



HORNETSECURITY

Damals im Osten...



HORNETSECURITY

Damals im Westen...



HORNETSECURITY

Und heute...



HORNETSECURITY

LOCALIQ

# Größte Risiken im Geschäftsumfeld weltweit Allianz Risk Barometer 2024



## Cyber incidents

(e.g., cyber crime, IT network and service disruptions, malware / ransomware, data breaches, fines, and penalties)

# The most important global business risks for 2024



HORNETSECURITY



# Wer sind „Die Hacker“?



HORNETSECURITY



# Wer sind „Die Hacker“?



HORNETSECURITY



# Lockbit durch Ermittler zerschlagen - zwei Festnahmen

 EUROPOL

OPERATION **CRONOS**



**10**  
< COUNTRIES  
IN TASKFORCE  
CRONOS />



**2**  
< ARRESTS />



MORE THAN  
**200**  
< CRYPTOCURRENCY  
ACCOUNTS FROZEN />



**34**  
< SERVERS TAKEN  
DOWN />



**14 000**  
< ROGUE ACCOUNTS  
CLOSED />



< LAW ENFORCEMENT HAS TAKEN  
CONTROL OF THE TECHNICAL  
INFRASTRUCTURE AND LEAK SITE />

📍 Quelle: <https://www.europol.europa.eu/>



HORNETSECURITY

# Social Engineering Attacken auf Unternehmen

- wer ist CEO des Unternehmens
- welche Personen befinden sich in Führungspositionen?
- wer ist befugt Überweisungen zu tätigen?
- wann sind Entscheidungsträger im Urlaub oder auf Geschäftsreise?
- welche geschäftlichen Aktivitäten finden derzeit statt?



HORNETSECURITY

A screenshot of a LinkedIn profile for Torben Hansen. The profile picture shows a man in a dark suit and white shirt. The background of the profile banner features the Hornetsecurity logo and the text "Follow me!" in a white, slanted font. Below the profile picture, the name "Torben Hansen" is displayed with a "Jetzt verifizieren" (Verify now) button. His current position is "Teamlead Inside Sales & Partner Account Manager at Hornetsecurity", and his location is "Berlin, Berlin, Deutschland". He has "500+ Kontakte" (500+ connections). The profile also shows two organizations: "Hornetsecurity" and "WBS Training Schulen Berlin".

