FH JOANNEUM
University of Applied Sciences

Digital Innovation Hub

Aktives Phishing zur Mitarbeitersensibilisierung
Erfahrungen/Tools/Einschränkungen

Fruhmann

DIHSÜD
Digital Innovation Hub

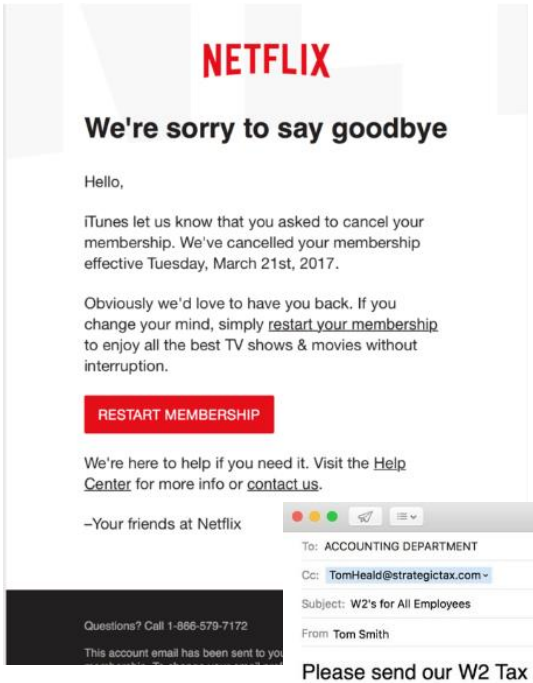
FH JOANNEUM
University of Applied Sciences

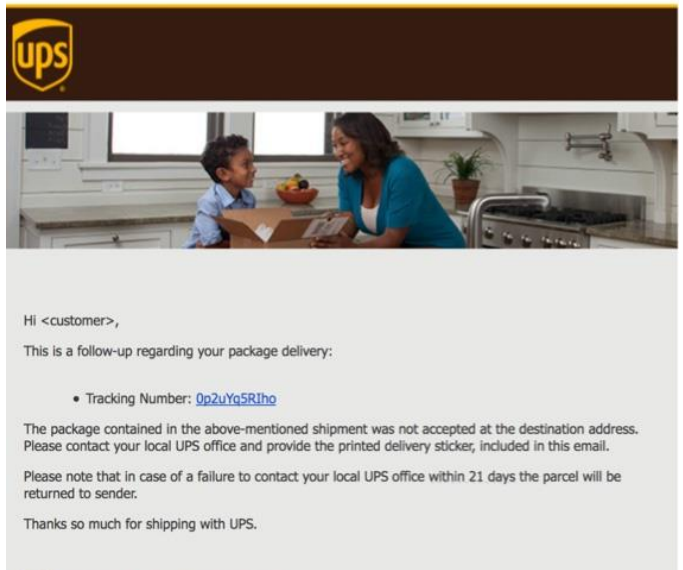
Über mich

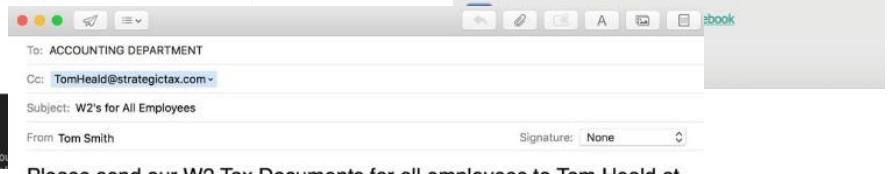
- **Martin Fruhmann**
- Studium IT & Mobile Security @ FH JOANNEUM
- Lehrender @ FH JOANNEUM
  - Netzwerk Technologien
  - Netzwerk Security
  - IT-Security
  - Penetration Testing
  - Phishing

