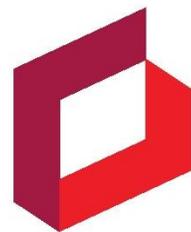




**HORNETSECURITY**



**IT-Systemhaus**  
Ruhrgebiet®

Wir starten in wenigen Augenblicken

# Agenda

- Wie sensibilisiere ich mein Team vor Cyber-Gefahren & Phishing-Mails?



- 45 Minuten

- Die aktuelle Bedrohungslage
- Sicherheitsfeatures von Hornetsecurity
- Sind die Mitarbeitenden ein Sicherheitsrisiko?
- Wie kann Hornetsecurity unterstützen?

- Marco Block

- Partner Account Manager
- Region: PLZ 4 / 58 / 59



HORNETSECURITY

# Die aktuelle (Bedrohungs-) Lage

ntv

Dienstag, 16. Januar 2024

RESSORTS

SPORT

BÖRSE

WETTER

VIDEO

AUDIO

TV PROGRAMM

LIVE-TV

WIRTSCHAFT



Globales Risiken-Barometer

## Hacker machen Managern die größte Angst

Weltweit haben Unternehmen wachsende Sorge vor Cyberkriminellen. Das Risiken-Barometer der Allianz-Versicherung zeigt für Deutschland allerdings interessante Besonderheiten: Auf Platz drei der Schrecken kommt hierzulande schon die Bürokratie.



HORNETSECURITY

IT-Systemhaus  
Ruhrgebiet\*

# Die aktuelle (Bedrohungs-) Lage

**ATU**

**Eberspächer**

Die Eberspächer Gruppe wurde Ziel eines organisierten Cyber-Angriffs. Die IT-Infrastruktur ist beeinträchtigt. Zum Schutz unserer Kunden, Mitarbeiter und Partner wurden unverzüglich die notwendigen Schritte ergriffen, um dem Angriff mit gezielten Maßnahmen entgegen zu wirken.

Unser Team arbeitet gemeinsam mit externen Cyber-Security-Spezialisten mit Hochdruck daran, die Gefährdung zu beseitigen und den Normalbetrieb wiederherzustellen. Die zuständigen Ermittlungsbehörden sind eingeschaltet.

organized cyberattack. The IT infrastructure is affected. To protect our the necessary steps were taken immediately to counter the attack with

[Unternehmen](#) [Aktuelles](#) [Karriere](#) [Kontakt](#) [Werksvertre](#)

Sehr geehrte Geschäftspartner,

Opfer eines kriminellen Cyberangriffes geworden. Unsere IT-Systeme sind standortübergreifend betroffen.

**ST+** Untersuchung eingeleitet

[Teilen](#) [Drucken](#) [Merken](#)

## Cyberattacke trifft Handwerkskammer Heilbronn-Franken – Alternative Webseite eingerichtet

Ein IT-Dienstleister der Handwerkskammern wurde Opfer einer Malware-Attacke – betroffen ist auch die Heilbronner Kammer.



von [Jürgen Paul](#)

15. Januar 2024, 10:46 Uhr | Update: 15. Januar 2024, 12:30 Uhr | ⌚ 1 Min

Stadt Bergisch Gladbach  
**Aufgrund eines Hackerangriffs auf unser Rechenzentrum (SIT) bleibt das Bürgerbüro vorerst geschlossen.**  
In dringenden Fällen melden Sie sich unter: 02202-142322

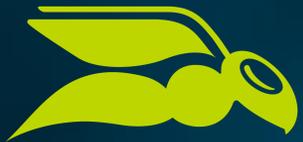
  
**HORNETSECURITY**

 **IT-Systemhaus Ruhrgebiet®**

Kann es auch SIE treffen?  
Ja  
Nein

# HORNETSECURITY'S SECURITY LAB

- Team aus internationalen Entwicklern und IT Security Spezialisten
- 24/7 Überwachung der Erkennungsmechanismen
- Exklusive Zahlen & Fakten:
  - 👉 14,5 Mrd Mails in 2023 über unsere Server
  - 👉 33,120 neue E-Mail basierte Bedrohungen an einem durchschnittlichen Tag beobachtet
  - 👉 12,996 Ransomware-Angriffe pro Stunde



HORNETSECURITY

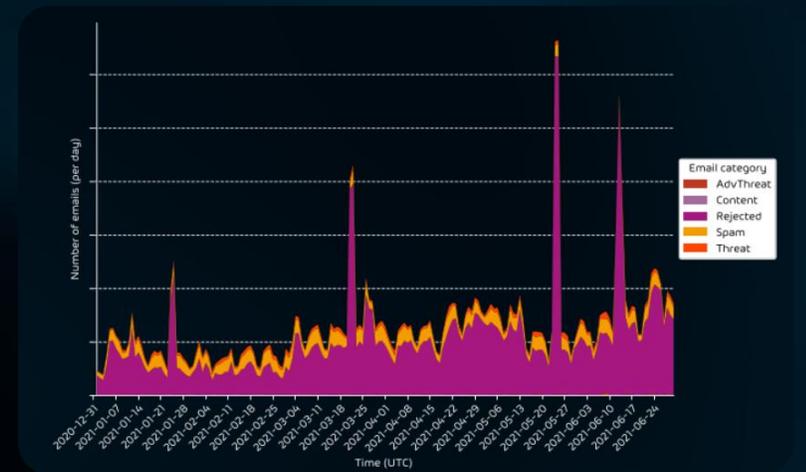
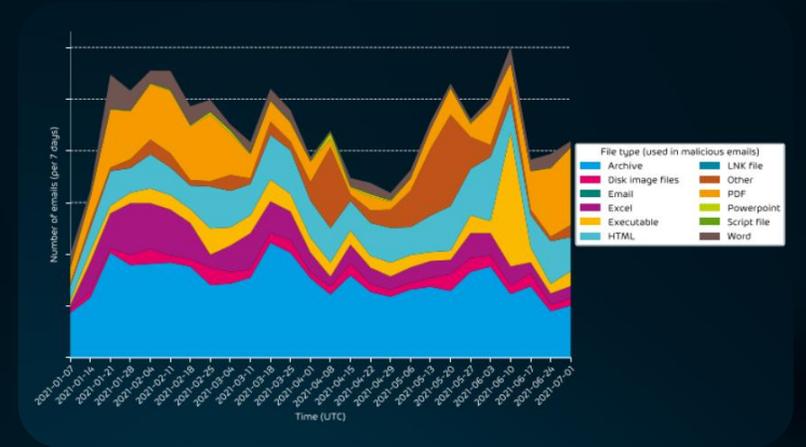


Abb. 1 & 2: Grafiken zu unterschiedlichen E-Mail Bedrohungen aus dem Hornetsecurity Security Lab

# Cyber Security Report 2023



## ANALYSE VON ÜBER 45 MILLIARDEN E-MAILS



Fig. 1: Klassifizierung der durch Hornetsecurity gescannten E-Mails



**96.4%**  
SPAM oder ABGELEHNT

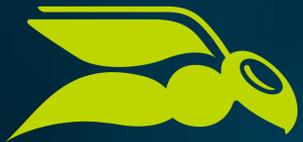


**3.6%**  
BÖSARTIG

Fig. 2: Klassifizierung von unerwünschten E-Mails

✉	26.1   DHL
💡	18.5   OTHER
📺	7.7   AMAZON
📶	5.7   POSTBANK
📧	2.5   STRATO
in	2.4   LINKEDIN
📄	2.4   MICROSOFT
🛒	2.3   FEDEX
N	2.2   NETFLIX
📱	2.1   1&1