**Follow me!**

**HORNETSECURITY**

**Torben Hansen** [Jetzt verifizieren](#)

Teamlead Inside Sales & Partner Account Manager at Hornetsecurity

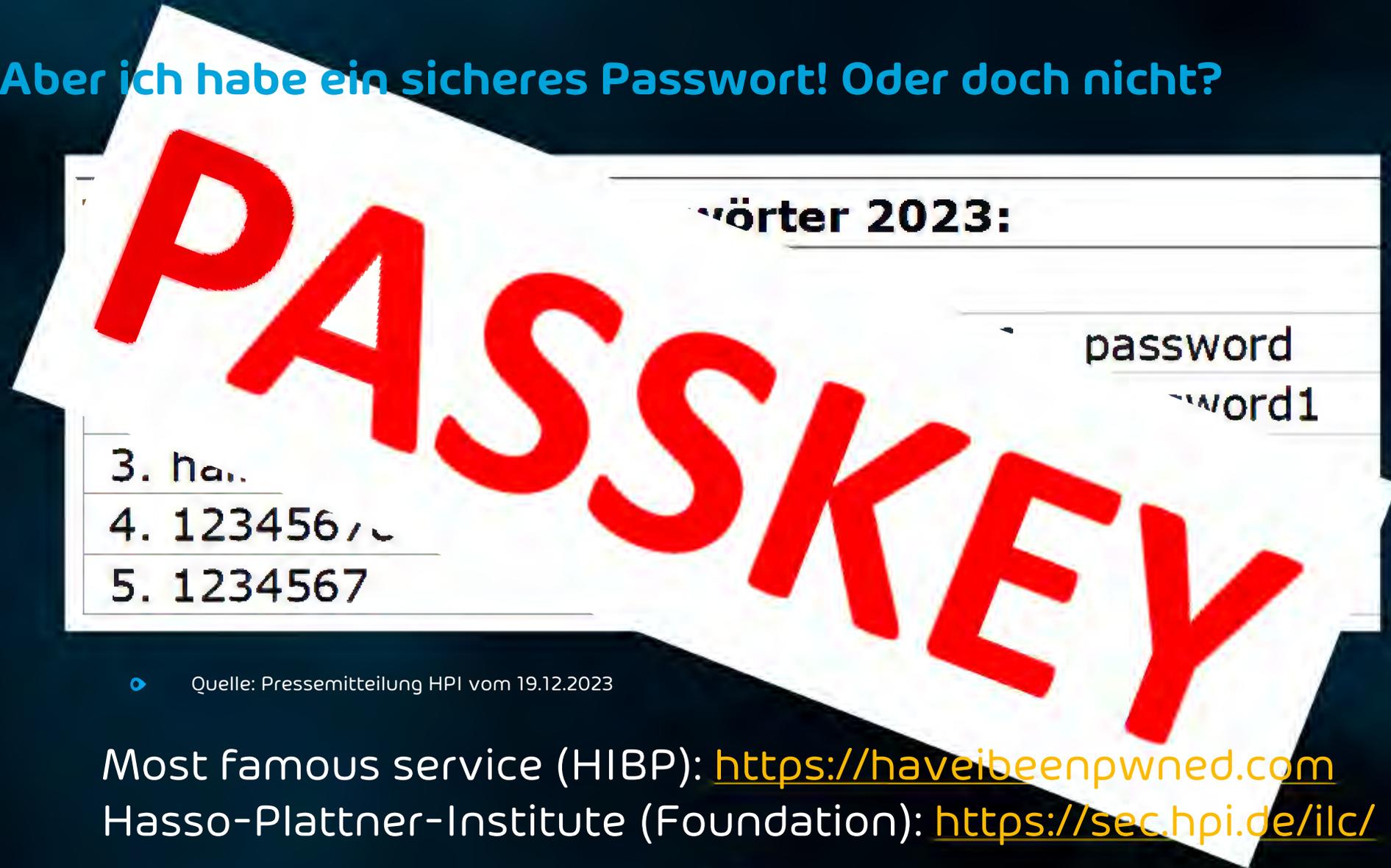
Berlin, Berlin, Deutschland · [Kontaktinfo](#)

500+ Kontakte

Hornetsecurity

WBS Training Schulen Berlin

Aber ich habe ein sicheres Passwort! Oder doch nicht?



Quelle: Pressemitteilung HPI vom 19.12.2023

Most famous service (HIBP): <https://haveibeenpwned.com>

Hasso-Plattner-Institute (Foundation): <https://sec.hpi.de/ilc/>

# Statistiken Zur Cybersicherheit für 2024

- Im Jahr 2024 wird es weltweit **3,5 Millionen unbesetzte Stellen** im Bereich Cybersicherheit geben.
- Es wird prognostiziert, dass die gesamte globale Datenspeicherung bis 2025 **200 Zettabyte überschreiten** wird.
- Der Markt für Cybersicherheit wird jährlich um **15% wachsen**.

Wächst Ihr Budget auch?

Quelle: [Top 10 Cybersecurity Predictions and Statistics For 2024 \(cybersecurityventures.com\)](https://www.cybersecurityventures.com)



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 % der Cybersicherheitsprobleme sind auf menschliches Versagen zurückzuführen**

[World Economic Forum:  
The Global Risks Report 2022]



**IT Security: Der Mensch ist Risikofaktor Nr. 1**



HORNETSECURITY

# DES HACKERS LIEBSTES TOOL...

E-Mail Kommunikation ist das größte Einfallstor für Cyberangriffe....