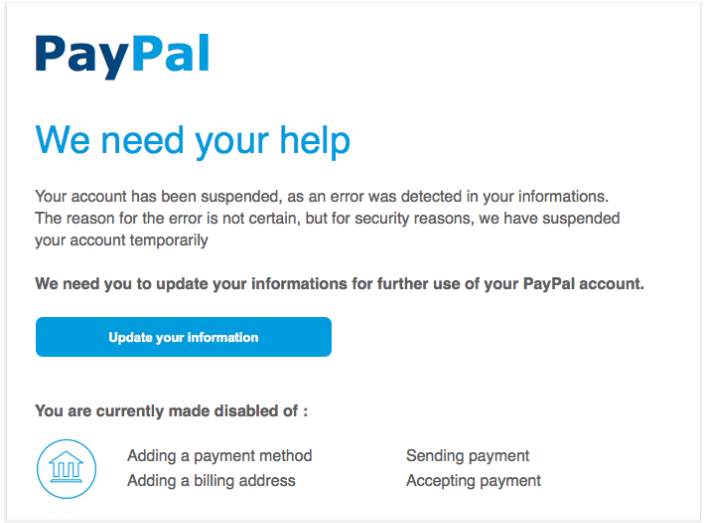
OFFENSIVE security
OSCP

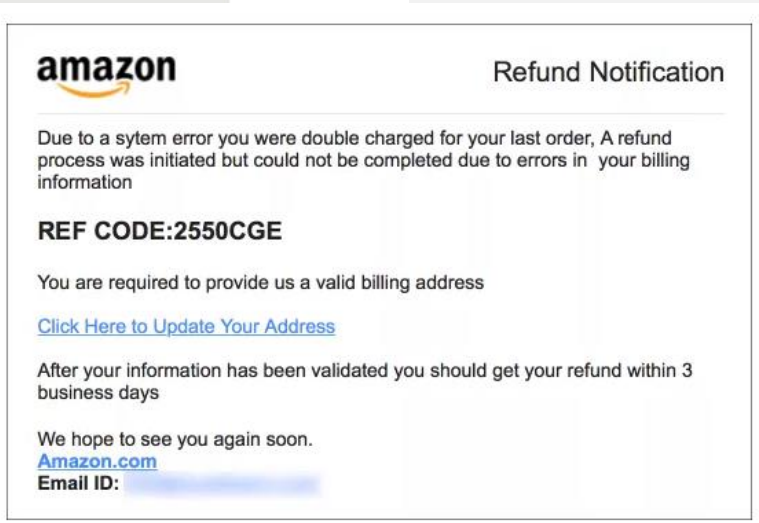
Phishing Basics







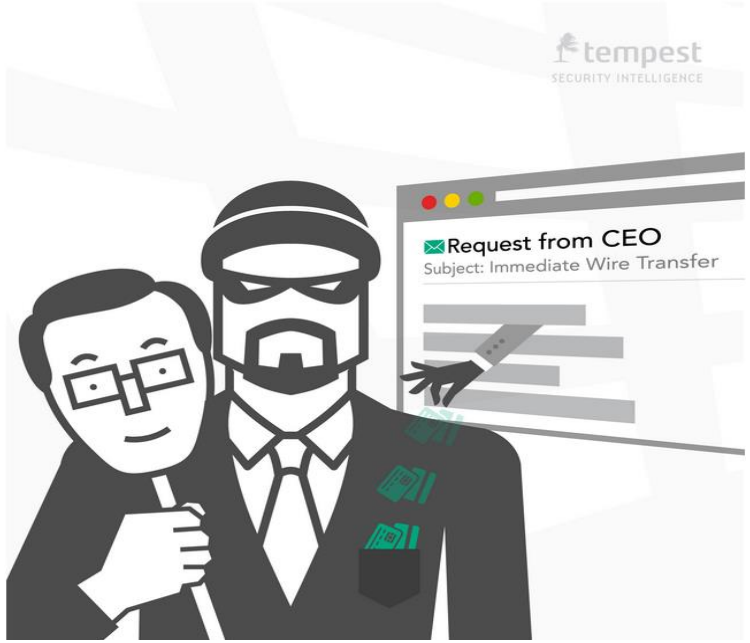




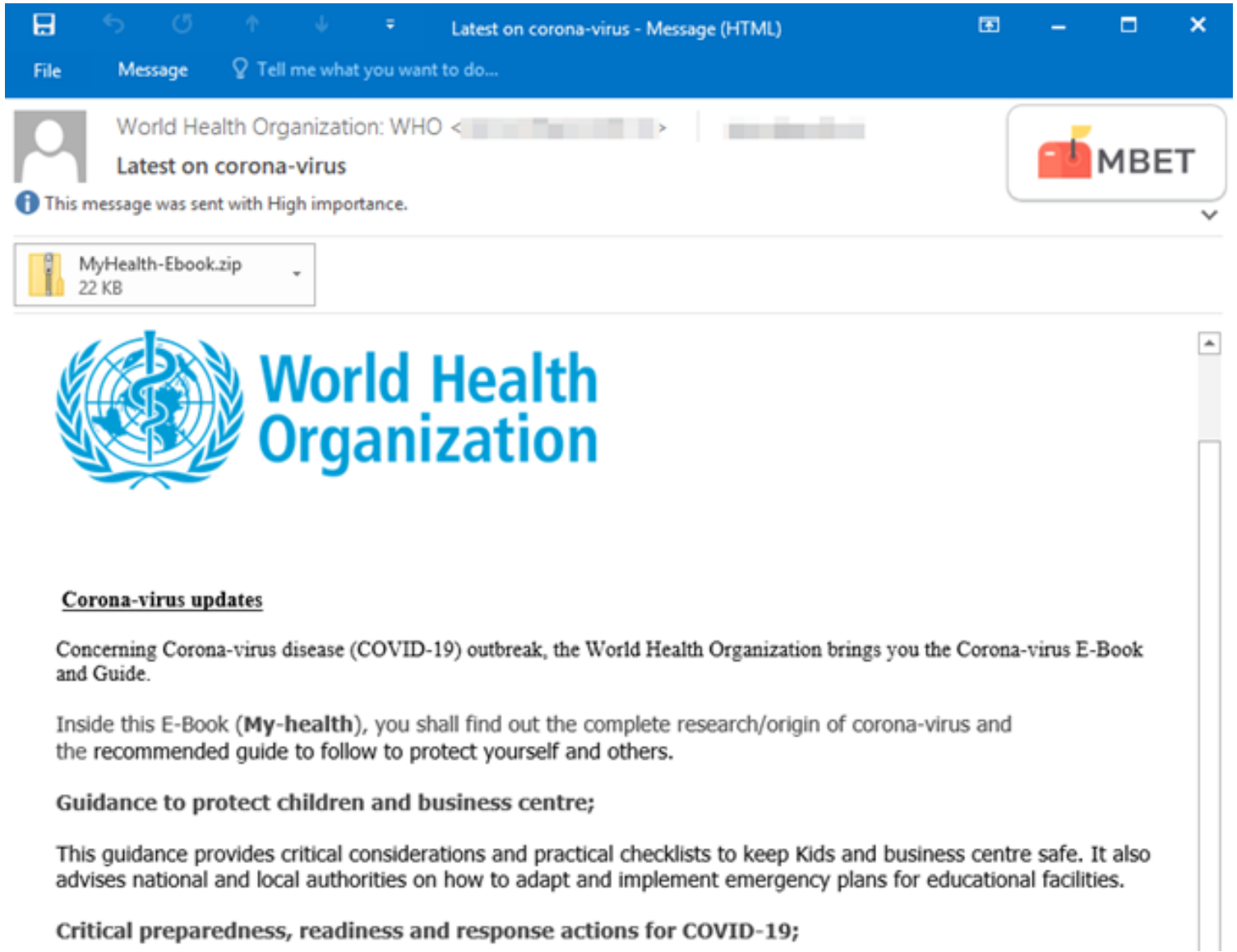
https://www.edts.com/edts-blog/15-examples-of-phishing-emails-from-2016-2017

Ziele von Angreifern

- Infektion mit Schadsoftware
  - Links auf Webseiten mit Schadsoftware
  - Infektiöse Anhänge (z.B. .xls, .doc, .exe)
- Abgreifen von Login Daten
  - Nachgeahmte Webseiten mit Login Feldern
  - Mögliches Abgreifen von MFA Tokens
- Erpressung, Täuschung, etc
  - CEO – Fraud
  - Afrikanischer Prinz
  - …

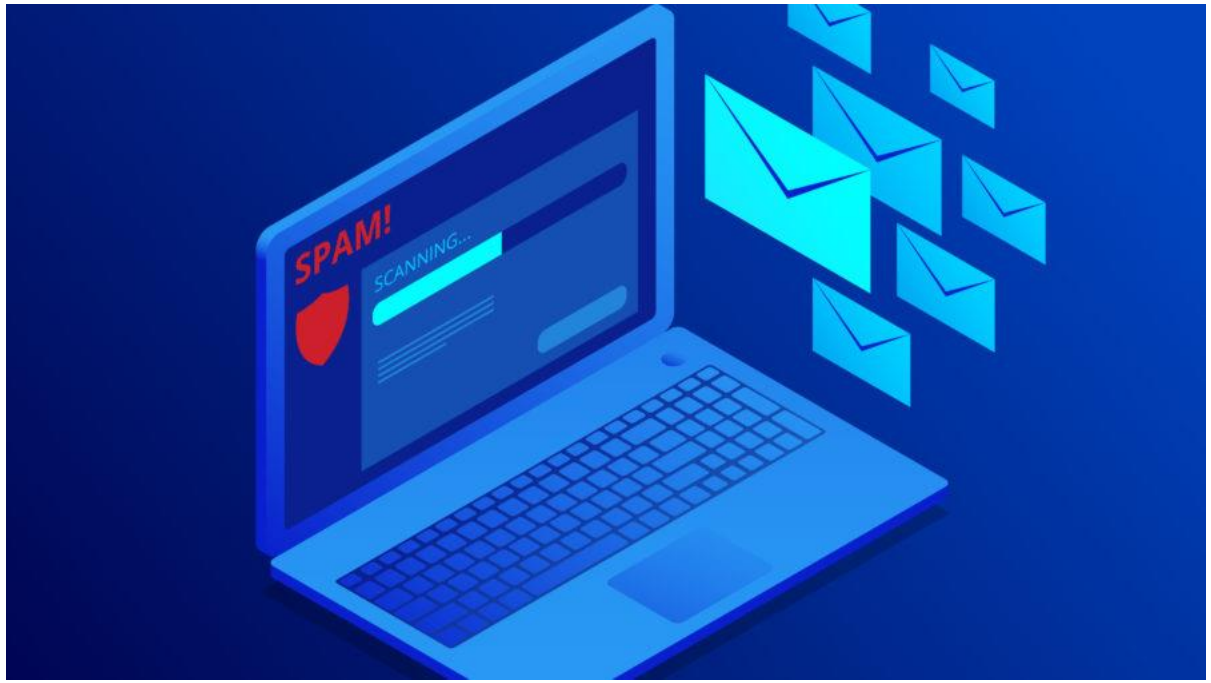


http://blog.tempest.com.br/static/attachments/joao-paulo-campello/increase-in-ceo-fraud-attacks-highlights-risks-to-corporate-envs/1.png

