

Digital Innovation Hub

Aktives Phishing zur Mitarbeitersensibilisierung
Erfahrungen/Tools/Einschränkungen

Fruhmann



Über mich

🏠 **Martin Fruhmann**

🏠 **Studium IT & Mobile Security @ FH JOANNEUM**

🏠 **Lehrender @ FH JOANNEUM**

-)) Netzwerk Technologien
-)) Netzwerk Security
-)) IT-Security
-)) Penetration Testing
-)) Phishing



Phishing Basics

NETFLIX

We're sorry to say goodbye

Hello,


iTunes let us know that you asked to cancel your membership. We've cancelled your membership effective Tuesday, March 21st, 2017.

Obviously we'd love to have you back. If you change your mind, simply [restart your membership](#) to enjoy all the best TV shows & movies without interruption.

RESTART MEMBERSHIP

We're here to help if you need it. Visit the [Help Center](#) for more info or [contact us](#).

-Your friends at Netflix



Hi <customer>,
This is a follow-up regarding your package delivery:

- Tracking Number: [0p2uYg5R1ho](#)

The package contained in the above-mentioned shipment was not accepted at the destination address. Please contact your local UPS office and provide the printed delivery sticker, included in this email.

Please note that in case of a failure to contact your local UPS office within 21 days the parcel will be returned to sender.

Thanks so much for shipping with UPS.

PayPal

We need your help

Your account has been suspended, as an error was detected in your informations. The reason for the error is not certain, but for security reasons, we have suspended your account temporarily

We need you to update your informations for further use of your PayPal account.

Update your information

You are currently made disabled of :

- Adding a payment method
- Adding a billing address
- Sending payment
- Accepting payment

To: ACCOUNTING DEPARTMENT
Cc: TomHeald@strategictax.com
Subject: W2's for All Employees
From: Tom Smith
Signature: None

Please send our W2 Tax Documents for all employees to Tom Heald at Strategic Tax Consultants. I have cc'd him here.

We need these documents for a review ordered by the Board of Directors.

Please send immediately as we are under a time crunch.

Thanks,

Tom Smith
CEO
BetterSystems Inc

amazon

Refund Notification

Due to a sytem error you were double charged for your last order, A refund process was initiated but could not be completed due to errors in your billing information

REF CODE:2550CGE

You are required to provide us a valid billing address

[Click Here to Update Your Address](#)

After your information has been validated you should get your refund within 3 business days

We hope to see you again soon.
[Amazon.com](#)
Email ID: [redacted]

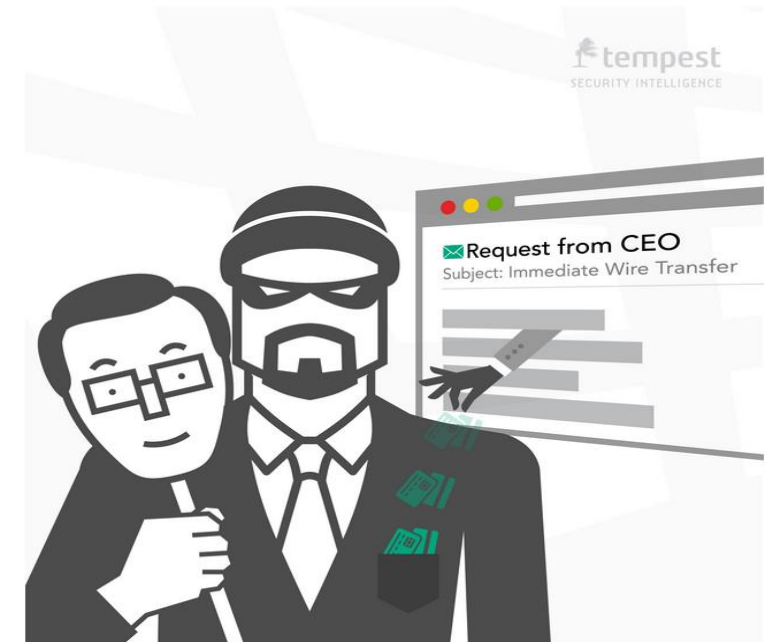
1 to this address. For immediate answers to your questions, visit our
1 N. First St., San Jose, CA 95131.

