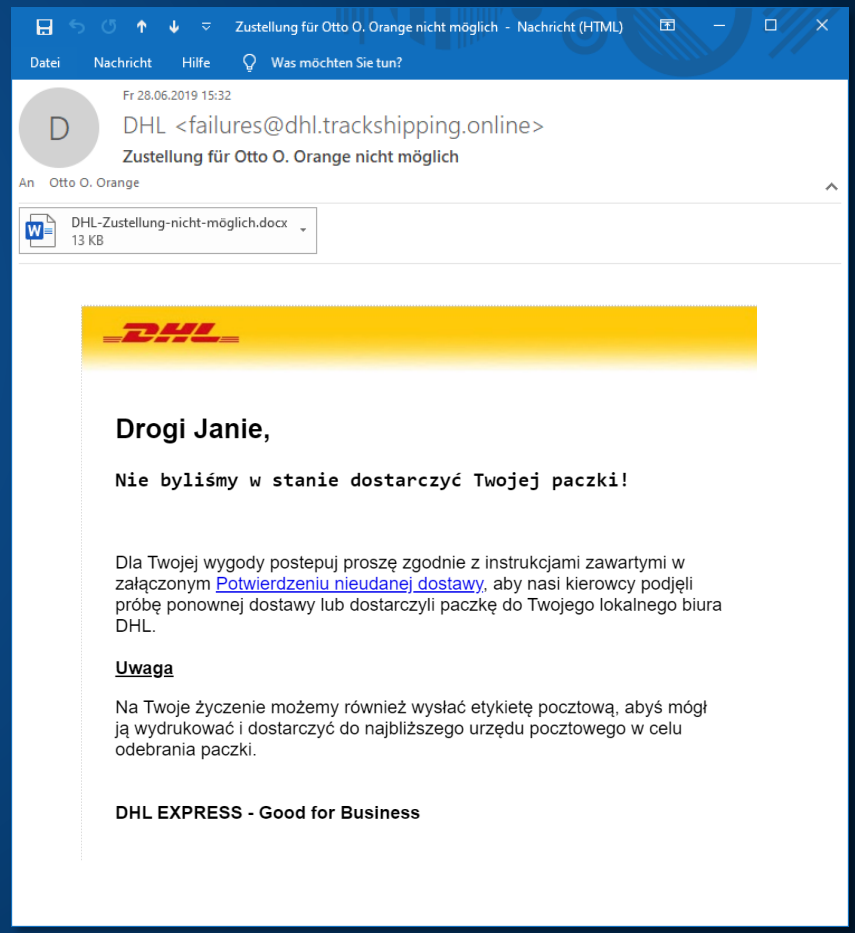
- Anti-Malware
- Anti-Exploit
- Anti-Ransomware
- Anti-Hacker

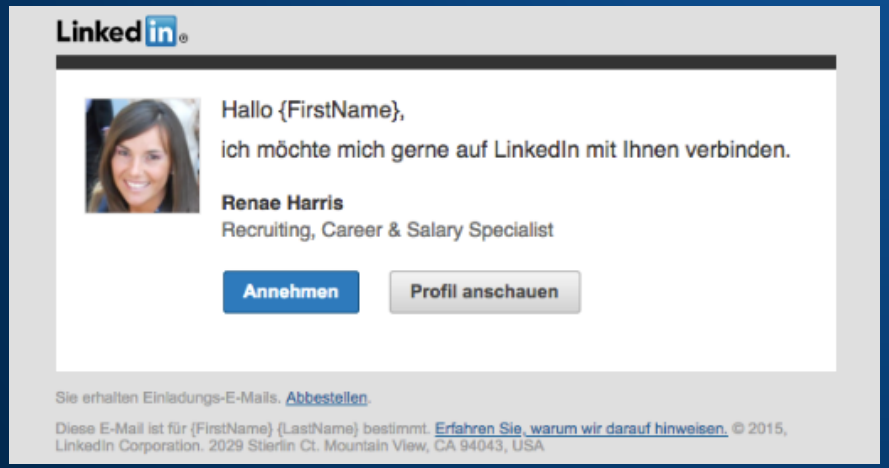
np. Sophos: ciągłe szkolenie i weryfikacja