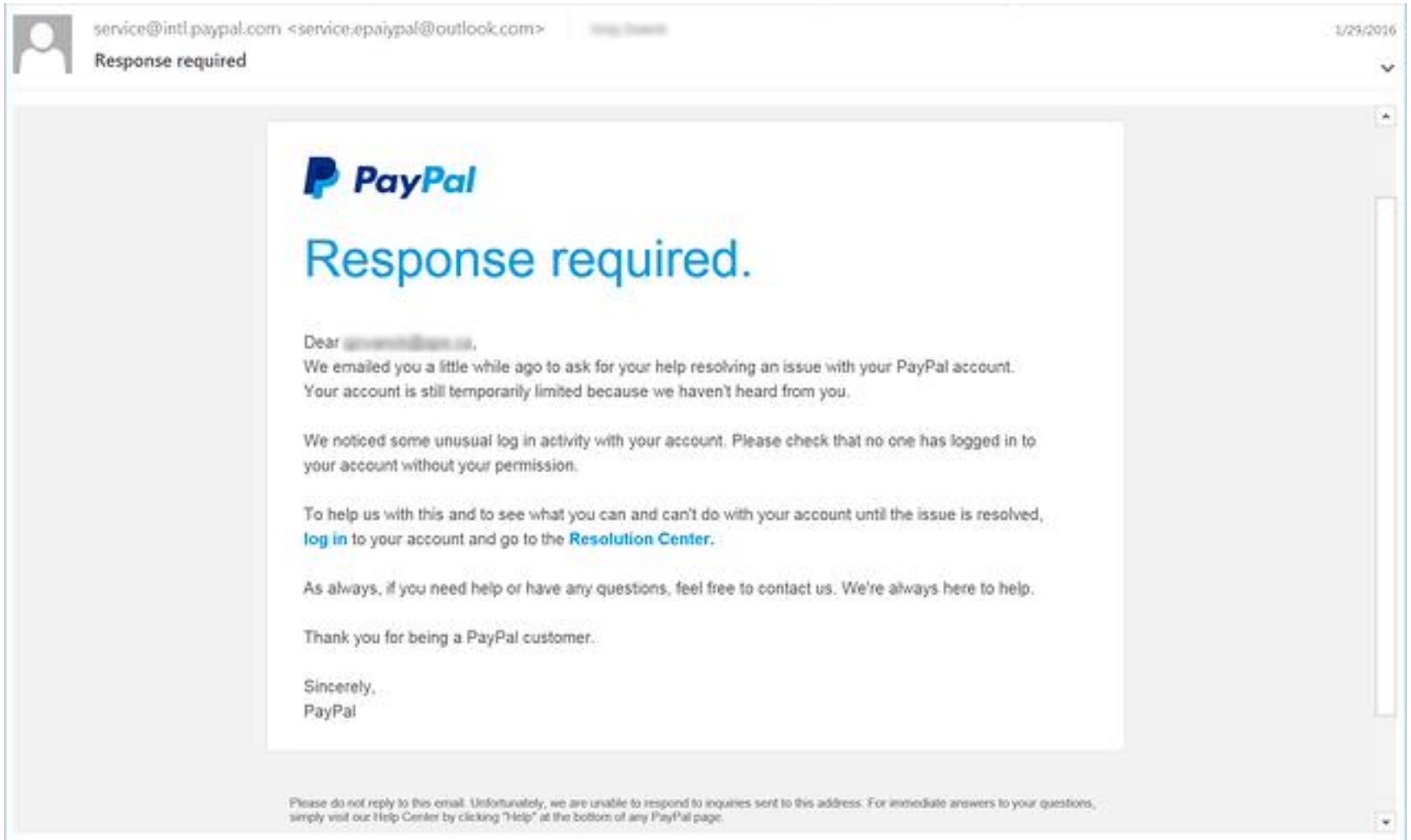

Latest on corona-virus - Message (HTML)
File
Message
Tell me what you want to do...
World Health Organization: WHO <
Latest on corona-virus
This message was sent with High importance.
MBET
MyHealth-Ebook.zip
22 KB
World Health Organization
Corona-virus updates
Concerning Corona-virus disease (COVID-19) outbreak, the World Health Organization brings you the Corona-virus E-Book and Guide.
Inside this E-Book (My-health), you shall find out the complete research/origin of corona-virus and the recommended guide to follow to protect yourself and others.
Guidance to protect children and business centre;
This guidance provides critical considerations and practical checklists to keep Kids and business centre safe. It also advises national and local authorities on how to adapt and implement emergency plans for educational facilities.
Critical preparedness, readiness and response actions for COVID-19;