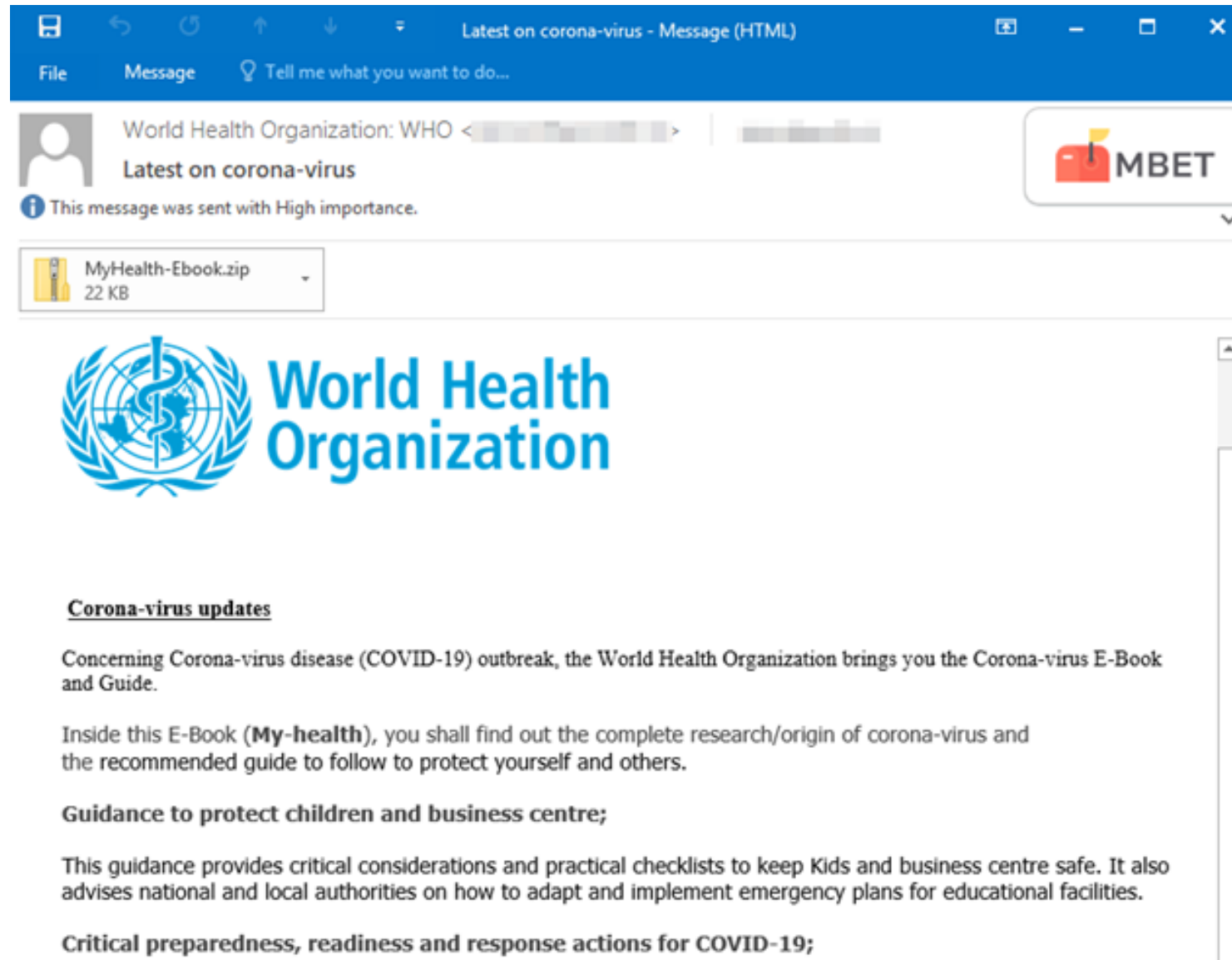
Ziele von Angreifern

- ☐ 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
 -)) ...





Latest on corona-virus - Message (HTML)


File Message Tell me what you want to do...

World Health Organization: WHO <[redacted]> | [redacted]

Latest on corona-virus

This message was sent with High importance.

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.