- leicht zu identifizieren
- keine Authentifizierung durch den Angreifer
- keine unternehmensspezifische Zugriffskontrollen
- am meisten genutzte Dienst für Unternehmen
- Mitarbeiter werden direkt kontaktiert
- Austausch sensibler Informationen
- personalisierbar und massenhafter Versand



**91%** aller Cyber-  
Attacken starten mit  
einer E-Mail



HORNETSECURITY

# Phishing ist größter Bedrohungsfaktor



HORNETSECURITY

## E-Mails bleiben größtes Sicherheitsrisiko

Anteil der Befragten in Deutschland, die 2021 folgende IT-Sicherheitsvorfälle erlebt haben (in %)



Basis: Über 2.000 Befragte (ab 16 Jahren) in Deutschland; Juni 2021

Quelle: Deutschland sicher im Netz e.V.



statista

Shit happens!



**A HIGH BUDGET  
CYBERSECURITY DEFENSE**



**ONE EMPLOYEE CLICKING A  
PHISHING EMAIL**



HORNETSECURITY

ABO WirtschaftsWoche

CYBER-ANGRIFF

## Wieso Unternehmen ihre IT-Sicherheit nicht in den Griff bekommen

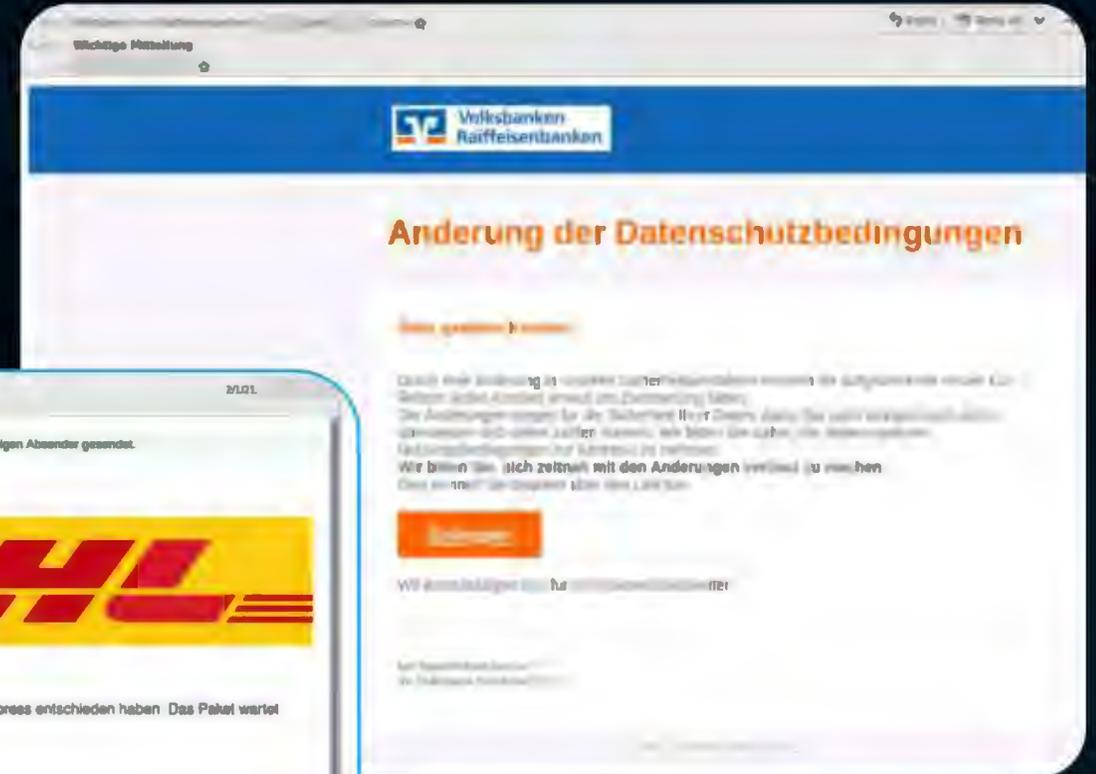
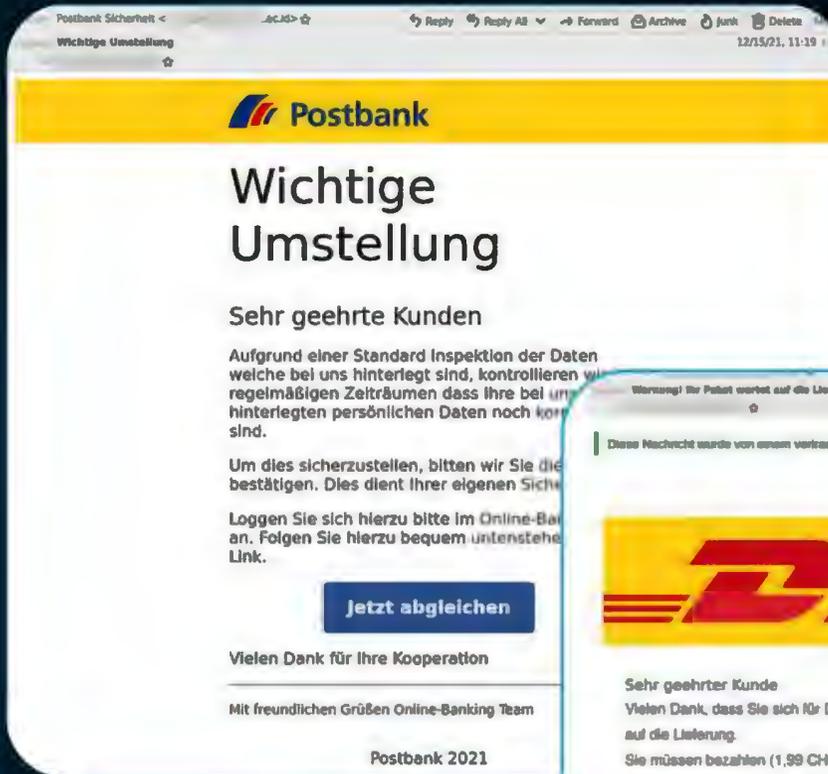
von Sebastian Schug  
20. April 2024