Fig. 13: Top 10 der imitierten Marken im Jahr 2023



HORNETSECURITY

# Cyber Security Report 2023

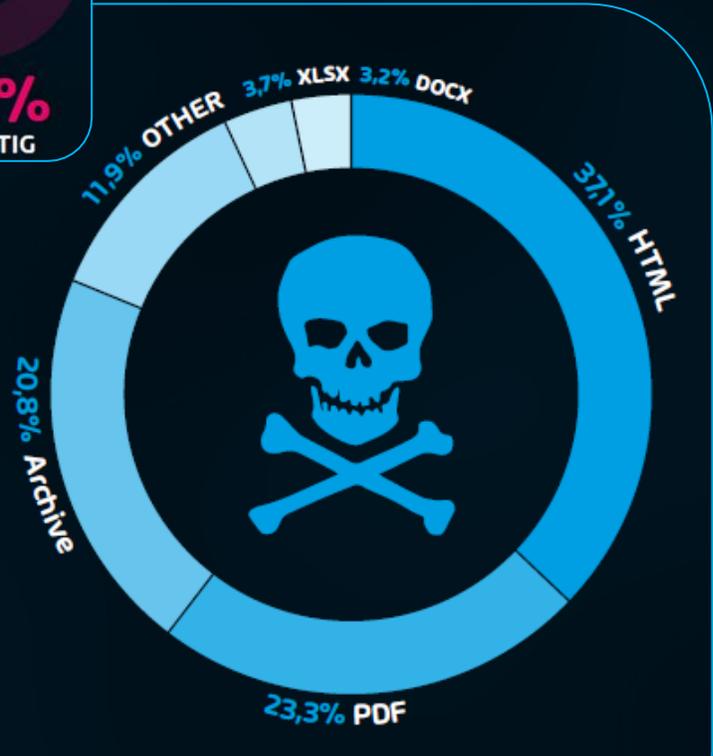


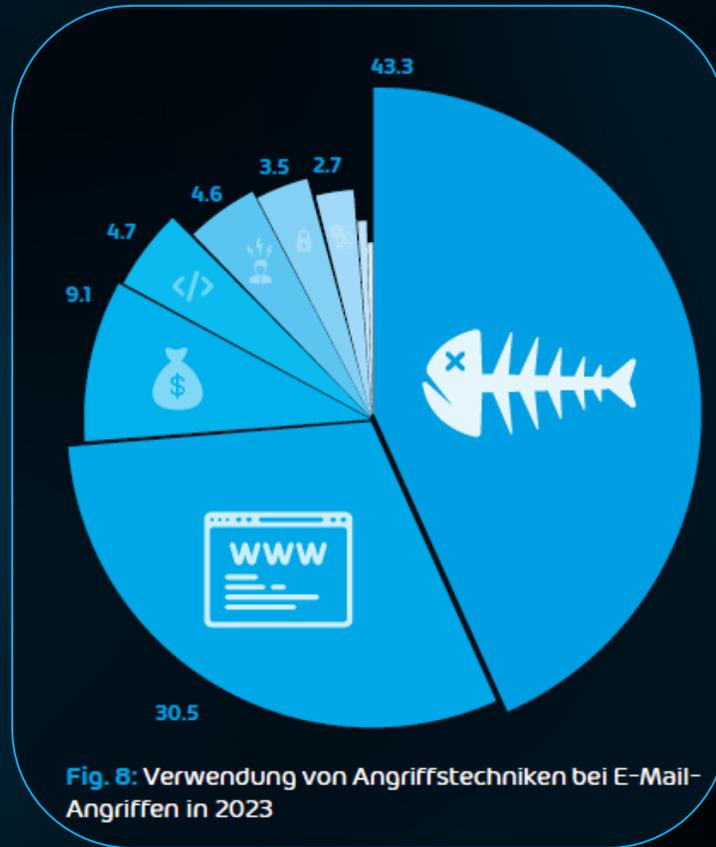
Fig. 4: Am häufigsten verwendete Dateitypen in bössartigen E-Mails



2022



# Cyber Security Report 2023



HORNETSECURITY

# WIE ALLES BEGANN - UNSERE FIRMENGESCHICHTE



Ready for  
**Take Off**

2007



Presence in more  
than **10 countries**  
with over **200**  
**sales partners**

2008

Beginning of  
**internationalization**

2010



Over **25,000**  
**companies**  
as customers

2013



**Market leader  
in Germany;**  
Awarded with  
Deloitte Technology  
**Fast 50 Award**

2014



antispameurope  
becomes  
**Hornetsecurity**

2015



Over  
**550 resellers**  
worldwide

2016



10 years of  
Hornetsecurity;  
**Foundation of  
US subsidiary**

2017



Acquisition of  
AVIRA Spamfilter  
division; **Market  
leader in German-  
speaking region**

2018



Partnership with  
Swisscom;  
**Acquisition of  
Spamina**

2019



**Acquisition of  
EveryCloud**

2020



Acquisition of  
**ALTARO;**  
Acquisition of  
**ZEROSPAM**

2021



**Acquisition of  
IT-Seal**

2022

# ERFOLG made in Germany (in Zahlen)



HORNETSECURITY

# 365 TOTAL PROTECTION PLAN 1

## BUSINESS



SPAM &  
MALWARE  
PROTECTION



EMAIL  
ENCRYPTION



EMAIL  
SIGNATURES  
& DISCLAIMERS

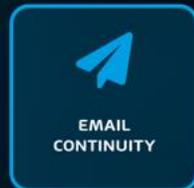
- Schnelles und einfaches Onboarding
- Nahtlose Integration in Microsoft 365
- Erweiterte Microsoft 365-Sicherheit
  - ◉ Spam and Malware Protection
  - ◉ Email Encryption
  - ◉ Email Signatures & Disclaimers



HORNETSECURITY

# 365 TOTAL PROTECTION PLAN 2

## ENTERPRISE



- ▶ Premium next-level Security für Microsoft 365
  - ▶ 365 Total Protection Business Features +
  - ▶ Advanced Threat Protection
  - ▶ Email Archiving
  - ▶ Email Continuity
    - ▶ Erhalten/Senden Sie auch noch Mails wenn der 365 Server down ist



HORNETSECURITY

# 365 TOTAL PROTECTION PLAN 3

## BACKUP



BACKUP  
& RECOVERY OF  
MAILBOXES  
& TEAMS

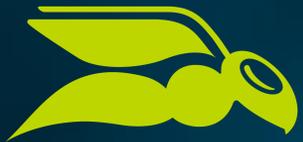


BACKUP  
& RECOVERY OF  
ONEDRIVE  
& SHAREPOINT



BACKUP  
& RECOVERY OF  
ENDPOINTS

- ▶ Vollumfängliche E-Mail-Security und Backup für M365
  - ▶ 365 Total Protection Enterprise Features +
  - ▶ Backup & Recovery von
    - ▶ Microsoft 365 Postfächern
    - ▶ Teams Chats
    - ▶ SharePoint Dokument Bibliotheken
    - ▶ Windows-basierte Endpoints
  - ▶ Separat erhältlich: Funktionen für
    - ▶ VMware / HyperV

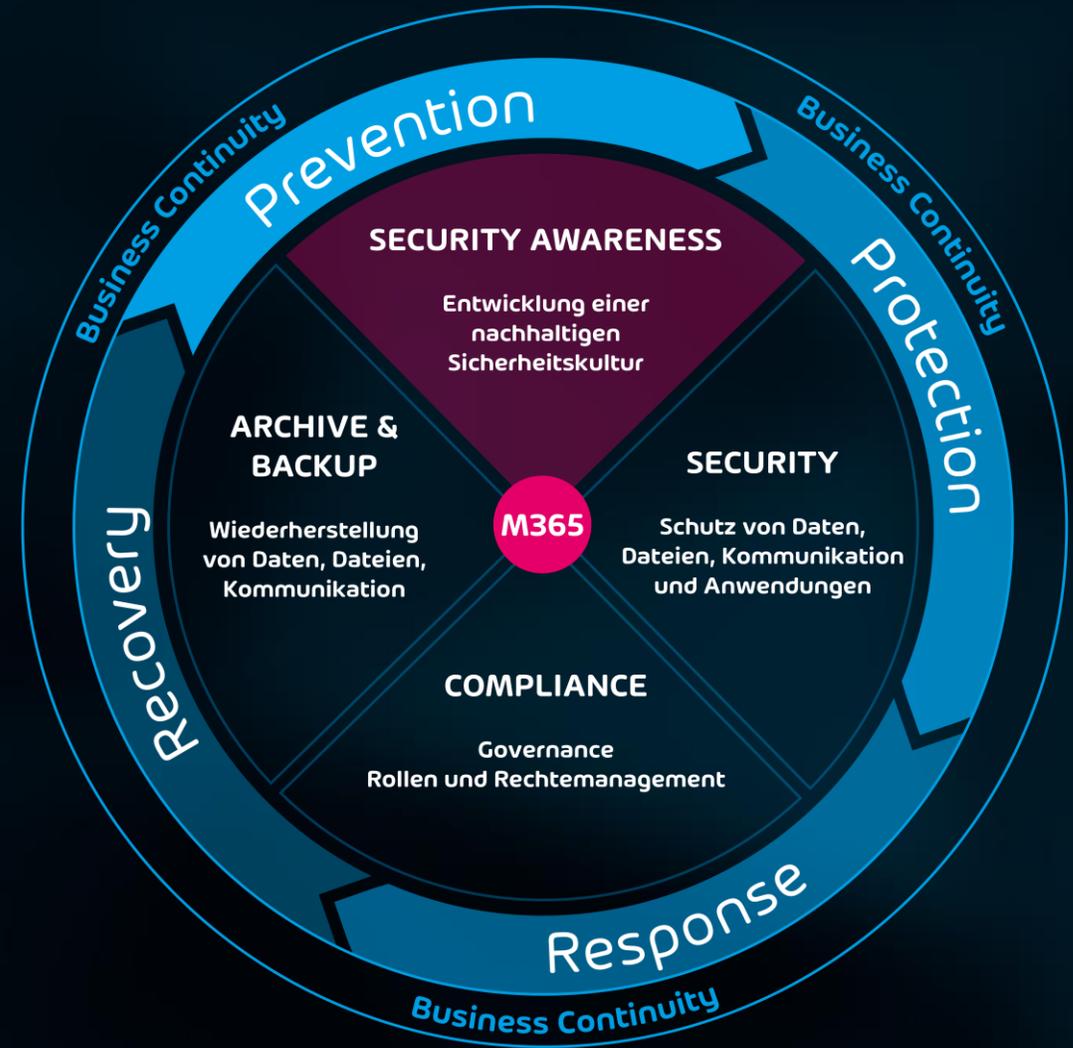


HORNETSECURITY

# SERVICE-ÜBERSICHT – DAS IST NEU!



**SECURITY  
AWARENESS  
SERVICE**



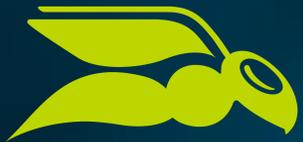
HORNETSECURITY

# 365 TOTAL PROTECTION PLAN 4

## COMPLIANCE & AWARENESS



- ▶ AI Recipient Validation.
  - ▶ Schützt vor fehlgeleiteten Emails, insbesondere im Postausgang
- ▶ Security Awareness Service
  - ▶ der vollautomatisch läuft und kontinuierlich das Sicherheitsverhalten der Mitarbeiter misst..
- ▶ 365 Permission Manager
  - ▶ Berechtigungen und Auditing, Management, Durchsetzung von Compliance-Richtlinien und Überwachung von Verstößen.