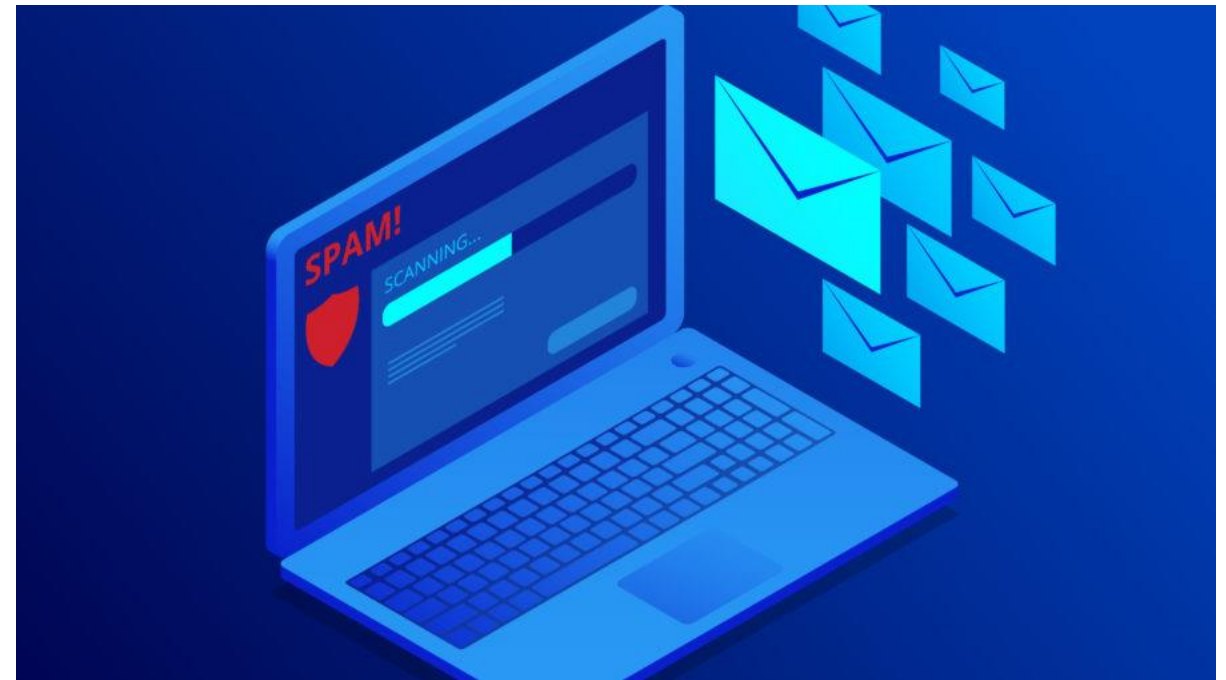
Guidance to protect children and business centre;

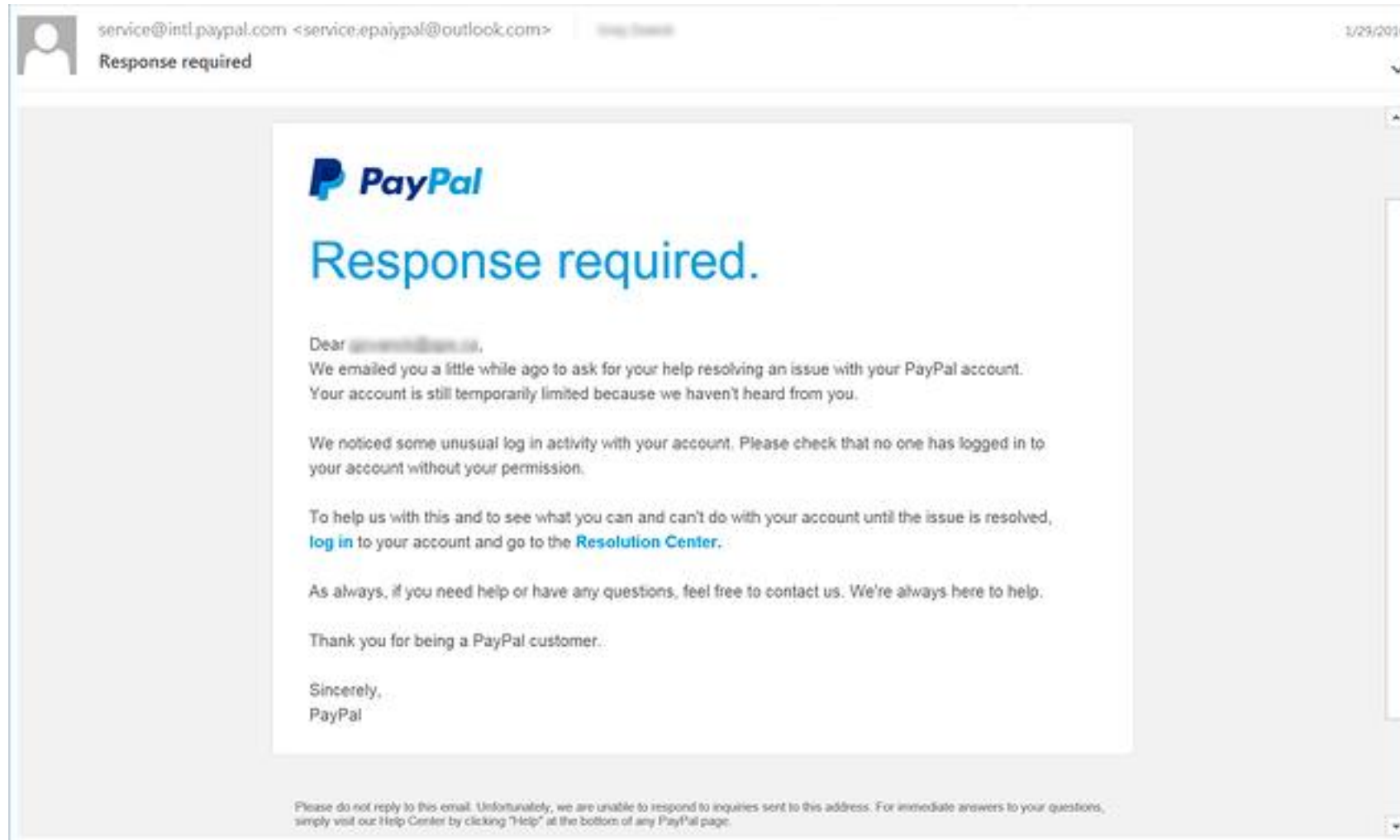
This guidance provides critical considerations and practical checklists to keep Kids and business centre safe. It also advises national and local authorities on how to adapt and implement emergency plans for educational facilities.