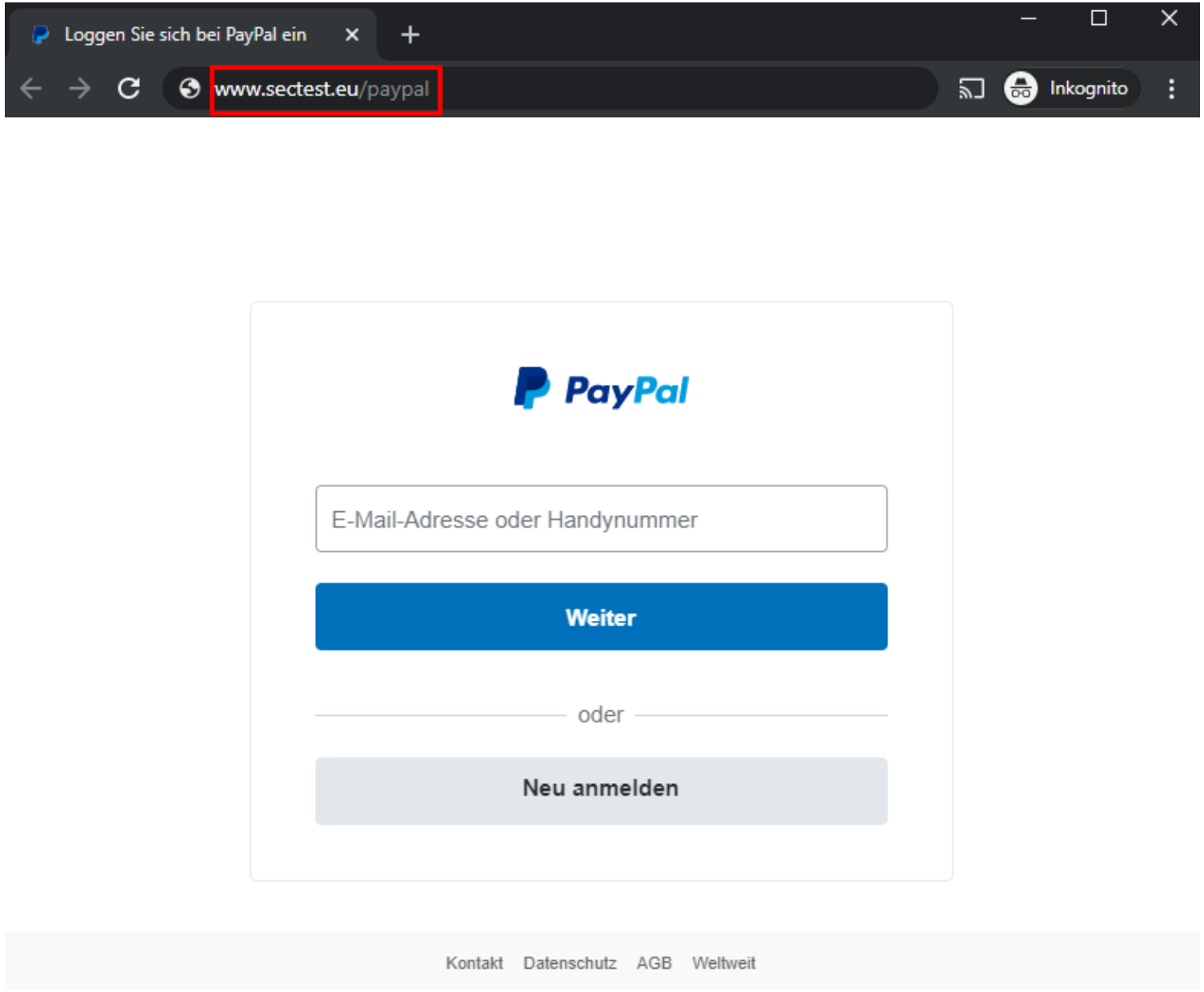
Emotet – Phishing Kampagne

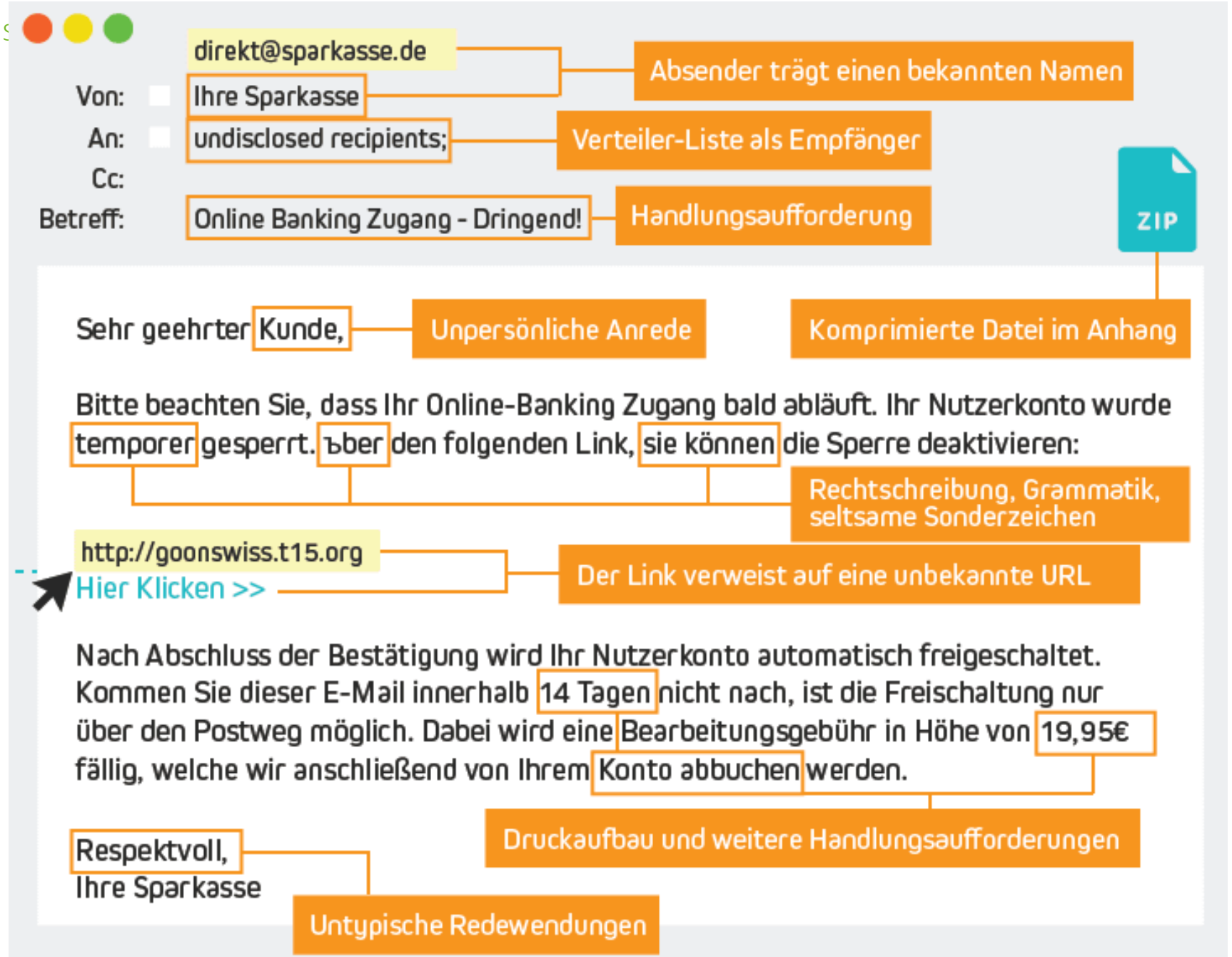
- Seit 2014 – zuerst Bank Trojaner
- Letzte Welle 2019
- Nutzung von alter E-Mail Kommunikation
- Infektion mit Ransomware



https://blog.malwarebytes.com/botnets/2019/09/emotet-is-back-botnet-springs-back-to-life-with-new-spam-campaign/

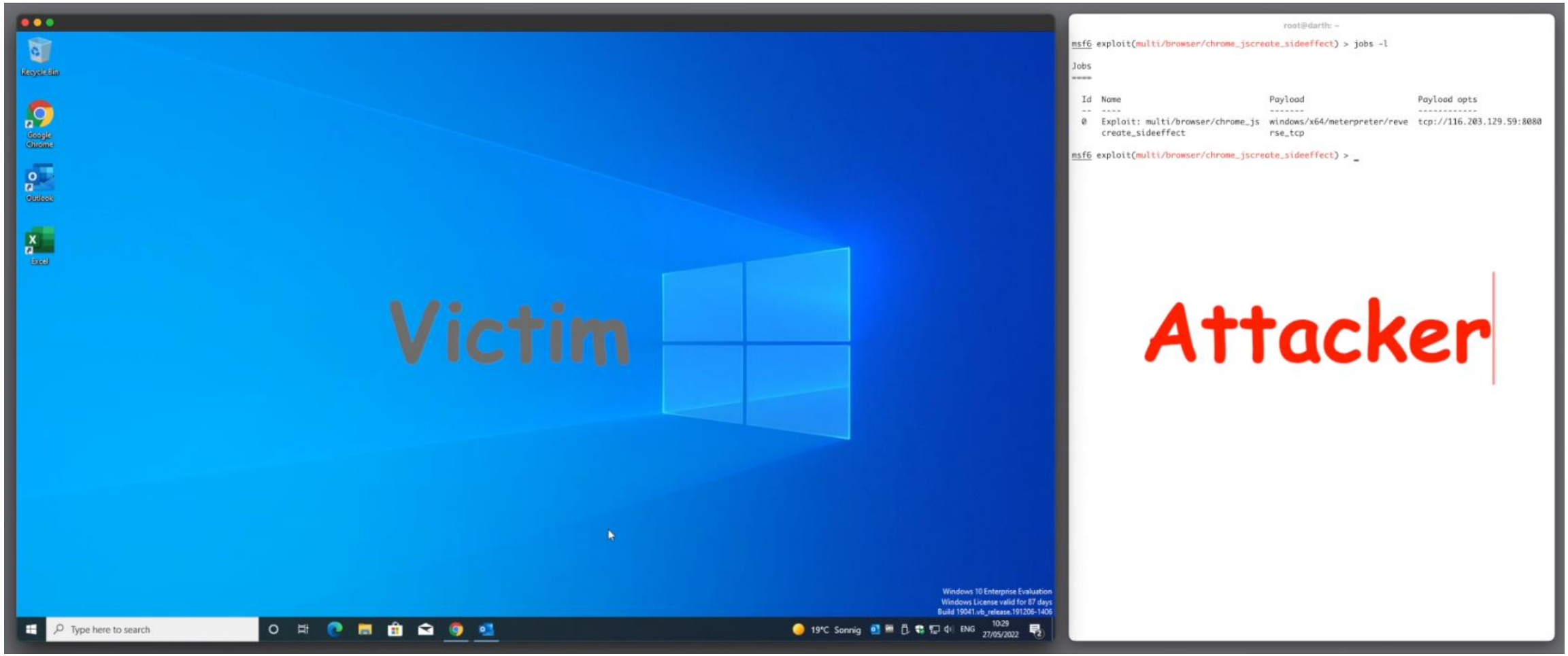

service@intl.paypal.com <service.epaypal@outlook.com>
1/29/2016
Response required
PayPal
Response required.
Dear
We emailed you a little while ago to ask for your help resolving an issue with your PayPal account.
Your account is still temporarily limited because we haven't heard from you.
We noticed some unusual log in activity with your account. Please check that no one has logged in to your account without your permission.
To help us with this and to see what you can and can't do with your account until the issue is resolved, log in to your account and go to the Resolution Center.
As always, if you need help or have any questions, feel free to contact us. We're always here to help.
Thank you for being a PayPal customer.
Sincerely,
PayPal
Please do not reply to this email. Unfortunately, we are unable to respond to inquiries sent to this address. For immediate answers to your questions, simply visit our Help Center by clicking "Help" at the bottom of any PayPal page.