HORNETSECURITY

# EINE FEHLENDE SICHERHEITSKULTUR FÜHRT ZU IMMENSEN SCHÄDEN



*„Ich werde sowieso nicht angegriffen.“*  
Maria (28) — HR Manager

*„Unsere IT kümmert sich bereits darum.“*

Roland (41) — Controller



*„Ich habe wichtigere Dinge zu tun, als mich um die IT-Sicherheit zu kümmern.“*

Gabi (54) — Head of Sales



Die Arbeit von zu Hause aus wird sich weiter durchsetzen

95% aller Cybersicherheitsvorfälle sind auf menschliches Fehlverhalten zurückzuführen.

Quelle: World Economic Forum - The Global Risks Report 2022]



IT-Security: Der Mensch ist Risikofaktor Nr. 1

**ALLE Mitarbeitenden müssen das gleiche Verständnis und Wissen haben!**



HORNETSECURITY

# VORAUSSETZUNGEN FÜR EINE NACHHALTIGE SICHERHEITSKULTUR



HORNETSECURITY

## MINDSET

Motivation und offene Kommunikation

- Verständnis für Bedrohungslage
- Eigenverantwortung betonen



Kommunikationshilfen für alle Stakeholder

## SKILLSET

Fähigkeiten und Wissen aneignen

- Phishing-Simulation
- E-Learning
- Kurzvideos



Awareness-Materialien

## TOOLSET

Aktiv ins Geschehen eingreifen

- Live-Dashboard
- Sicherheitsmeldekettchen



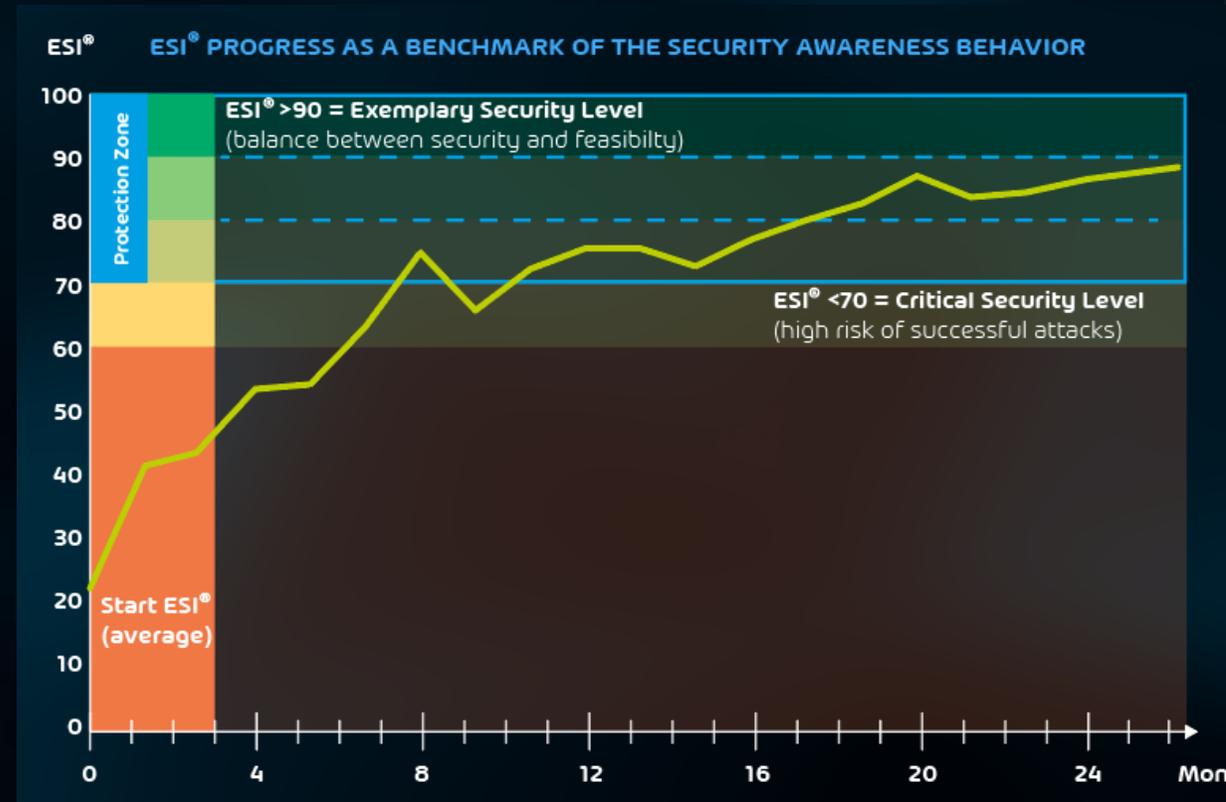
Reporter-Button  
Outlook Add-In

# ESI® - EMPLOYEE SECURITY INDEX

- ESI® - Ein wissenschaftlich fundiertes und patentiertes Verfahren, um das Sicherheitsverhalten der Mitarbeiter messbar zu machen.
- Der ESI® Awareness-Benchmark ermöglicht eine **standardisierte, transparente Messung** und Steuerung des Sicherheitsverhaltens auf Unternehmens-, Gruppen- und User-Ebene.



HORNETSECURITY



# PATENTIERTE SPEAR-PHISHING-ENGINE

VORGEHEN WIE EIN ECHTER ANGREIFER



Die patentierte Spear-Phishing-Engine nutzt individuell zugeschnittene Spear-Phishing-Angriffe unterschiedlicher Schwierigkeits-Level.



Diese orientieren sich am Aufwand, die ein Angreifer zur Vorbereitung der Phishing-Mails benötigt: je mehr Zeit ein Angreifer in die Vorbereitung investiert, desto ausgeklügelter der Angriff und höher die Wahrscheinlichkeit, dass man auf eine Phishing-Mail reinfällt.



Die Erstellung und Versendung von Phishing-E-Mails wird von der Spear Phishing Engine zu individuellen Zeitpunkten vollautomatisch gesteuert.