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





service@intl.paypal.com <service:epaiypal@outlook.com> 1/29/2016

Response required

 **Response required.**

Dear [redacted],

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.

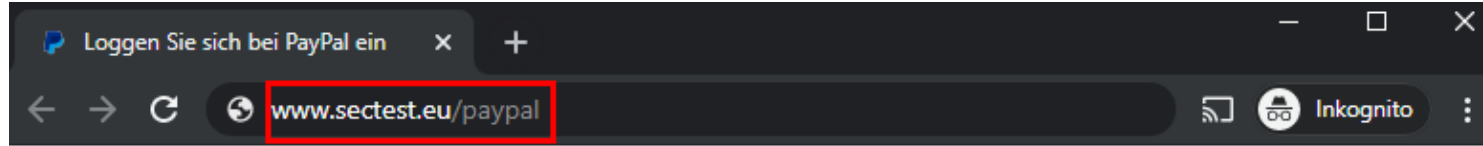
To help us with this and to see what you can and can't do with your account until the issue is resolved, [log in](#) to your account and go to the [Resolution Center](#).

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.

A screenshot of the PayPal login page. At the top center is the PayPal logo. Below it is a text input field containing the placeholder text 'E-Mail-Adresse oder Handynummer'. Underneath the input field is a blue button with the text 'Weiter'. Below the blue button is the word 'oder' centered between two horizontal lines. At the bottom of the form is a light gray button with the text 'Neu anmelden'.

Von: direkt@sparkasse.de — Absender trägt einen bekannten Namen

An: Ihre Sparkasse — Verteiler-Liste als Empfänger

Cc: undisclosed recipients;

Betreff: Online Banking Zugang - Dringend! — Handlungsaufforderung

ZIP

Sehr geehrter Kunde, — Unpersönliche Anrede — Komprimierte Datei im Anhang

Bitte beachten Sie, dass Ihr Online-Banking Zugang bald abläuft. Ihr Nutzerkonto wurde temporär gesperrt. Über den folgenden Link, sie können die Sperre deaktivieren:

Rechtschreibung, Grammatik, seltsame Sonderzeichen

<http://goonswiss.t15.org> — Der Link verweist auf eine unbekannte URL

Hier Klicken >>

Nach Abschluss der Bestätigung wird Ihr Nutzerkonto automatisch freigeschaltet. Kommen Sie dieser E-Mail innerhalb 14 Tagen nicht nach, ist die Freischaltung nur über den Postweg möglich. Dabei wird eine Bearbeitungsgebühr in Höhe von 19,95€ fällig, welche wir anschließend von Ihrem Konto abbuchen werden.

Respektvoll, Ihre Sparkasse — Druckaufbau und weitere Handlungsaufforderungen — Untypische Redewendungen

Phishing – Bösertige Links

The image illustrates a phishing attack scenario. On the left, a Windows 10 desktop environment is shown with the word "Victim" in large, semi-transparent letters. On the right, a terminal window shows a Metasploit (msf6) session with a job list for a chrome_jscreate_sideeffect exploit. The word "Attacker" is written in large, red, semi-transparent letters on the right side of the terminal window.

```
root@darth: -  
msf6 exploit(multi/browser/chrome_jscreate_sideeffect) > jobs -l  
Jobs  
----  
Id  Name                               Payload                               Payload opts  
--  ---                               -  
0   Exploit: multi/browser/chrome_js   windows/x64/meterpreter/reve        tcp://116.203.129.59:8080  
    create_sideeffect                rse_tcp  
msf6 exploit(multi/browser/chrome_jscreate_sideeffect) > _
```