Netzwerkkabel stecken in einem Schrankraum in München (Bayern) in einem Switch.  
Bild: dpa

Cyber-Angriffe auf Unternehmen sind ein wiederkehrendes Übel. Aber wieso eigentlich? Wie so oft in der IT, sitzt die Antwort vor dem Bildschirm.

# BEISPIEL PHISHING MAIL



# SMISHING via WhatsApp oder SMS

07:22

LTE



9 Personen

iMessage

So., 8. Okt., 09:34

spunfedrottan95@icsh4z.itunespartlight.com

Hallo! Wir brauchen jemanden, der Hotelreservierungen auf Expedia überprüft. Verdienen Sie 400-700 Euro pro Tag mit kostenlosem Training.

Unsere Aufgabe ist einfach: Wir müssen nur das Hotel bewerten oder mögen. Es kann ohne Beeinträchtigung Ihrer aktuellen Tätigkeit absolviert werden und es gibt keine akademischen Qualifikationsbeschränkungen. Wenn Sie bei uns mitmachen möchten, WhatsApp-Daten: +4915216395142

(Voraussetzung: 22 Jahre und älter)



haskamde@icloud.com

iMessage

Heute, 09:14

Willkommen! Wir haben festgestellt, dass Ihr Werdegang und Ihr Lebenslauf von mehreren Online-Personalvermittlungsagenturen empfohlen wurden. Deshalb möchten wir Ihnen einen Teilzeitjob anbieten, den Sie in Ihrer Freizeit ausüben können. Unsere Aufgabe ist einfach: Wir bewerten einfach Ihre Lieblingshotels. Es gibt keine zeitliche Begrenzung und Sie können die Beurteilung zu Hause durchführen. Der Tageslohn liegt zwischen 300 und 1000 Euro, alle Löhne werden am selben Tag ausgezahlt. Wenn Sie teilnehmen möchten, kontaktieren Sie uns bitte per WhatsApp: +4915212552742 (Hinweis: Sie müssen über 20 Jahre alt sein)



HORNETSECURITY

# Phishing Attacken via QR Codes



Hornetsecurity erkennt QR Codes die in Bildern integriert sind.

```
qrs (master) X du -h qr-mixed.png
2.2M  qr-mixed.png
->qrs (master) X file qr-mixed.png
qr-mixed.png: PNG image data, 1500 x 843, 8-bit/color RGB, non-interlaced
->qrs (master) X ./qrs qr-mixed.png
Hurra! Task completed in 69.874459ms.
```