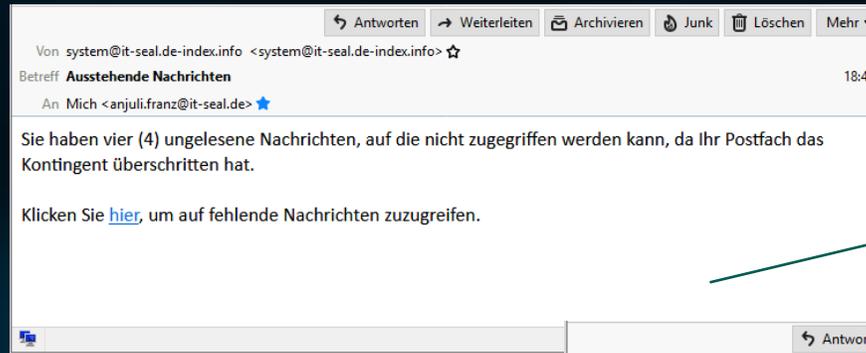


HORNETSECURITY

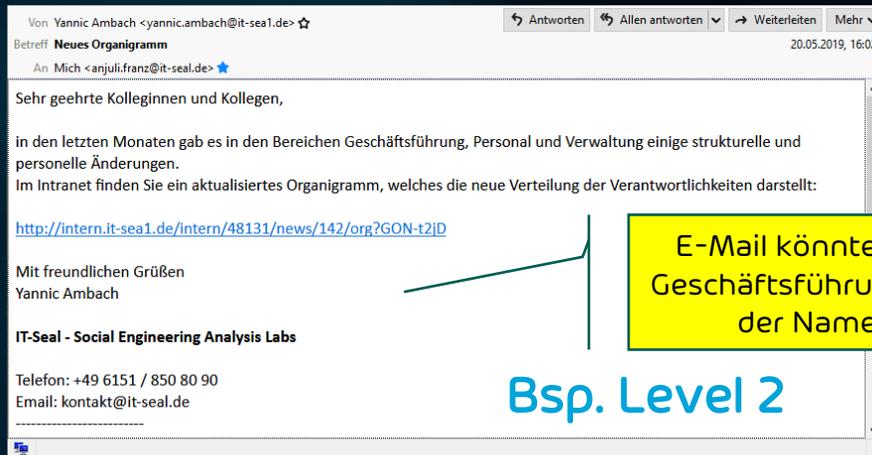
# PATENTIERTE SPEAR-PHISHING-ENGINE

## VORGEHEN WIE EIN ECHTER ANGREIFER

### Bsp. Level 1

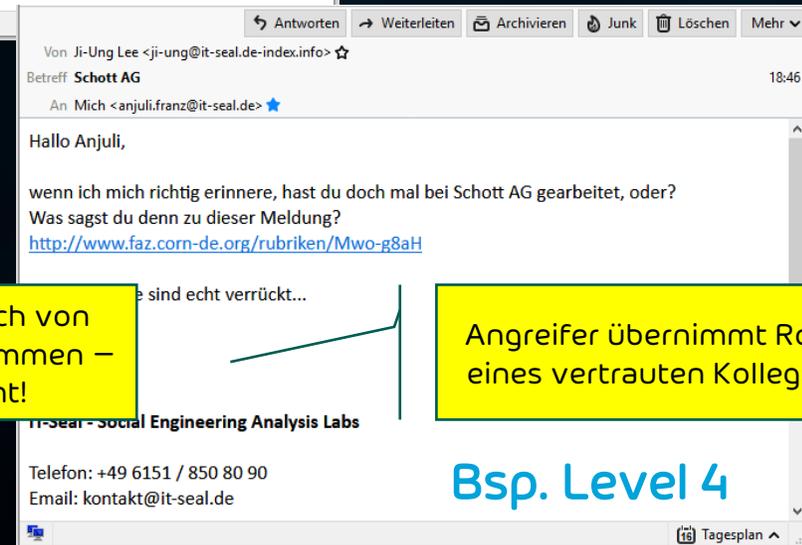


Autom. generierte System-E-Mail – könnte echt sein.



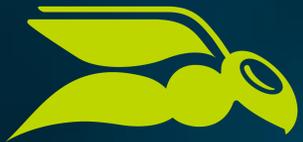
E-Mail könnte wirklich von Geschäftsführung stammen – der Name stimmt!

### Bsp. Level 2



Angreifer übernimmt Rolle eines vertrauten Kollegen.

### Bsp. Level 4



HORNETSECURITY

# PATENTIERTE SPEAR-PHISHING-ENGINE

## Vandalismus an parkenden Autos



HR Musterfrau <hr.musterfrau@it-sea1.de>  
An ✓ Christian Klos

👉 Klicken Sie hier, um Bilder herunterzuladen. Um den Datenschutz zu erhöhen, hat Outlook den automatischen Download von Bildern in dieser Nachricht verhindert.

Sehr geehrte Kolleginnen und Kollegen,

vergangene Woche wurden mehrere Fahrzeuge auf dem Firmenparkplatz von einem Unbekannten beschädigt. Bitte melden Sie sich bei mir, falls Sie Ihr Fahrzeug auf den Bildern erkennen:  
[https://www.dropbox.com/sh/dfS-u1fv/m/Dokumente/besch%C3%A4digte\\_autos?dl=0](https://www.dropbox.com/sh/dfS-u1fv/m/Dokumente/besch%C3%A4digte_autos?dl=0)

Mit freundlichen Grüßen  
HR Musterfrau

## Mal wieder was lustiges..



Maxine Musterfrau <maxine.musterfrau@it-sea1.de>  
An ✓ Max Mustermann

👉 Klicken Sie hier, um Bilder herunterzuladen. Um den Datenschutz zu erhöhen, hat Outlook den automatischen Download von Bildern in dieser Nachricht verhindert.

Hallo Max,

schau mal was ich gefunden habe:  
<https://lustich.de/file/lustig.docx?eDE-w3nV>

Liebe Grüße  
Maxine

## [GERPRÜFT] Neues Organigramm



Maxine Musterfrau <maxine.musterfrau@it-sea1.de>  
An ✓ Max Mustermann

👉 Klicken Sie hier, um Bilder herunterzuladen. Um den Datenschutz zu erhöhen, hat Outlook den automatischen Download von Bildern in dieser Nachricht verhindert.

Sehr geehrte Kolleginnen und Kollegen,

in den letzten Monaten gab es in den Bereichen Geschäftsführung, Personal und Verwaltung Änderungen. Im Intranet finden Sie ein aktualisiertes Organigramm, welches die neue Verteilung der Verantwortlichkeiten zeigt.

<http://safe-browsing.de/intern/news/142/org?xmi-d4ff>

Mit freundlichen Grüßen  
Maxine Musterfrau

## Artikel über IT-Seal



Theo Koch <theo.koch@faz.safe-browsing.de>  
An ✓ Max Mustermann

👉 Klicken Sie hier, um Bilder herunterzuladen. Um den Datenschutz zu erhöhen, hat Outlook den automatischen Download von Bildern in dieser Nachricht verhindert.

Guten Tag Herr Mustermann,

mein Name ist Theo Koch, ich arbeite bei der Frankfurter Allgemeine Zeitung und habe einen Artikel über IT-Seal geschrieben. Falls er Sie interessiert, finden Sie ihn [hier](#).

Mit freundlichen Grüßen  
Theo Koch

--  
Theo Koch  
Redakteur

Frankfurter Allgemeine Zeitung GmbH (Herausgeber)  
Hellerhofstraße 2-4  
60327 Frankfurt am Main

Zentrale: 0261/89200  
Fax: 0261/892770

Handelsregister: HRB 7344  
Amtsgericht Frankfurt am Main USt.-IDNr.: DE 114 232 723  
Verleger und Geschäftsführer:  
Thomas Lindner (Vorsitzender), Dr. Volker Breid

Herausgeber:  
Werner D'Inka, Jürgen Kaube, Berthold Kohler, Holger Steltzner



HORNETSECURITY

# PATENTIERTE SPEAR-PHISHING-ENGINE



HORNETSECURITY

High-severity: Action Required



Microsoft Online Service <warning@office365.safe-browsing.de>  
An  Max Mustermann

 Klicken Sie hier, um Bilder herunterzuladen. Um den Datenschutz zu erhöhen, hat Outlook den automatischen Download von Bildern in dieser Nachricht deaktiviert.

Office 365

## Your mail is 99% full

Hello Max Mustermann,

This message was sent to you because your mailbox [max.mustermann@hornetsecurity.com](mailto:max.mustermann@hornetsecurity.com) registered to is 99% full.

Once your mail is full, you won't be able to send or receive.

We notify you about this, to help regain your access.

[Clean Up Mail](#)

Thank You,  
Microsoft © 2019 Secured Service.

This email was sent to [max.mustermann@hornetsecurity.com](mailto:max.mustermann@hornetsecurity.com).

AccID : ##72112-7835

Wichtig: Transaktionsbestätigung benötigt



Amazon Sicherheitswarnung <securitywarning@amazon.safe-browsing.de>  
An  Max Mustermann

 Wenn Probleme mit der Darstellungsweise dieser Nachricht bestehen, klicken Sie hier, um sie im Webbrowser anzuzeigen.

[Meine Bestellungen](#) | [Mein Konto](#) | [Amazon.de](#)

Amazon Sicherheitswarnung  
Fremdlogin festgestellt

# amazon

Guten Tag Mustermann,

Ihr Amazon-Konto wurde zu Ihrem Schutz vorübergehend limitiert: Nach einem Fremdlogin wurde Ihr Konto zur Bestellung BE3025276735-6154725 genutzt.

Bitte bestätigen Sie die Transaktion, wenn diese ursprünglich von Ihnen getätigt wurde.

Beachten Sie: Die Bestellung wurde nur temporär limitiert. Erfolgt innerhalb von 7 Tagen keine Bestätigung, wird die Transaktion automatisch freigegeben.

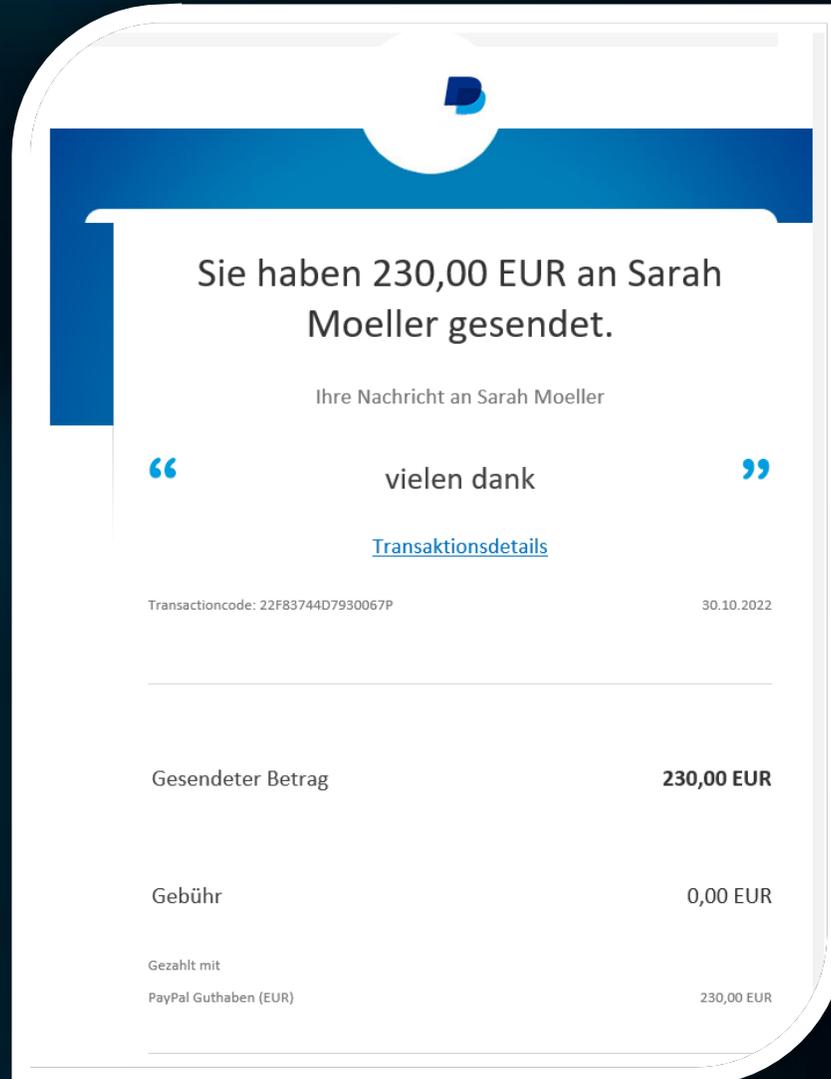
Um die Bestellung einsehen zu können, klicken Sie bitte auf [diesen Link](#).