Mögliche Awareness Maßnahmen

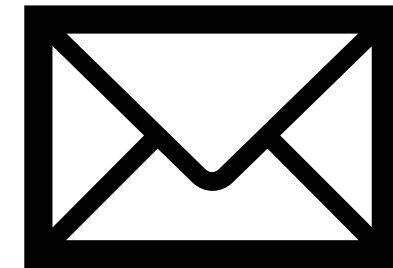
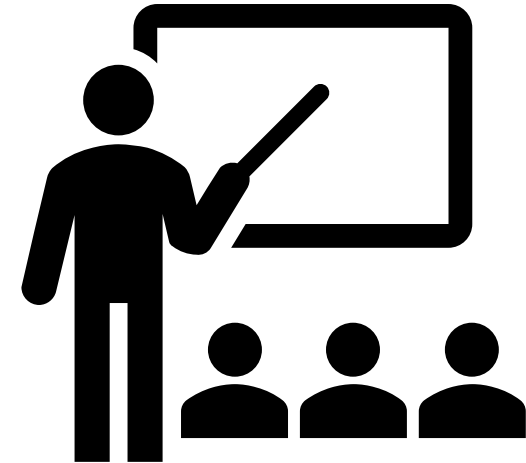
☐ Awareness Training Vortrag

-)) Teils schwierige Zielgruppen
-)) Zeitintensiv
-)) Sehr kurze Halbwertszeit im Bezug auf Wissen

vs.

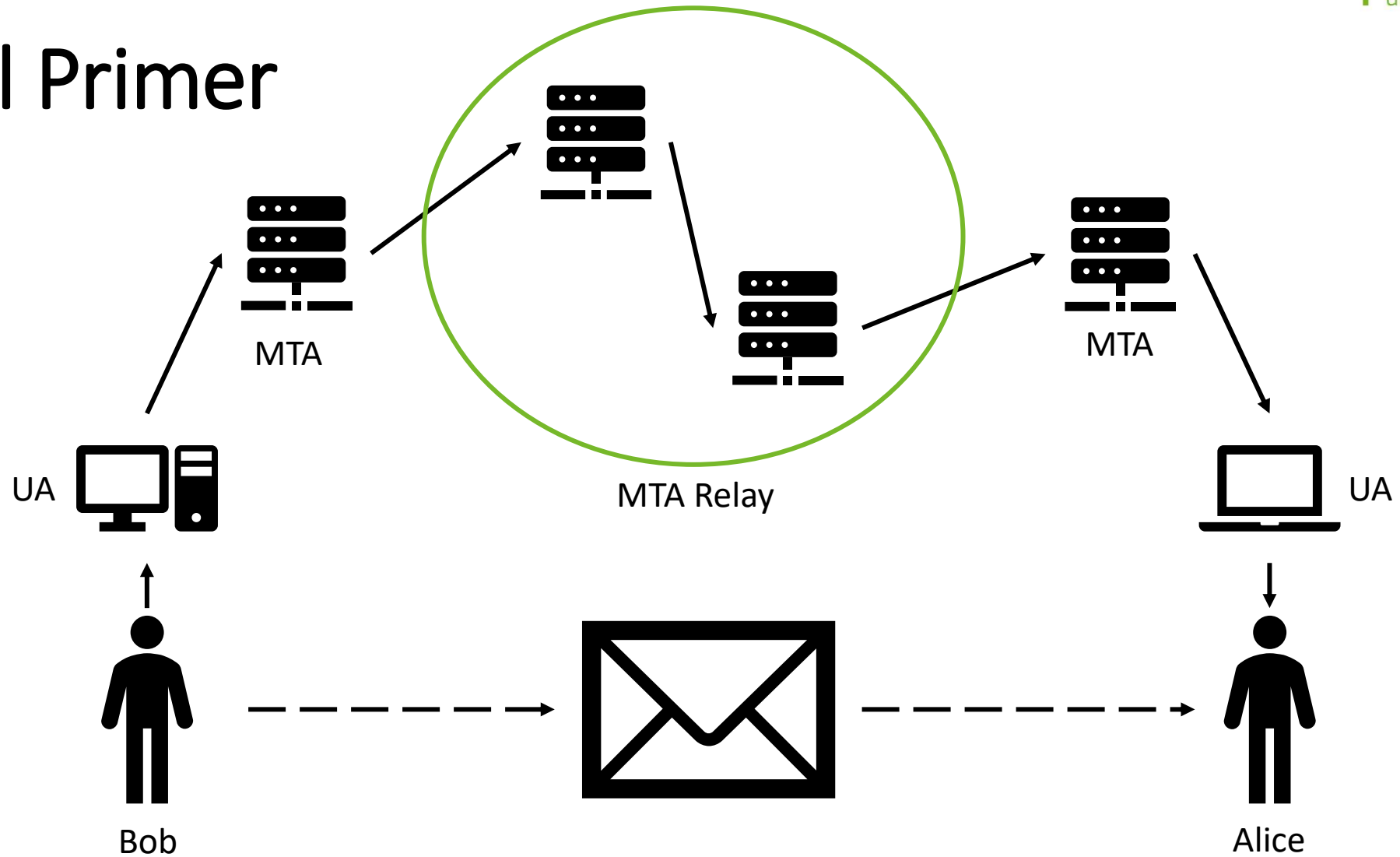
☐ Aktives Phishing

-)) 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 (asymmetric 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