Loggen Sie sich bei PayPal ein
www.sectest.eu/paypal
Inkognito
PayPal
E-Mail-Adresse oder Handynummer
Weiter
oder
Neu anmelden
Kontakt
Datenschutz
AGB
Weltweit



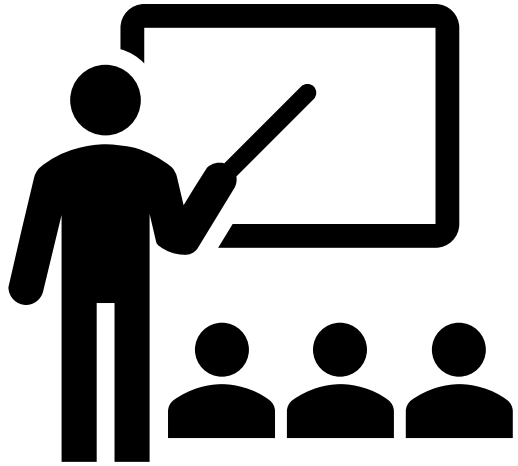
https://www.betrugstest.com/phishing

Phishing – Bösartige Links



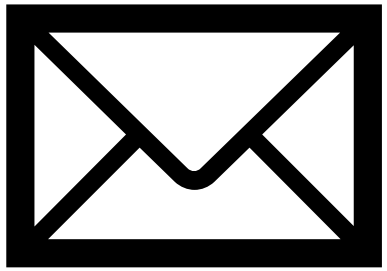
Mögliche Awareness Maßnahmen

- Awareness Training Vortrag
  - Teils schwierige Zielgruppen
  - Zeitintensiv
  - Sehr kurze Halbwertszeit im Bezug auf Wissen



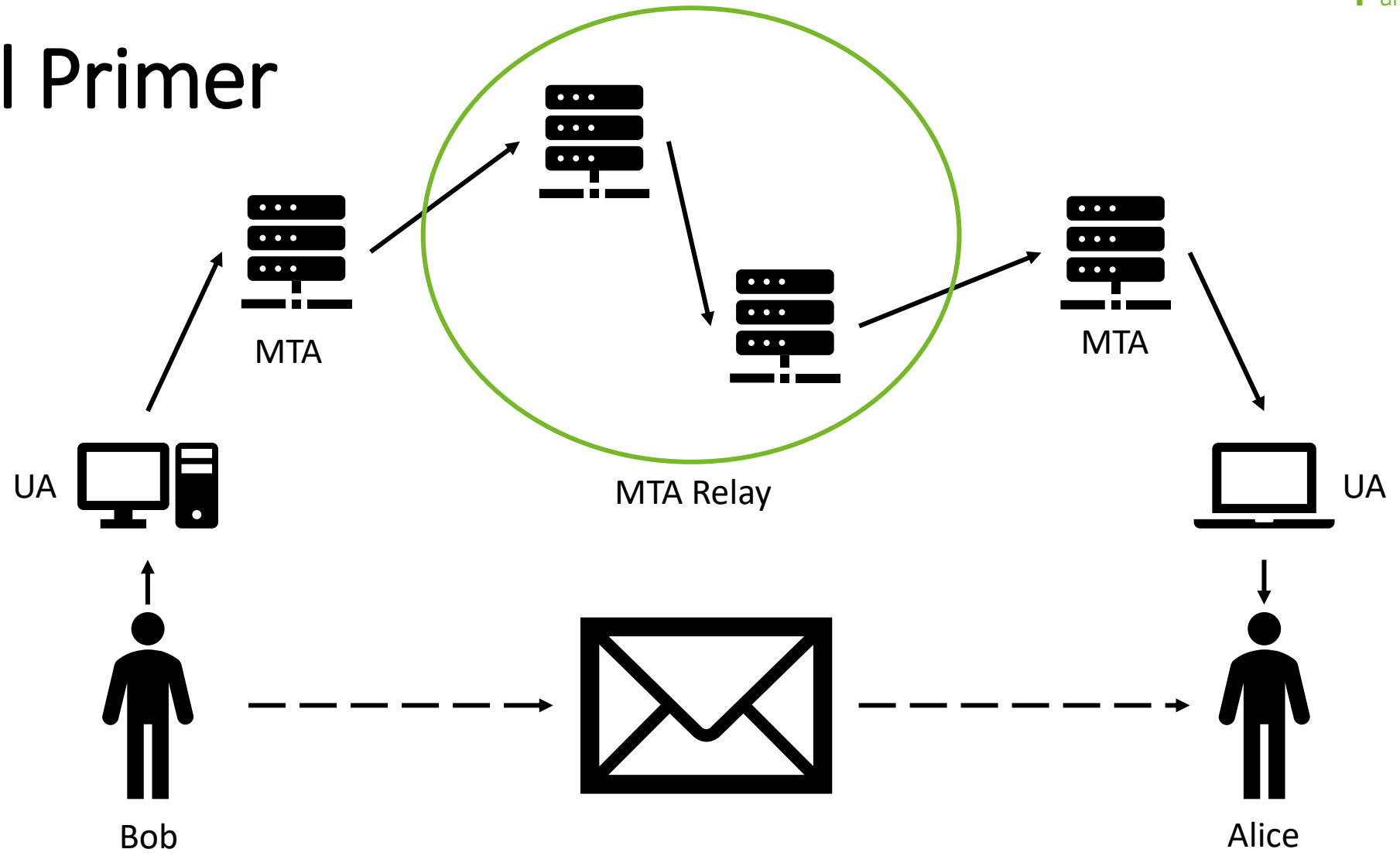
vs.

- Aktives Phishing
  - Relevant für jeden -> niemand will „reinfallen“
  - Sehr kurz (für die zu Schulenden)
  - Durch praktische Anwendung besser verankert



E-Mail Basics

E-Mail Primer



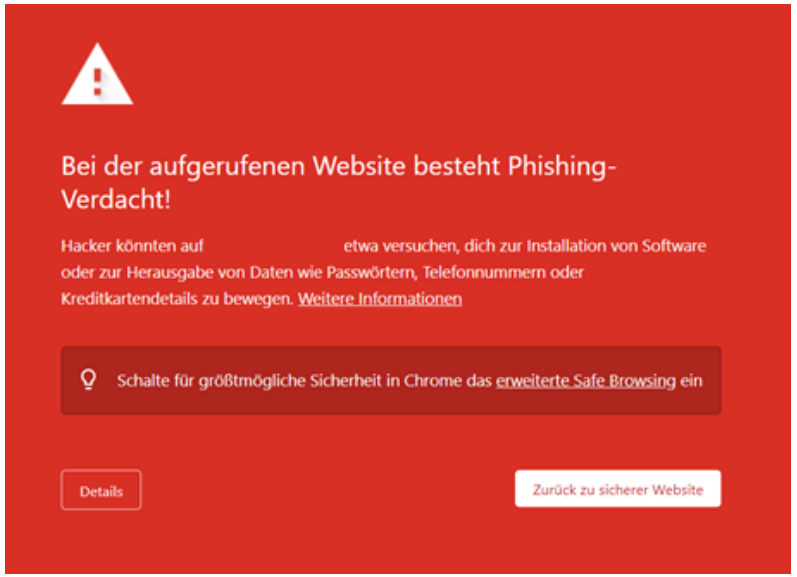
UA : User Agent (z.B. Outlook)
MTA: Mail Transfer Agent (z.B. Office 365)

E-Mail Spoofing/Phishing Schutz - Basis

- Sender Policy Framework (SPF)
  - Definition von validen MTAs für sendende Domänen
  - Empfänger MTA überprüft Eintrag
- DomainKeys Identified Mail (DKIM)
  - Digitale Signatur jeder E-Mail am sendenden MTA (asymetric Crypto)
- Domain-based Message Authentication, Reporting and Conformance (DMARC)
  - Baut auf SPF und DKIM auf
  - Definiert Empfehlungen wie der Empfänger MTA mit Mails umgeht

E-Mail Spoofing/Phishing Schutz - Advanced

- Web-Filtering
  - Unbekannte, oder neue Domänen können blockiert werden
- Multi-Factor Authentication
  - Schutz vor Diebstahl der Logindaten
- Black-Lists / Malware Checks
  - Schutz vor bekannten schadhaften Webseiten
- ...