Vielen Dank!  
**Ihr Amazon-Supportteam**

Bitte beachten Sie: Diese E-Mail dient lediglich zu Ihrer Information. Bei weiteren Fragen klicken Sie auf den Link und öffnen Sie das Supportmenü.

Dies ist eine automatisch versendete Nachricht. Bitte antworten Sie nicht auf dieses Schreiben, da die Adresse nur zur Versendung von E-Mails eingerichtet ist.

# PATENTIERTE SPEAR-PHISHING-ENGINE



The screenshot shows an email notification from WeTransfer. At the top, it says "Sie haben 230,00 EUR an Sarah Moeller gesendet." Below this, it says "Ihre Nachricht an Sarah Moeller" and contains a quote: "vielen dank". There is a link for "Transaktionsdetails". At the bottom, it shows transaction details: Transactioncode: 22F83744D7930067P, 30.10.2022, Gesendeter Betrag: 230,00 EUR, Gebühr: 0,00 EUR, and Gezahlt mit: PayPal Guthaben (EUR), 230,00 EUR.

Sie haben 230,00 EUR an Sarah Moeller gesendet.

Ihre Nachricht an Sarah Moeller

“ vielen dank ”

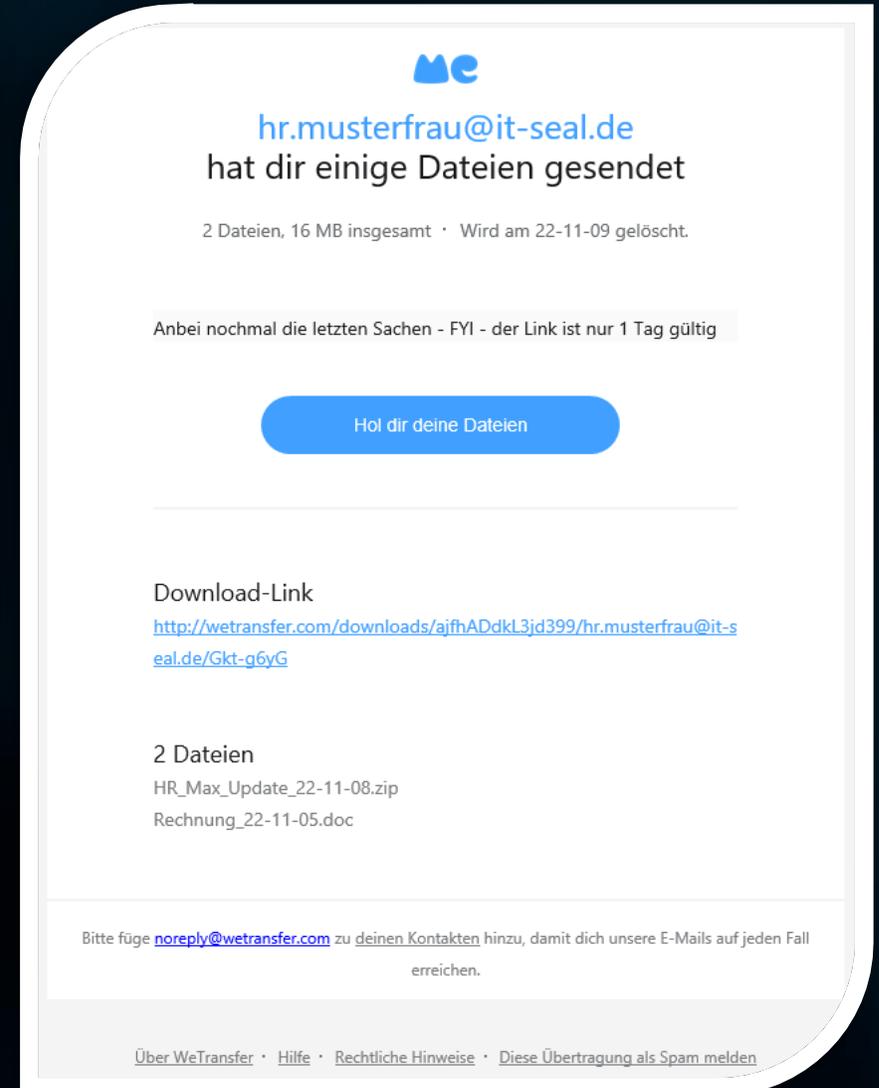
[Transaktionsdetails](#)

Transactioncode: 22F83744D7930067P 30.10.2022

---

Gesendeter Betrag	<b>230,00 EUR</b>
Gebühr	0,00 EUR

Gezahlt mit  
PayPal Guthaben (EUR) 230,00 EUR



The screenshot shows an email notification from WeTransfer. At the top, it says "hr.musterfrau@it-seal.de hat dir einige Dateien gesendet". Below this, it says "2 Dateien, 16 MB insgesamt · Wird am 22-11-09 gelöscht." There is a button that says "Hol dir deine Dateien". Below this, it says "Download-Link" and provides a URL: <http://wettransfer.com/downloads/ajfhADdKL3jd399/hr.musterfrau@it-seal.de/Gkt-g6yG>. At the bottom, it says "2 Dateien" and lists "HR\_Max\_Update\_22-11-08.zip" and "Rechnung\_22-11-05.doc". There is a footer with the text "Bitte füge noreply@wettransfer.com zu deinen Kontakten hinzu, damit dich unsere E-Mails auf jeden Fall erreichen." and a footer bar with links: "Über WeTransfer · Hilfe · Rechtliche Hinweise · Diese Übertragung als Spam melden".

hr.musterfrau@it-seal.de hat dir einige Dateien gesendet

2 Dateien, 16 MB insgesamt · Wird am 22-11-09 gelöscht.

Anbei nochmal die letzten Sachen - FYI - der Link ist nur 1 Tag gültig

Hol dir deine Dateien

---

Download-Link

<http://wettransfer.com/downloads/ajfhADdKL3jd399/hr.musterfrau@it-seal.de/Gkt-g6yG>

2 Dateien

HR\_Max\_Update\_22-11-08.zip  
Rechnung\_22-11-05.doc

Bitte füge [noreply@wettransfer.com](mailto:noreply@wettransfer.com) zu deinen Kontakten hinzu, damit dich unsere E-Mails auf jeden Fall erreichen.

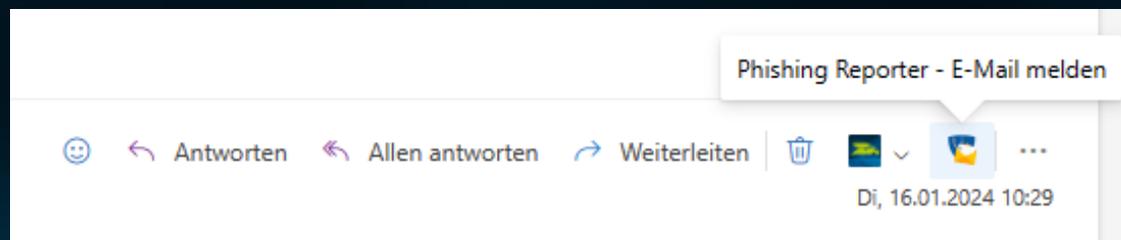
Über WeTransfer · Hilfe · Rechtliche Hinweise · Diese Übertragung als Spam melden



HORNETSECURITY

 IT-Systemhaus  
Ruhrgebiet®

# PATENTIERTE SPEAR-PHISHING-ENGINE



Phishing Reporter

## Möchten Sie diese E-Mail melden?

Folgende Anzeichen helfen Ihnen dabei eine **Phishing-Mail** zu erkennen:

- Die Absenderadresse (**noreply@spamquarantine.corn-de.org**) wirkt merkwürdig oder verdächtig
- Sie erhalten normalerweise nie Mails dieser Art
- Sie werden aufgefordert Zahlungen zu tätigen oder Login-Daten preiszugeben

Unterstützen Sie die IT, indem Sie Auffälligkeiten kurz im Textfeld auflisten. Dies ist optional.