QR Code ID	Data
0	#hornetrocks
1	https://www.hornetsecurity.com
2	https://www.youtube.com/channel/UC7gf25rTAlVqv2acMQfCE0g/videos
3	BEGIN:VCARD VERSION:3.0 N:Doe;John ORG: Example Inc TITLE:Doctor EMAIL;TYPE=INTERNET:john.doe@example.com URL:https://en.wikipedia.org/wiki/John_Doe TEL;TYPE=CELL:9876543210 TEL:0123456789 TEL;TYPE=FAX:0123498765 ADR;;; 123 Main Street;Anywhere;;12345;United States END:VCARD



Cyberkriminelle senden Emails oder Bilder mit QR Codes die zu schadhafte Seiten oder Dokumenten führen.

In den QR Scan Ergebnissen werden unterschiedliche QR Codes analysiert (URLs, Texte und Kontakte). Dabei werden die Formate GIF, JPG, PNG und BMP unterstützt.

# Awareness in anderen Unternehmensbereichen



## Brände verhüten

 Keine offene Flamme; Feuer, offene Zündquelle und Rauchen verboten

### Verhalten im Brandfall

**Ruhe bewahren**

**Brand melden**

-  Handfeuermelder betätigen
-  Notruf 112  
Notruf intern 0561 804-2222

**In Sicherheit bringen**

- Getährdete Personen warnen/  
Handfeuermelder betätigen
- Hilflose mitnehmen
- Türen schließen
-  Gekennzeichneten  
Fluchtwegen folgen
- Aufzug nicht benutzen
-  Sammelstelle aufsuchen  
Auf Anweisungen achten

**Löschversuch unternehmen**

-  Feuerlöscher benutzen
-  Löschechlauch benutzen
-  Mittel und Geräte zur  
Brandbekämpfung benutzen  
(z. B. Löschdecke)



HORNETSECURITY



HORNETSECURITY



# VERHALTEN BEI IT-NOTFÄLLEN



**Ruhe bewahren & IT-Notfall melden**  
Lieber einmal mehr als einmal zu wenig anrufen!



IT-Notfallrufnummer:



Wer meldet?



Welches IT-System ist betroffen?



Wie haben Sie mit dem IT-System gearbeitet?  
Was haben Sie beobachtet?



Wann ist das Ereignis eingetreten?



Wo befindet sich das betroffene IT-System?  
(Gebäude, Raum, Arbeitsplatz)

## Verhaltenshinweise

Weitere Arbeit  
am IT-System  
einstellen

Beobachtungen  
dokumentieren

Maßnahmen nur  
nach Anweisung  
einleiten

Herausgeber: Bundesamt für Sicherheit in der Informationstechnik



Bundesamt  
für Sicherheit in der  
Informationstechnik

[www.bsi.bund.de](http://www.bsi.bund.de)



[www.allianz-fuer-cybersicherheit.de](http://www.allianz-fuer-cybersicherheit.de)



[www.klicksafe.de](http://www.klicksafe.de)