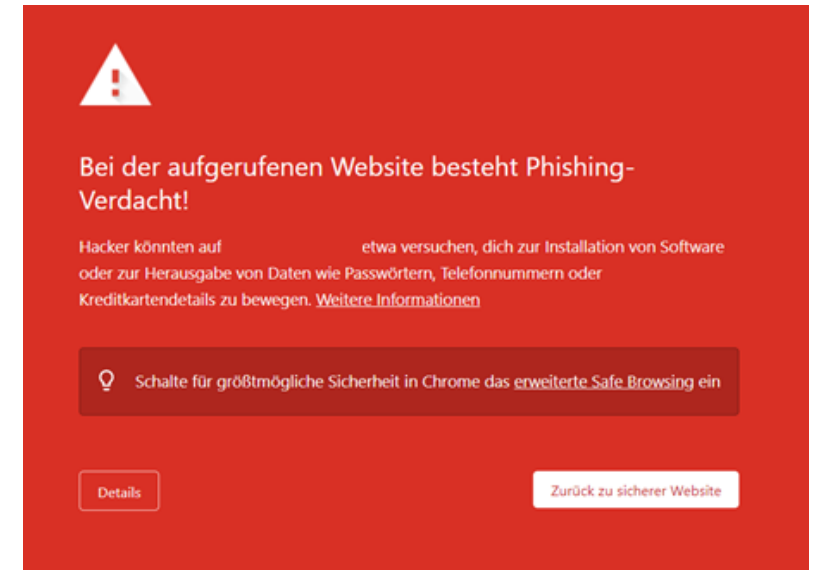
Multi-Factor Authentication

») 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)



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



Domain registration

[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

ZEICHEN:

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

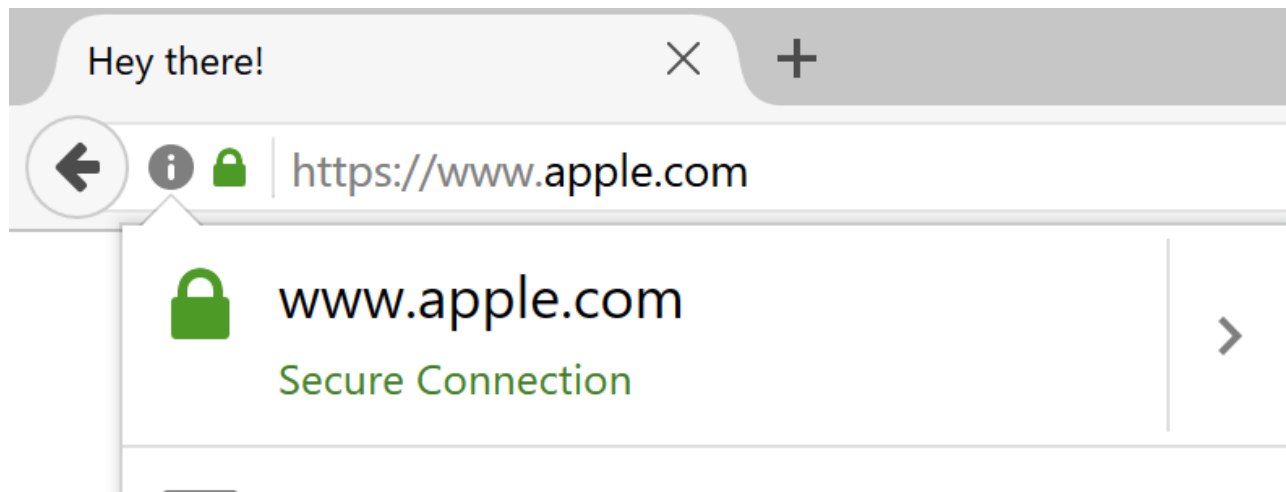
fh-joaneum.com Domain hinzufügen zum Preis von: **€1,36**

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



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=MIBljANBgk...	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.