Sonstiges

**Absender verdächtig**

URL verdächtig

Anhang verdächtig

Inhalt verdächtig



HORNETSECURITY

# PATENTIERTE SPEAR-PHISHING-ENGINE

Phishing Reporter

**Gut gemacht!**

Sie haben soeben eine unserer Phishing-Simulations E-Mails entdeckt



Sie sind  
**DIE FIREWALL**  
Ihres Unternehmens

Großartig! Eine solche E-Mail hätte für Ihr Unternehmen gefährlich werden können! Gut, dass Sie die Gefahr erkannt und gehandelt haben. Machen Sie weiter so!

Mail löschen und weiterarbeiten

## PHISHING AWARENESS-TRAINING

EIN SERVICE FÜR IT-SEAL GMBH



# GLÜCK GEHABT!

Das hätte eine Phishing-Mail sein können.

Drei einfache Schritte, wie Sie eine Phishing-Mail erkennen:

**Jetzt ansehen** ca. 3 Minuten

### Ihre Teilnahme ist 100% anonym!

Niemand erhält Informationen darüber, wer welche E-Mail geöffnet oder welchen Link angeklickt hat. Das Training dient dazu, Sie im Umgang mit Betrugsversuchen zu schulen.

### Schutz vor Cyber-Kriminellen

Cyber-Angriffe sind oft auf Ihre Organisation oder auf Sie persönlich zugeschnitten. Bleiben Sie wachsam, um sich und Ihre Organisation vor Betrug, Abzocke und weitreichenden Konsequenzen zu schützen.

AR CS DA **DE** EN ES FR HI HR HU IT JA NL NO PL PT RO RU SK SR TR ZH

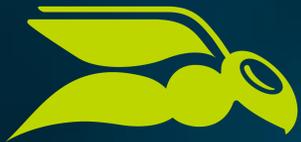
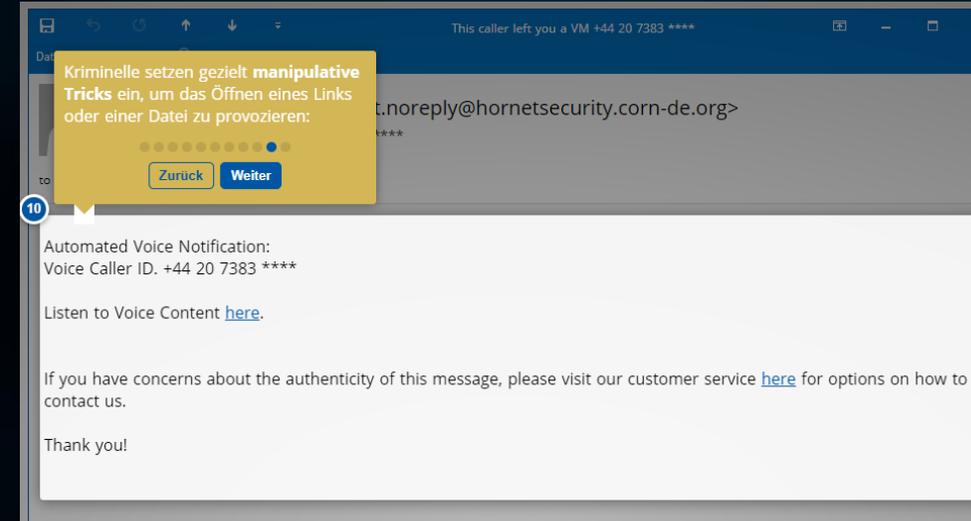
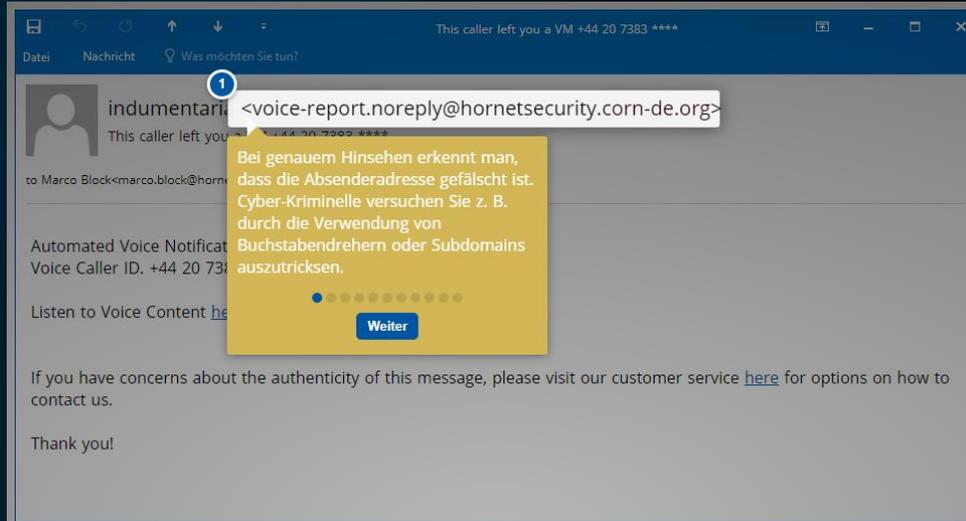
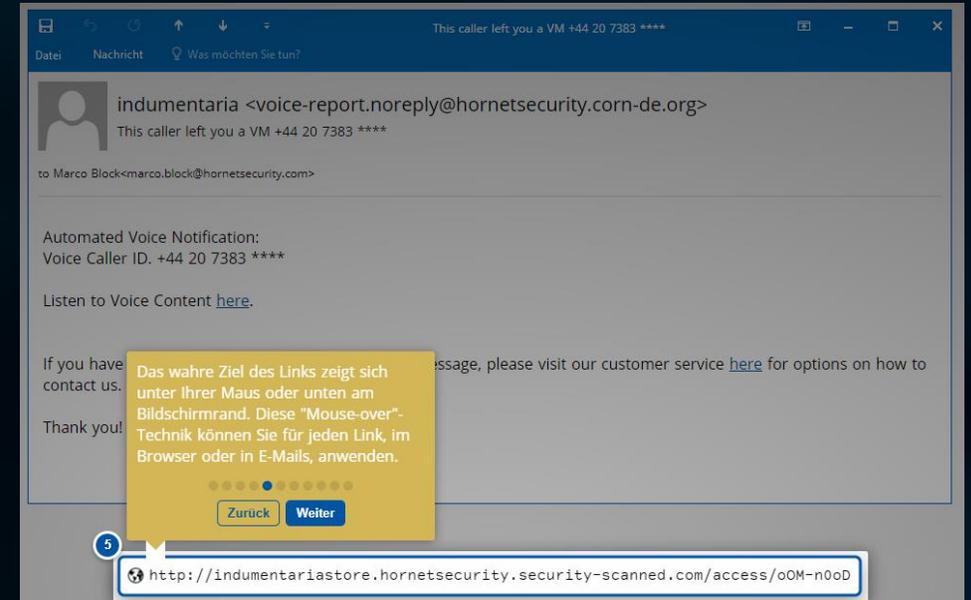
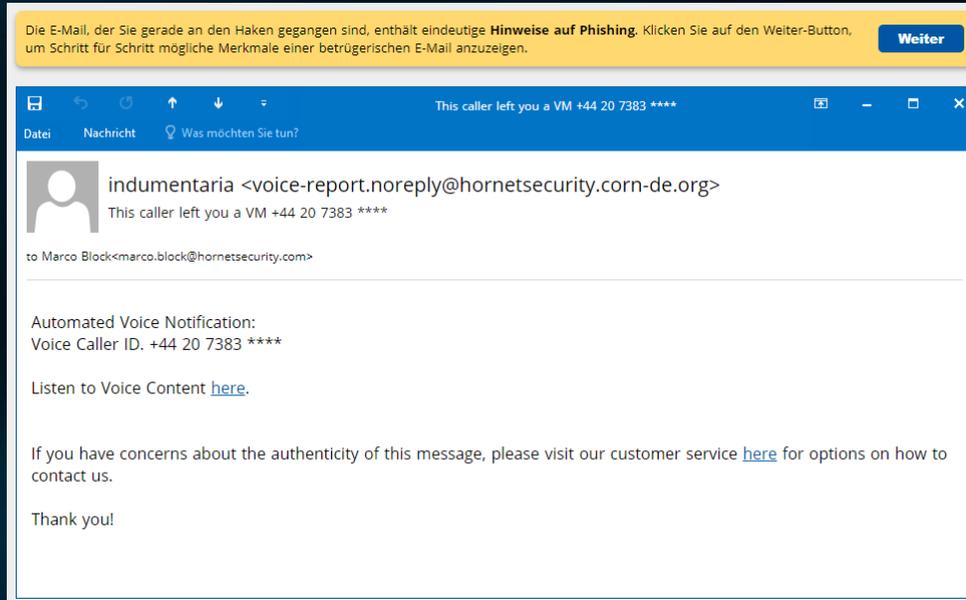