HORNETSECURITY

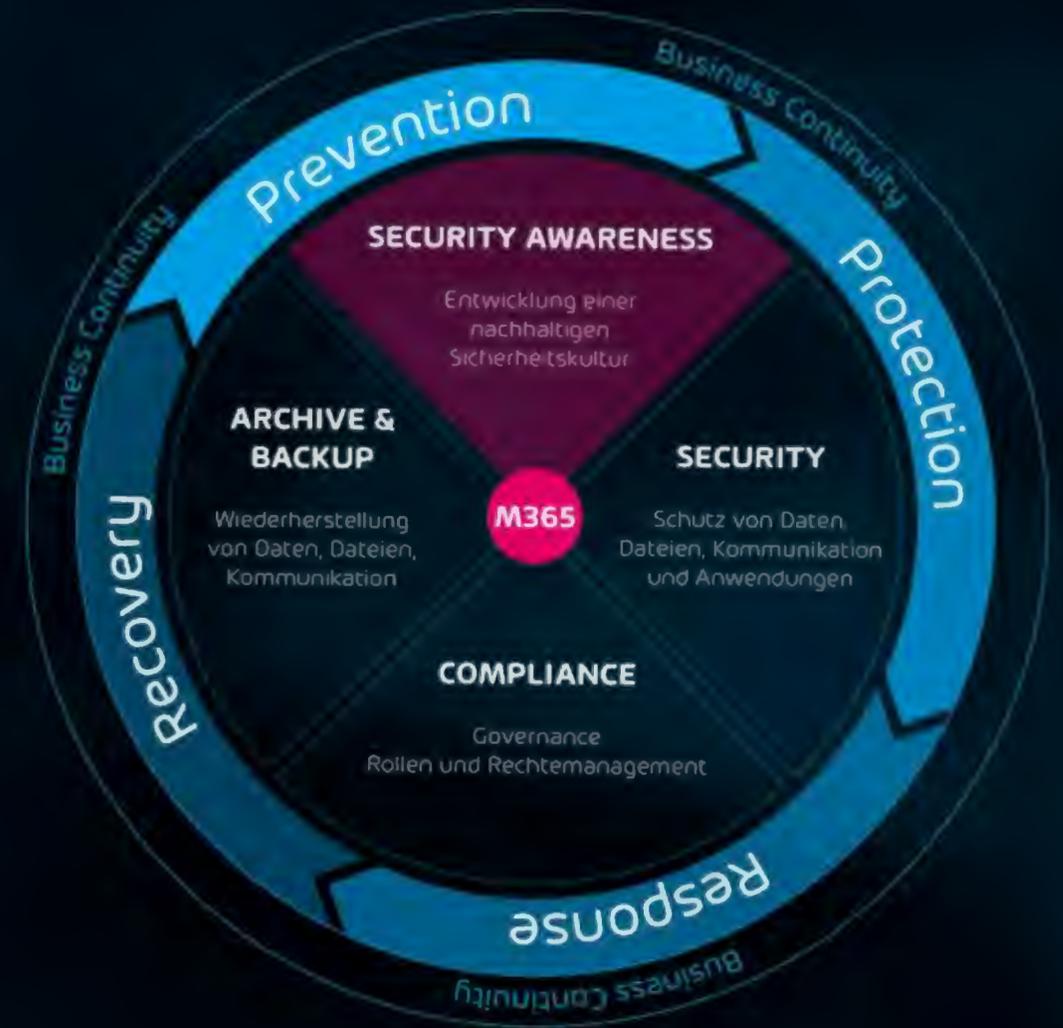
# NEXT-GEN SECURITY AWARENESS SERVICE



HORNETSECURITY



SECURITY  
AWARENESS  
TRAINING



# 1 von 4

Unternehmen erleidet eine E-Mail-Sicherheitsverletzung

# 28,7 %

der Unternehmen schulen ihre Endbenutzer nicht darin, wie sie potenzielle Ransomware-Angriffe erkennen und melden können.

# 1,3 Mrd. €

Höhe der Geldbußen, die für Verstöße gegen die DSGVO allein in der ersten Hälfte des Jahres 2023 verhängt wurden, verglichen mit 800 Millionen Euro für das gesamte Jahr 2022.\*\*

# 43 %

bestätigte Datenschutz-Verletzungen aufgrund von menschlichen Fehlern durch fehlgeleitete E-Mails\*.

# 62 %

E-Mail-Sicherheitsverletzungen wurden durch kompromittierte Passwörter und Phishing-Angriffe verursacht.

# 15,2 %

der Unternehmen schützen ihre Backups nicht vor Ransomware.

Sources:

[Hornetsecurity Research and Publications](#)

\* [2023 Data Breach Investigations Report](#),

\*\* [www.enforcementtracker.com](http://www.enforcementtracker.com)



# 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
- Sicherheitsmeldekette



Reporter-Button  
Outlook Add-In



# Phishing Mails Beispiele



Sehr geehrte/r Tassilo Totzeck,

wir sind Ourobit - ein Unternehmen, das sich auf Highspeed-Internetausbau spezialisiert hat. Damit Sie und Ihre Kollegen mit schnelleren Internet noch bequemer im Homeoffice arbeiten können, ermöglichen wir zusammen mit Ihrem Arbeitgeber Highspeed-Internet für Sie zu Hause. Damit wir Ihnen die bestmögliche Internet-Lösung anbieten können, führen wir derzeit stichprobenartig Mitarbeiterumfragen durch, um zu erfahren, ob bei Ihnen und Ihren Kollegen Interesse an unserem **Highspeed-Internet-Kombipaket** besteht.