How to phish

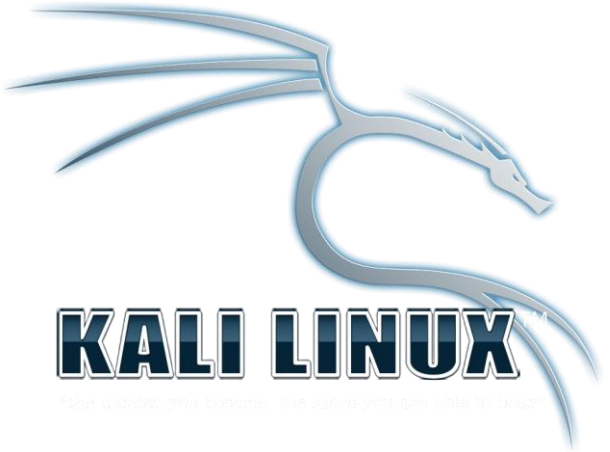
Was wird benötigt?

- MTA aka SMTP Server
- User Agent
- DNS Server
- Rückkanal (z.B. HTTP Server)

https://twitter.com/smtpcom https://www.lewisroberts.com/2016/05/28/using-azure-dns-dynamic-dns/ https://duckduckgo.com/i/388b8a3c.png

Unser Setup

- RPi 3
  - MTA (SMTP) – exim4
  - DNS Server - bind
  - Öffentliche IP
- Kali Linux PC
  - GoPhish
  - Apache2
- Verbindung von RPi und PC via SSH tunneling



https://www.raspberrypi.org/products/

Domain registration

GoDaddy

fh-joaneum.at

Weiter zum Warenkorb

Alle Domains verfügen über grundlegenden Datenschutz.

fh-joanneum.eu

Es gelten Einschränkungen.

~~€14,07~~ €6,60

für das erste Jahr bei einer 2-Jahres-Registrierung

In den Warenkorb

im ersten Jahr

- "Fh-joaneum" ist eindeutig.
- Mit grundlegendem Datenschutz

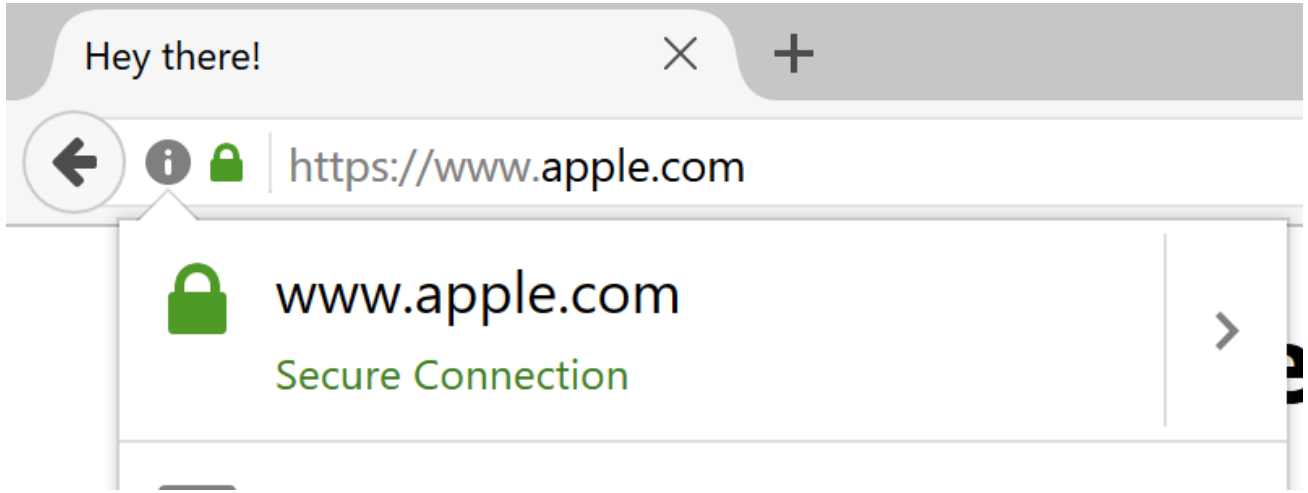
fh-joaneum.com Domain hinzufügen zum Preis von: €1,36

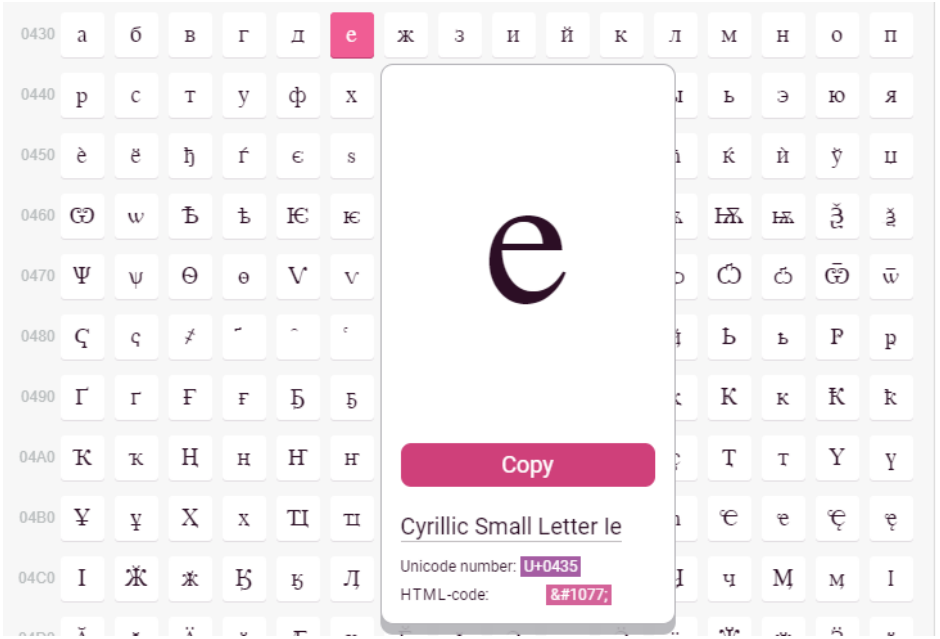
wenn du dich für mindestens 2 Jahre registrierst. Preis im ersten Jahr €1,36 Weitere Jahre €22,96

In den Warenkorb

UTF-8 Domains

- UTF-8 Zeichen in Domäne





https://www.xudongz.com/blog/2017/idn-phishing/ https://unicode-table.com/en/

Provider - DNS

- Alternative zu eigenem DNS
- Einfach zu bearbeiten

DNS-Verwaltung

aribus.at

Datensätze

Zuletzt aktualisiert: 17.10.19 15:25

Typ	Name	Wert	TTL
A	@	91.143.101.212	600 Sekunden
CNAME	www	@	1 Stunde
CNAME	_domainconnect	_domainconnect.gd.domaincontrol.com	1 Stunde
MX	@	mail.sectest.eu (Priorität: 1)	1 Stunde
NS	@	ns63.domaincontrol.com	1 Stunde
NS	@	ns64.domaincontrol.com	1 Stunde
SOA	@	Primärer Nameserver: ns63.domaincontrol.c...	1 Stunde
TXT	@	v=spf1 a ip4:91.143.101.212 ?all	1 Stunde
TXT	default._domainkey	"v=DKIM1; h=sha256; k=rsa; p=MIIBIjANBgk...	1 Stunde
TXT	_dmarc	"v=DMARC1; p=none;"	1 Stunde

MxToolBox – Check your DNS

spf:fh-joanneum.at Find Problems Solve Email Delivery Problems

```
v=spf1 ip4:91.229.57.22 ip4:91.229.57.250 ip4:91.229.57.251 ip4:91.118.154.85 include:spf.protection.outlook.com -all
```

Prefix	Type	Value	PrefixDesc	Description
v	version	spf1		The SPF record version
+	ip4	91.229.57.22	Pass	Match if IP is in the given range
+	ip4	91.229.57.250	Pass	Match if IP is in the given range
+	ip4	91.229.57.251	Pass	Match if IP is in the given range
+	ip4	91.118.154.85	Pass	Match if IP is in the given range
+	include	spf.protection.outlook.com	Pass	The specified domain is searched for an 'allow'.
-	all		Fail	Always matches. It goes at the end of your record.