HORNETSECURITY

**IT-Systemhaus**  
Ruhrgebiet®

# PATENTIERTE SPEAR-PHISHING-ENGINE

Benutzer bei Klick auf Phishing-Mail aufklären: Most teachable moment

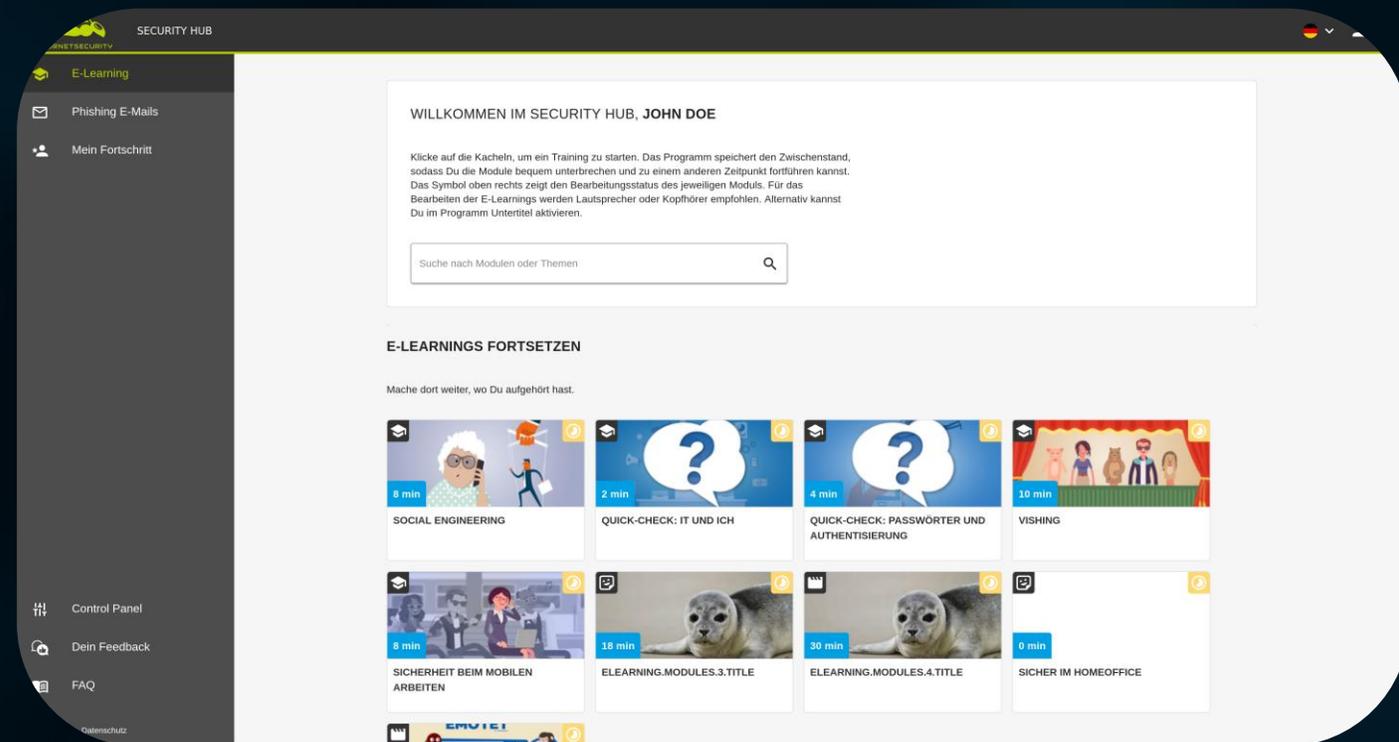


HORNETSECURITY

# SECURITY HUB

SCHAFFEN SIE EINE MOTIVIERENDE LERNUMGEBUNG FÜR IHRE BENUTZER

- Zentraler Zugriff auf alle Lerninhalte
- Auswertung der individuellen Phishing Simulation
- Gamification-Ansatz spornt Nutzer an, "ihr Bestes zu geben"
- Lerninhalte in mehreren Sprachen verfügbar



HORNETSECURITY

# AWARENESS DASHBOARD FÜR DIE USER

## IHRE SIMULIERTEN PHISHING-E-MAILS

Hier sehen Sie den Verlauf der Phishing-E-Mails, die im Rahmen der Simulation an Sie gesendet wurden. Klicken Sie auf eine Erläuterungen aufzurufen. Über den Filter können Sie den Verlauf einschränken.

erkannt

gemeldet

hereingefallen

January 2024



Gesendet am: 15.01.2024

Voice Message

Neugier

November 2023



Gesendet am: 28.11.2023

This caller left you a VM +44 20 7383 \*\*\*\*

Routine

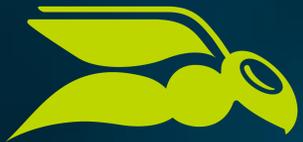
## AUSWERTUNG DER PHISHING-SIMULATION

Wie viele simulierte Phishing-E-Mails wurden an Sie gesendet? Und wie haben Sie auf diese E-Mails reagiert? Hier sehen Sie eine Zusammenfassung.

E-MAILS NACH TYP



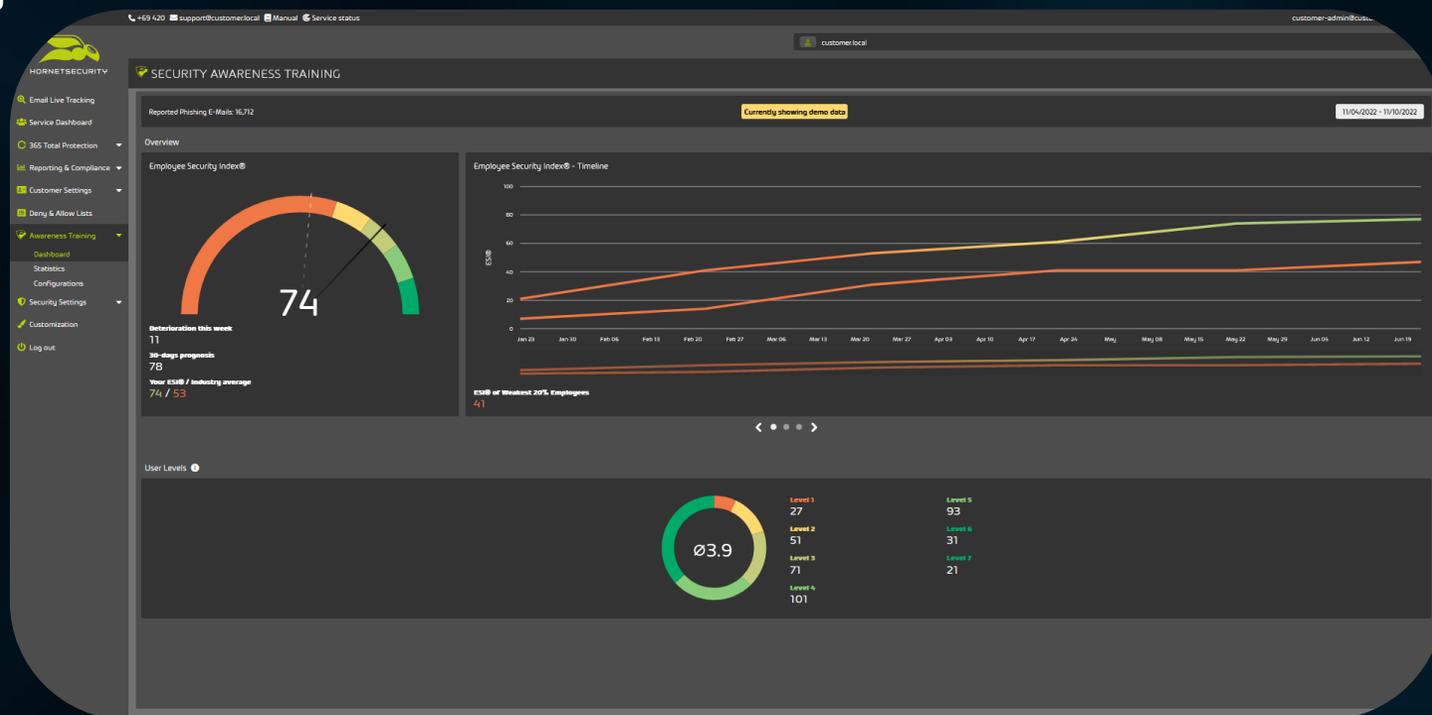
Erkannt	2	33%
Gemeldet	4	67%
Hereingefallen	0	0%



HORNETSECURITY

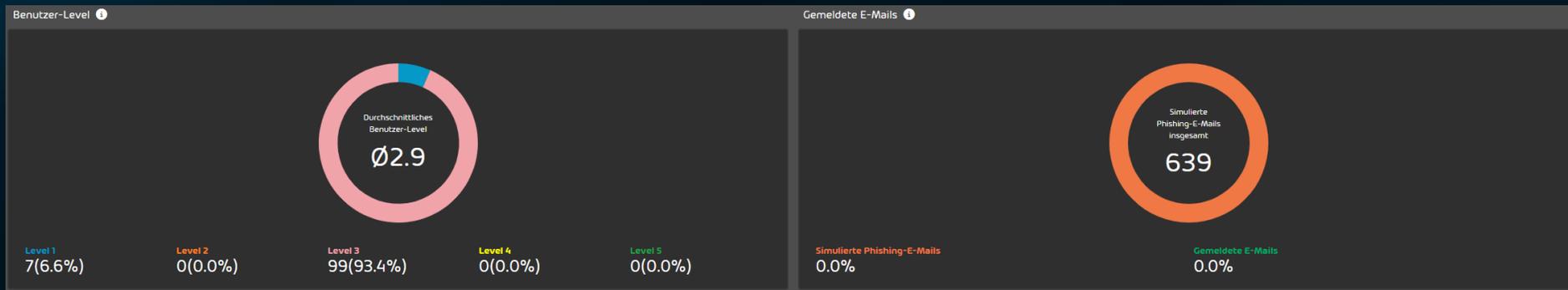
# AWARENESS DASHBOARD IM CONTROL PANEL

- Entwicklung des Security Awareness Trainings im Blick behalten
- ESI®-Reporting inkl. Historie und Forecast und Training KPIs
- Konfigurieren und passen Sie das Awareness Training an die Bedürfnisse Ihres Unternehmens an