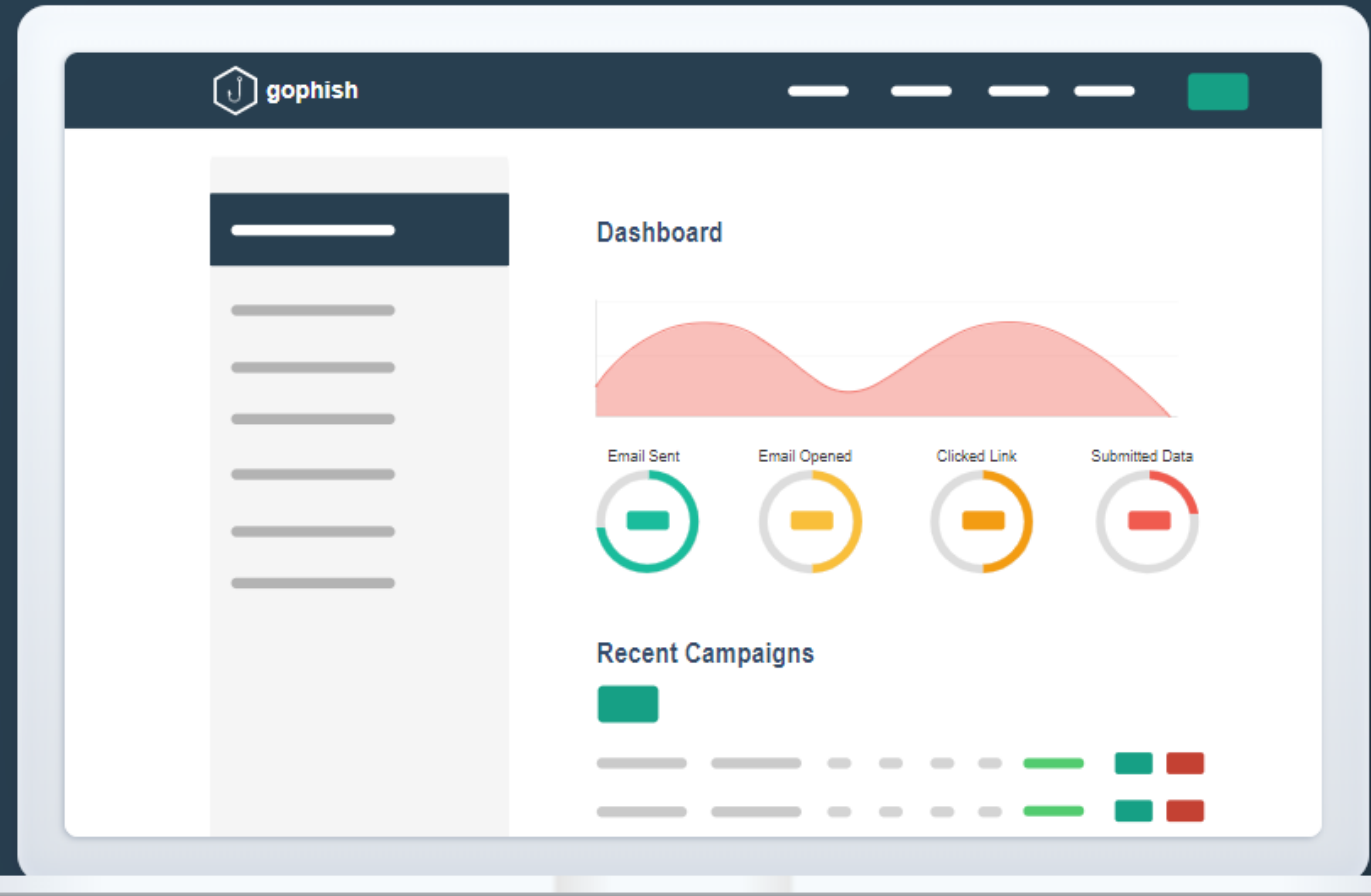
Open-Source Phishing Framework

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



Demo Gophish

The screenshot displays the Gophish web interface. At the top, a dark blue navigation bar contains the Gophish logo and menu items: Dashboard, Campaigns, Users & Groups, and Email Templates. A left sidebar lists various management options: Dashboard, Campaigns, Users & Groups, Email Templates, Landing Pages, Sending Profiles, Account Settings, User Management (with an 'Admin' button), User Guide, and API Documentation. The main content area is titled 'Results for FH-Demo DPD' and features a toolbar with buttons for Back, Export CSV, Complete, Delete, and Refresh. Below this is a 'Campaign Timeline' section with a single event: 'Tuesday, Dec 03 1:19:15 pm Event: Campaign Created Email:'. At the bottom, three circular progress indicators show the following statistics: Email Sent (1), Email Opened (0), and Clicked Link (0). A timestamp '13:19:15.500' is visible on the right side of the timeline area.