Przykłady w praktyce





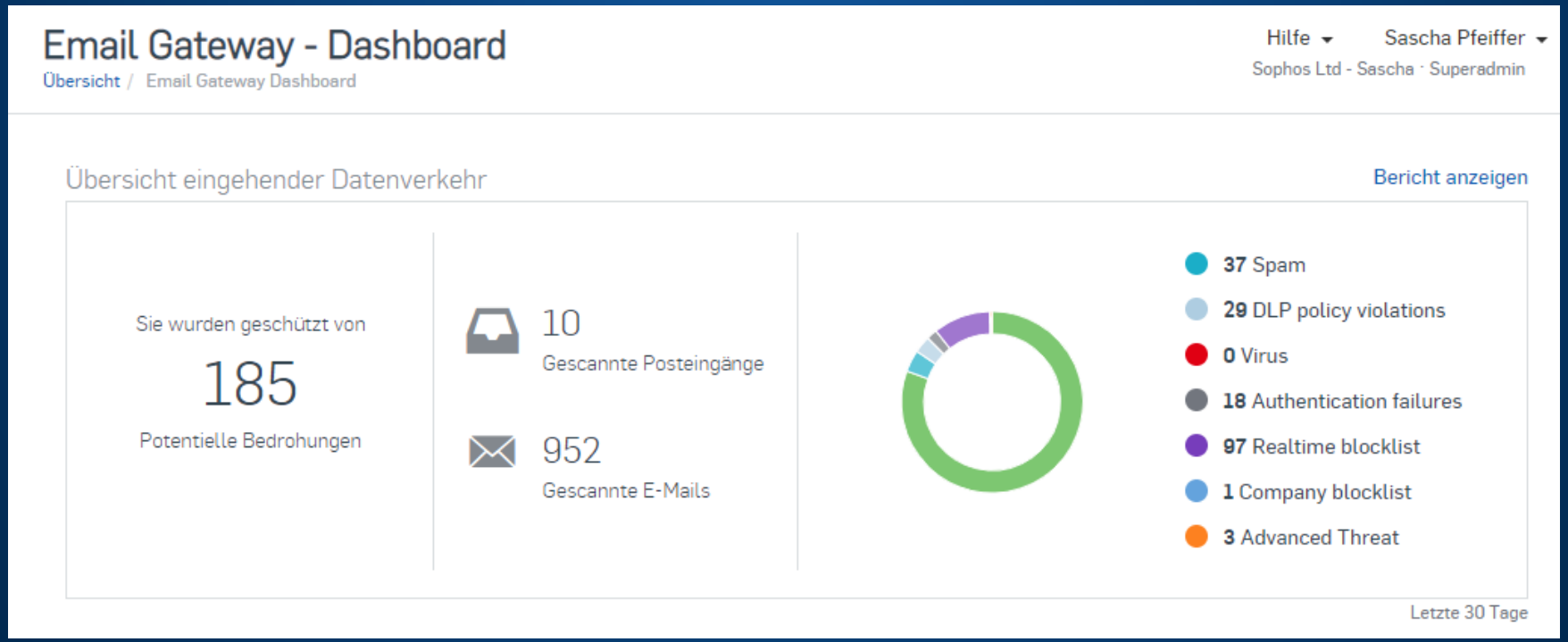


Jak SOPHOS może pomóc?

SOPHOS

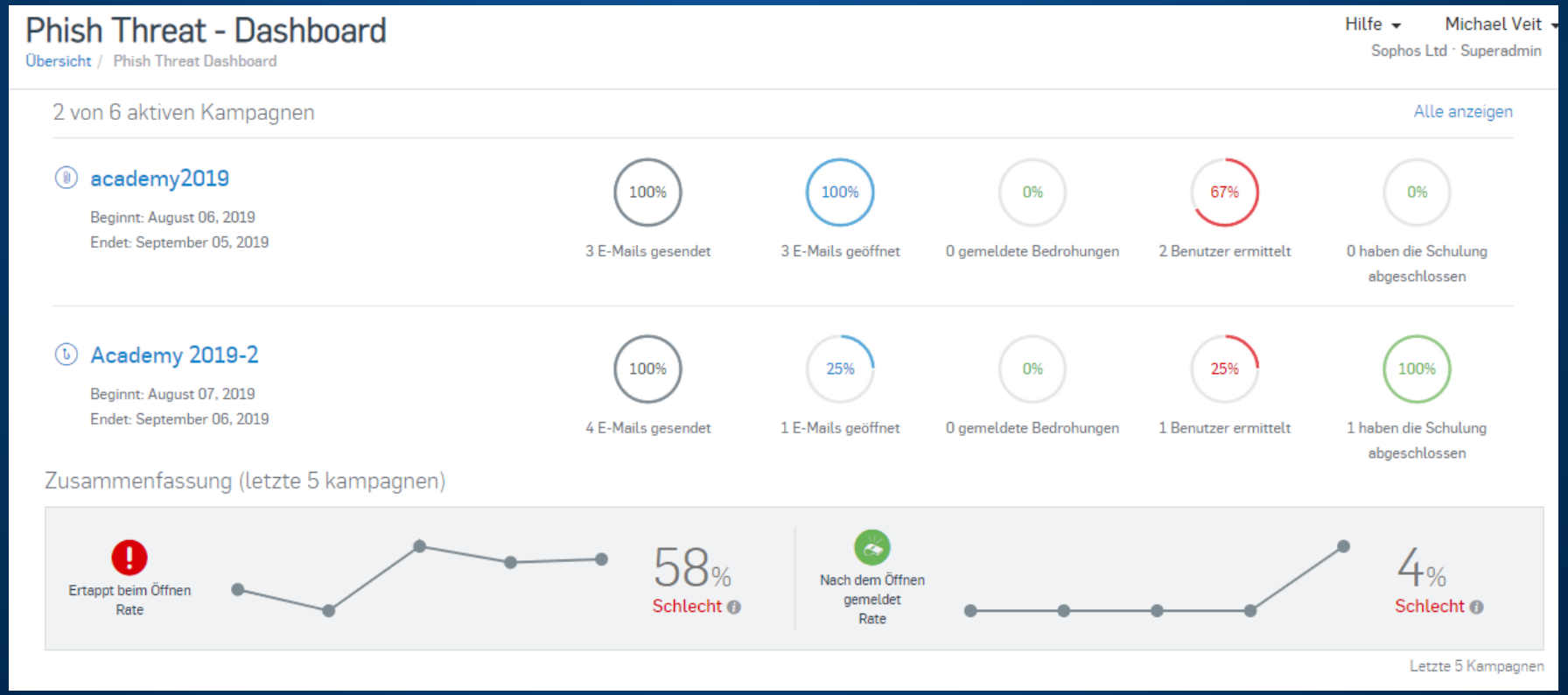
Central Email

- Pełna ochrona poczty e-mail przed złośliwym oprogramowaniem, spamem i phishingiem, w tym sanboxing, 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



SOPHOS

Pytania?

MidMarketSalesDE@sophos.de