HORNETSECURITY

# AWARENESS DASHBOARD IM CONTROL PANEL



## Erfolgreiche Phishing-E-Mails

Betreff	Trefferquote	Level	Anzahl	Links	Zugangsdaten	Dokumente
Bewerbung (Level 2)	0%	2	5	0	0	0
Warnung vom BKA (Level 3)	0%	3	2	0	0	0
Onlineumfrage (Level 2)	0%	2	7	0	0	0
Astrologie-Newsletter (Level 3)	0%	3	1	0	0	0
Spendenaufruf (Level 1)	0%	1	24	0	0	0
Kalender-App (Level 2)	0%	2	6	0	0	0
Passwort setzen (Level 1)	0%	1	27	0	0	0
Möbel zu verschenken (Level 3)	0%	3	2	0	0	0
kununu: Arbeitgeber bewerten (Level 1)	0%	1	12	0	0	0
Migration zu Outlook 2019 (Level 1)	0%	1	29	0	0	0

Sie haben eine gute Idee für ein Phishing-Szenario oder sind auf eine gut gestaltete Phishing-E-Mail gestoßen? Verwenden Sie dieses [Formular](#), um realistische Phishing-Szenarien direkt an unsere Produktentwicklung zu übermitteln.

## Trainingsstatus

Allgemein Benutzer

Suchen

Gruppe

Nur Benutzer mit nicht abgeschlossenen Modulen anzeigen

Vorname	Nachname	E-Mail-Adresse	Modul
IT	Administration	admins@cloudsecuritysolutions.onmicrosoft.com	<div style="width: 100%; height: 10px; background-color: green;"></div>
Dale	Dennett	dennett@cloudsecuritysolutions.co.uk	<div style="width: 100%; height: 10px; background-color: red;"></div>
Sam	Harris	harris@cloudsecuritysolutions.co.uk	<div style="width: 100%; height: 10px; background-color: red;"></div>
Alex	Wyllie	alex.wyllie@cloudsecuritysolutions.co.uk	<div style="width: 100%; height: 10px; background-color: red;"></div>
Laura	Wünsche	wuensche@cloudsecuritysolutions.co.uk	<div style="width: 100%; height: 10px; background-color: red;"></div>
Lola	Climent Sánchez	lola@cloudsecuritysolutions.co.uk	<div style="width: 100%; height: 10px; background-color: red;"></div>
Luis	Prado	prado@cloudsecuritysolutions.co.uk	<div style="width: 100%; height: 10px; background-color: green;"></div>
Lydia	Cheung	cheung@cloudsecuritysolutions.co.uk	<div style="width: 100%; height: 10px; background-color: red;"></div>
Manuel	Buttigieg	manuel.buttigieg@cloudsecuritysolutions.co.uk	<div style="width: 100%; height: 10px; background-color: red;"></div>
Marcel	Künzenbach	kuenzenbach@cloudsecuritysolutions.co.uk	<div style="width: 100%; height: 10px; background-color: red;"></div>

## Individuelle Ergebnisse

Sie können die individuellen Ergebnisse aller Benutzer zur Phishing-Simulation als Excel-Datei exportieren.

Herunterladen

	E-Mail	GivenName	FamilyName	group_name	attacks	clicks_total	macros_total	logins_total	clicks_lvl_1	clicks_lvl_2	clicks_lvl_3	clicks_lvl_4	clicks_lvl_5
0	admins@cloudsecuritysolutions.onmicrosoft.com	IT	Administration	All Company	6	0	0	0	0	0	0	0	0
1	dennett@cloudsecuritysolutions.co.uk	Dale	Dennett		8	0	0	0	0	0	0	0	0
2	harris@cloudsecuritysolutions.co.uk	Sam	Harris	Sales	6	0	0	0	0	0	0	0	0
3	alex.wyllie@cloudsecuritysolutions.co.uk	Alex	Wyllie		5	0	0	0	0	0	0	0	0
4	wuensche@cloudsecuritysolutions.co.uk	Laura	Wünsche		7	0	0	0	0	0	0	0	0
5	lola@cloudsecuritysolutions.co.uk	Lola	Climent Sánchez		6	0	0	0	0	0	0	0	0
6	prado@cloudsecuritysolutions.co.uk	Luis	Prado		6	0	0	0	0	0	0	0	0



HORNETSECURITY

# AWARENESS DASHBOARD IM CONTROL PANEL

Benutzer und Gruppen Phishing-Simulation E-Training

## AUSGEWERTETE GRUPPEN

Die Auswertung des Security Awareness Services basiert auf Gruppen. Je mehr Gruppen Sie zum Security Awareness Service hinzufügen, desto detaillierter werden die Ergebnisse der Auswertung.

+ Gruppe hinzufügen

Gruppe
Standard
1 All Company
2 Sales

## AUSGESCHLOSSENE BENUTZER

Standardmäßig wird der Security Awareness Service auf alle Benutzer des Kunden angewendet. Sie können jedoch einzelne Benutzer vom Security Awareness Service ausschließen.

Neue synchronisierte Benutzer automatisch aus dem Security Awareness Service ausschließen

Suchen

Alle Gruppen

Benutzer ausschließen Gruppe ausschließen **Alle Benutzer ausschließen** **Alle Benutzer von der Liste entfernen**

E-Mail-Adresse : Gruppe(n)

Es sind keine Daten vorhanden.

Benutzer und Gruppen Phishing-Simulation **E-Training**

E-Trainings für Benutzer aktivieren

Die E-Trainings erhöhen durch die Schulung Ihrer Benutzer zu IT-Sicherheitsthemen.

### Beginn des ersten E-Trainings

11.01.2023

Alle E-Trainings für alle Benutzer bereitstellen

Erinnerungs-E-Mails für E-Trainings senden

### Maximale Anzahl von Monaten ohne E-Trainings

2

Änderungen verwerfen **Änderungen übernehmen**

## AWARENESS ENGINE

Awareness Engine aktivieren

Single User Booster

Productivity Booster

E-Trainings unabhängig von der Sprache des Benutzers senden

## GRUNDLEGENDE EINSTELLUNGEN FÜR DIE PHISHING-SIMULATION

### Beginn der Phishing-Simulation

18.01.2023

### Frequenz der simulierten Phishing-E-Mails

Automatisch  Benutzerdefiniert

Mittel (etwa 2 E-Mails pro Monat)

### Allgemeine Einstellungen

Datenschutzmodus

### Einstellungen des Phishing Reporters

Phishing Reporter **Herunterladen**

Gemeldete E-Mails an die folgende E-Mail-Adresse weiterleiten

Standardadresse **Speichern**

### Besondere Arten von simulierten Phishing-E-Mails

Anhänge

Makros

Phishing nach Zugangsdaten

Domain-Spoofing

## ORGANISATIONSEINSTELLUNGEN

Name: cloudsecuritysolutions.co.uk

Anrede: Nachname

Sprache: Englisch

Art der Organisation:  Unternehmen  Behörde

**Auswertung der Daten der Organisation auf Kununu**

URL der Kununu-Seite Ihrer Organisation



HORNETSECURITY

# Unsere Services

## 365 TOTAL PROTECTION SUITE PLANS

NEXT-GEN SECURITY, BACKUP, COMPLIANCE & SECURITY AWARENESS FOR MICROSOFT 365



### BUSINESS

### ENTERPRISE

### BACKUP

### COMPLIANCE & AWARENESS

SPAM & MALWARE PROTECTION

ADVANCED THREAT PROTECTION

BACKUP & RECOVERY OF MAILBOXES & TEAMS

PERMISSION MANAGEMENT

PHISHING & ATTACK SIMULATION

COMMUNICATION PATTERN ANALYSIS

EMAIL ENCRYPTION

EMAIL ARCHIVING

BACKUP & RECOVERY OF ONEDRIVE & SHAREPOINT

PERMISSION ALERTS

SECURITY AWARENESS

AI RECIPIENT VALIDATION

EMAIL SIGNATURES & DISCLAIMERS

EMAIL CONTINUITY

BACKUP & RECOVERY OF ENDPOINTS

PERMISSION AUDIT

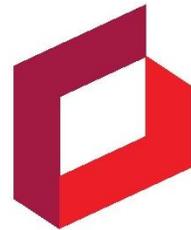
ESI® REPORTING

SENSITIVE DATA CHECK





**HORNETSECURITY**



**IT-Systemhaus**  
Ruhrgebiet®

Fragen? Wünsche? Anregungen?  
Interesse?