Metric	Value
Email Sent	1
Email Opened	0
Clicked Link	0

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



Credential Harvest
Social Engineering

Microsoft landing page






Attack technique goal

Target supplies username and password.

Description

In this type of technique, a malicious actor creates a message, with a URL in the message. When the target clicks on the URL within the message, they are taken to a website, the website often shows input boxes for luring the target to submit their username and password. Typically, the page attempting to lure the target will be themed to represent a well-known website to build trust in the target.

Simulation steps

-  Step 1: User opens the email payload
-  Step 2: User clicks the link in email payload
-  Step 3: User enters credentials in form on website

[Learn about MITRE technique](#)

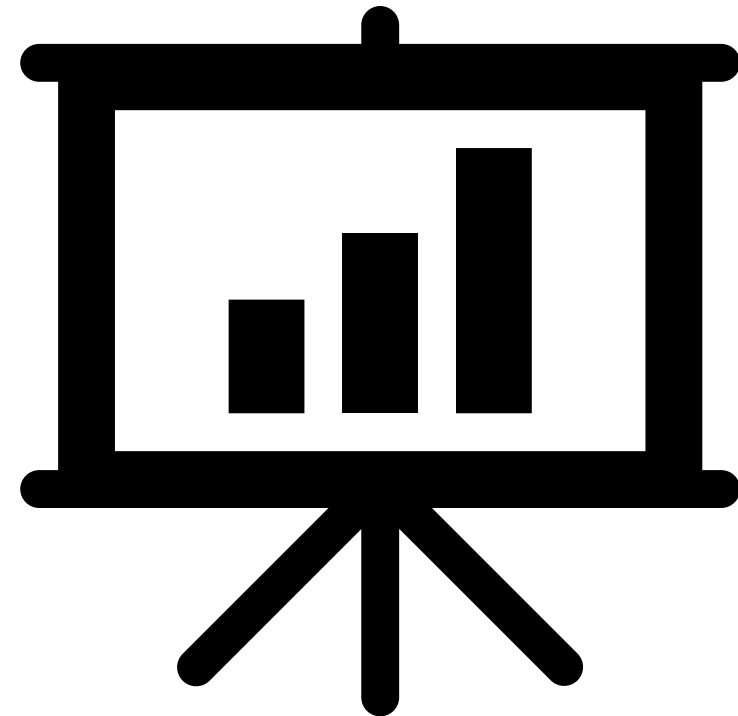
Ergebnisse - Allgemein

☐ „Schlechte“ – Phishing Mail

~5-30%

☐ Personalisierte Phishing Mail

~10-60%



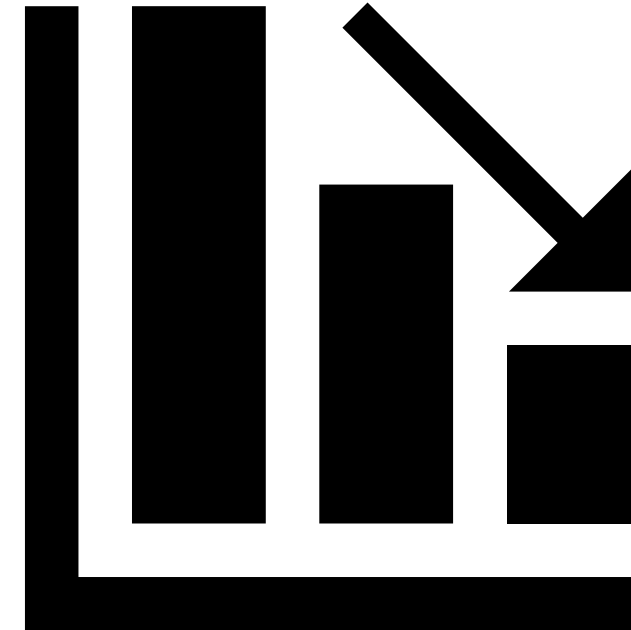
Ergebnisse – Erneute Überprüfung

Personalisierte Phishing Mail – Welle1

~44%

Nach 2 Monaten Welle 2

~27%



Probleme

☐ Große Kampagnen

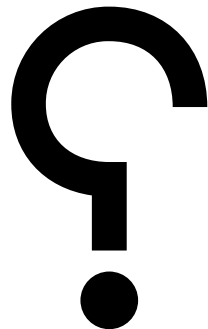
-)) Sende / Empfangs Limits

☐ “intelligente” Spam Filter

☐ UTF-8 Unterstützung

☐ Rückkanal über ID

-)) Alternativer Webserver
 -)) Erstellen von Error Requests
-)) DNS Abfragen
-)) ...



Fragen?