https://mxtoolbox.com/spf.aspx

Gophish

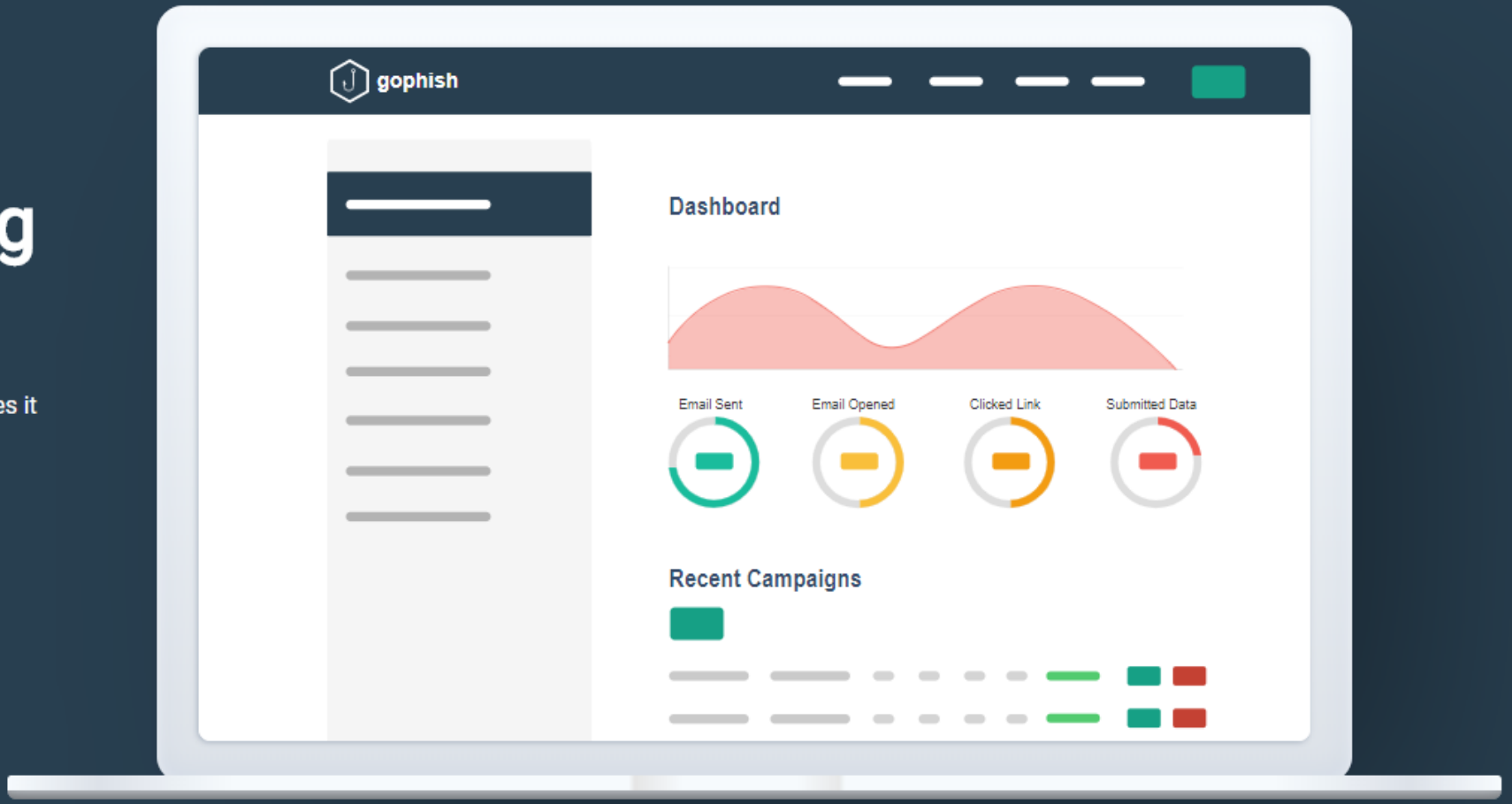
Documentation Support Blog Download

Open-Source Phishing Framework

Gophish is a powerful, open-source phishing framework that makes it easy to test your organization's exposure to phishing.

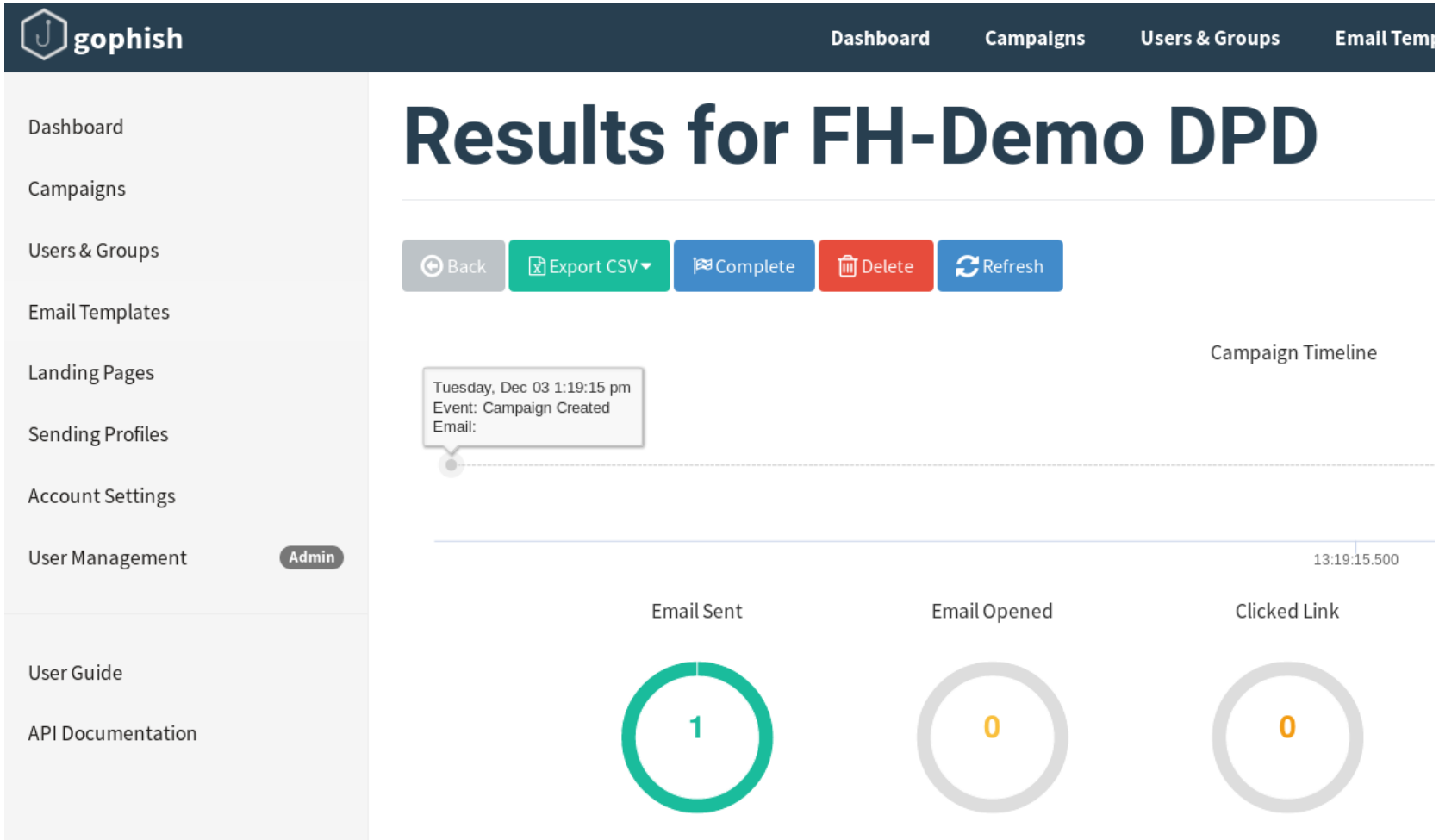
For free.

Download Learn More



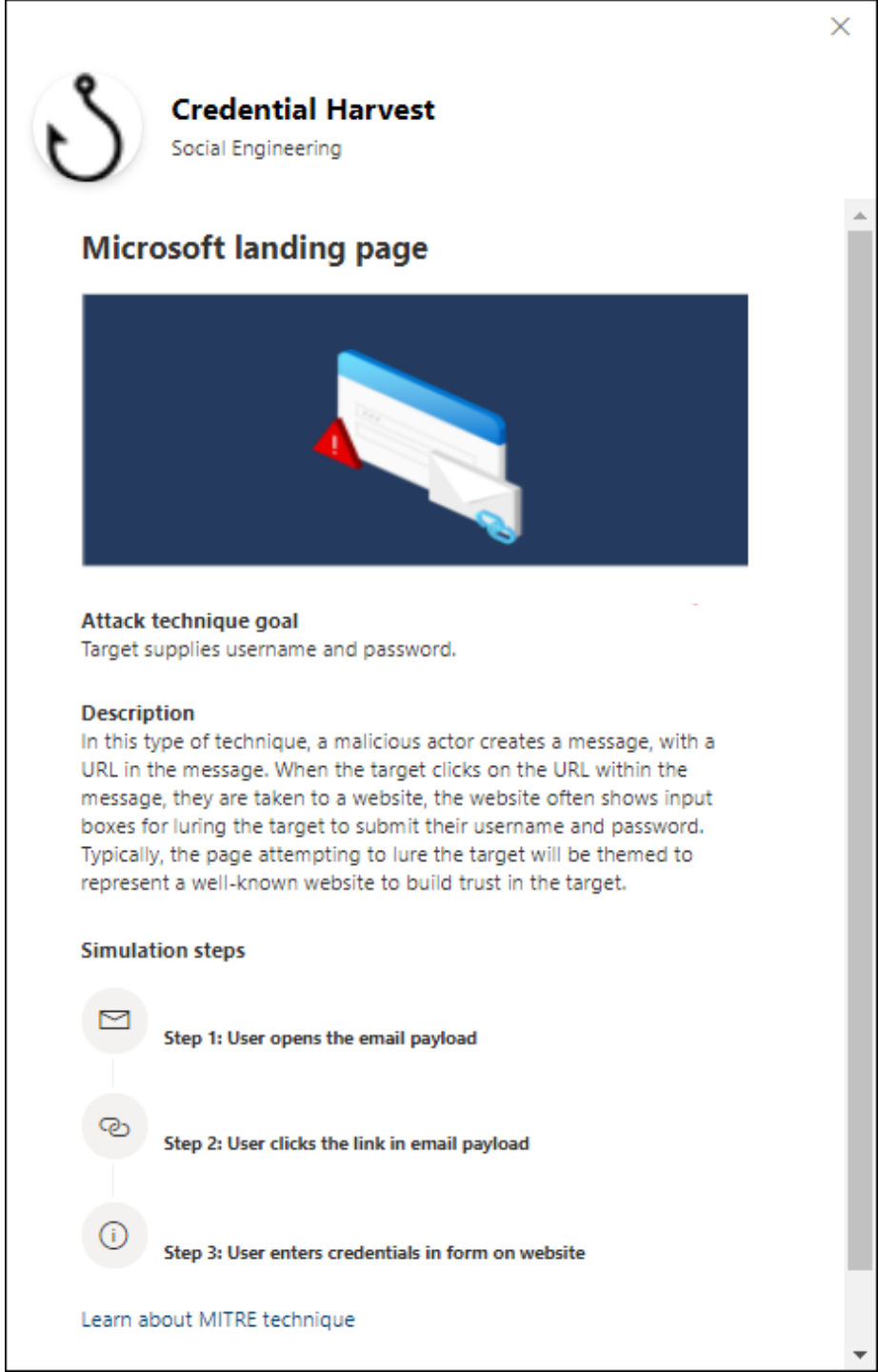
https://getgophish.com/

Demo Gophish



M365 – Attack Simulation

- Verfügbar in
  - Microsoft 365 E5
  - or Microsoft Defender for Office 365 Plan 2
- Einfach zu verwenden / auszuwerten
- Oft bereits im Paket enthalten



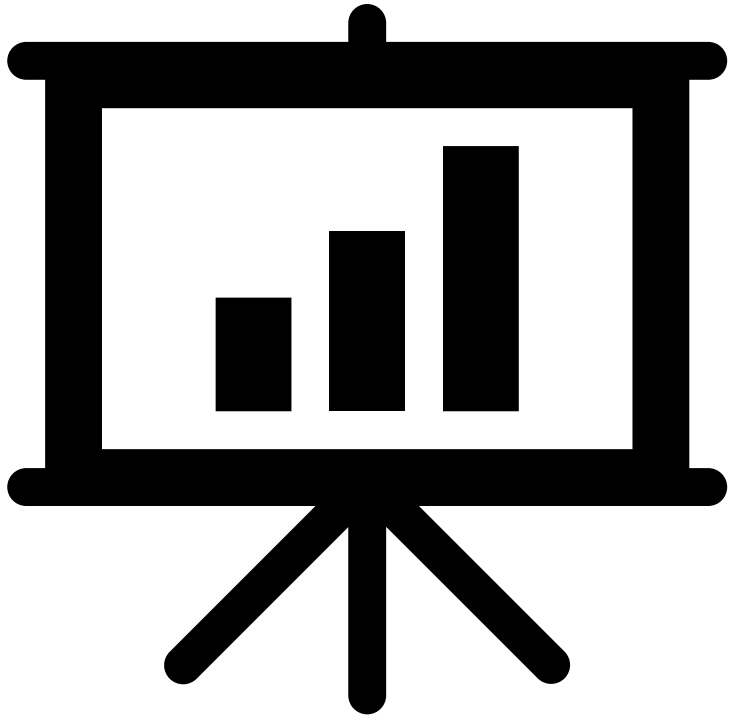
Ergebnisse - Allgemein

- „Schlechte“ – Phishing Mail

~5-30%

- Personalisierte Phishing Mail

~10-60%



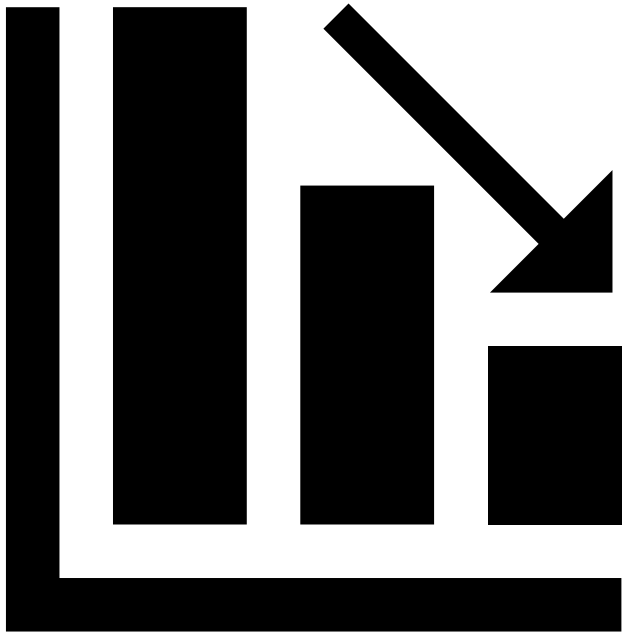
Ergebnisse – Erneute Überprüfung

- Personalisierte Phishing Mail – Welle1

~44%

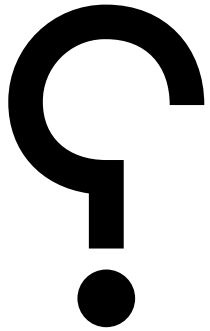
- Nach 2 Monaten Welle 2

~27%



Probleme

- Große Kampagnen
  - Sende / Empfangs Limits
- “intelligente” Spam Filter



- UTF-8 Unterstützung
- Rückkanal über ID
  - Alternativer Webserver
    - Erstellen von Error Requests
  - DNS Abfragen
  - …

Fragen?