Unser Kombipaket umfasst den Ausbau Ihres Heimanschlusses und das Ihrer Kollegen für ein flüssigeres Arbeiten im Homeoffice.

Um sicherzustellen, dass Sie von unserem Angebot profitieren können, würden wir uns freuen, wenn Sie uns bei unserer Umfrage unterstützen. Die Umfrage wird nur wenige Minuten in Anspruch nehmen und wird uns helfen, Ihre Bedürfnisse besser zu verstehen.

[Zur Umfrage](#)

Vielen Dank im Voraus für Ihre Teilnahme an unserer Umfrage. Wir freuen uns darauf, Ihnen schon bald schnelleres Internet nach Hause zu bringen

Mit freundlichen Grüßen  
Ihr Ourobit

Dietmar Ick  
Leiter für Kundenzufriedenheit

[Impressum](#) [Datenschutz](#) [Partner](#) [Nutzungsbedingungen](#)

© Ourobit AG

Ihre Amazon.de-Bestellung "Canon PowerShot SX7..." wurde versandt!

Amazon [versandbestaetigung@amazon.de](mailto:versandbestaetigung@amazon.de) [index.info](mailto:index.info)

Amazon.de

amazon.de

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

**Versandbestätigung**

Order #1110, [AMZ2551906351](#)

**Gueltig**

Wir möchten Ihnen hiermit mitteilen, dass sich der letzte Artikel aus Ihrer Bestellung in Zustellung befindet. Alle weiteren Artikel aus dieser Bestellung wurden bereits versandt.

Ihre Sendung bezieht sich nun auf dem Versandweg, eine Änderung durch Sie oder unseren Kundenservice ist nicht mehr möglich. Möchten Sie einen Artikel aus Ihrer Bestellung zurückgeben oder andere Bestellungen ansehen oder verändern, nutzen Sie bitte den Bereich [Meine Bestellungen](#) auf unserer Website [Amazon.de](#).

**Zustellung**  
05.04.2024

[Lieferung verfolgen](#)

Die Sendung geht an:

**Tassilo Totzeck**  
[tt@togo.de](mailto:tt@togo.de)

Die Lieferung wurde mit Amazon Logistics versandt. Wenn Sie diese Optionen verfügbar machen, können Sie Ihre Amazon Prime Mitgliedschaft nutzen. Amazon Logistics ist ein Dienst, der Ihnen eine schnelle und zuverlässige Lieferung von Amazon Prime Mitgliedschaften ermöglicht. Dies ist die Paketversandoption, die am nächsten dem Erhalten dieser E-Mail nach nicht über Amazon Prime verfügbar ist.

Wenn Sie ein mobiles Gerät verwenden, können Sie mit der kostenlosen Amazon Mobile App, die heruntergeladen werden kann, den Verlauf Ihrer Sendung auch unterwegs verfolgen.

Bestellen Sie diese Artikel zu: [Klicken Sie hier](#)

**Einzelheiten Ihrer Lieferung**

- Canon PowerShot SX70 HS (20.1 MP, 99-bildschirm, 24mm, Dual- und wasserabweisend, 7.5cm LCD, WLAN, 4K-Video) **EUR 485,00**  
Versand by Amazon EU S.a.r.l.

Zwischensumme **EUR 485,00**

Verpackung und Versand: **EUR 4,99**

Große Lieferung: **-EUR 4,99**

Zwischensumme ohne USt.: **EUR 393,05**

Umsatzsteuer: **EUR 62,34**

**Endbetrag inkl. USt.: EUR 485,00**

Zahlung über Visa **EUR 485,00**

Rücksendungen sind einfach. Besuchen Sie unser [Rücksendezentrum](#).

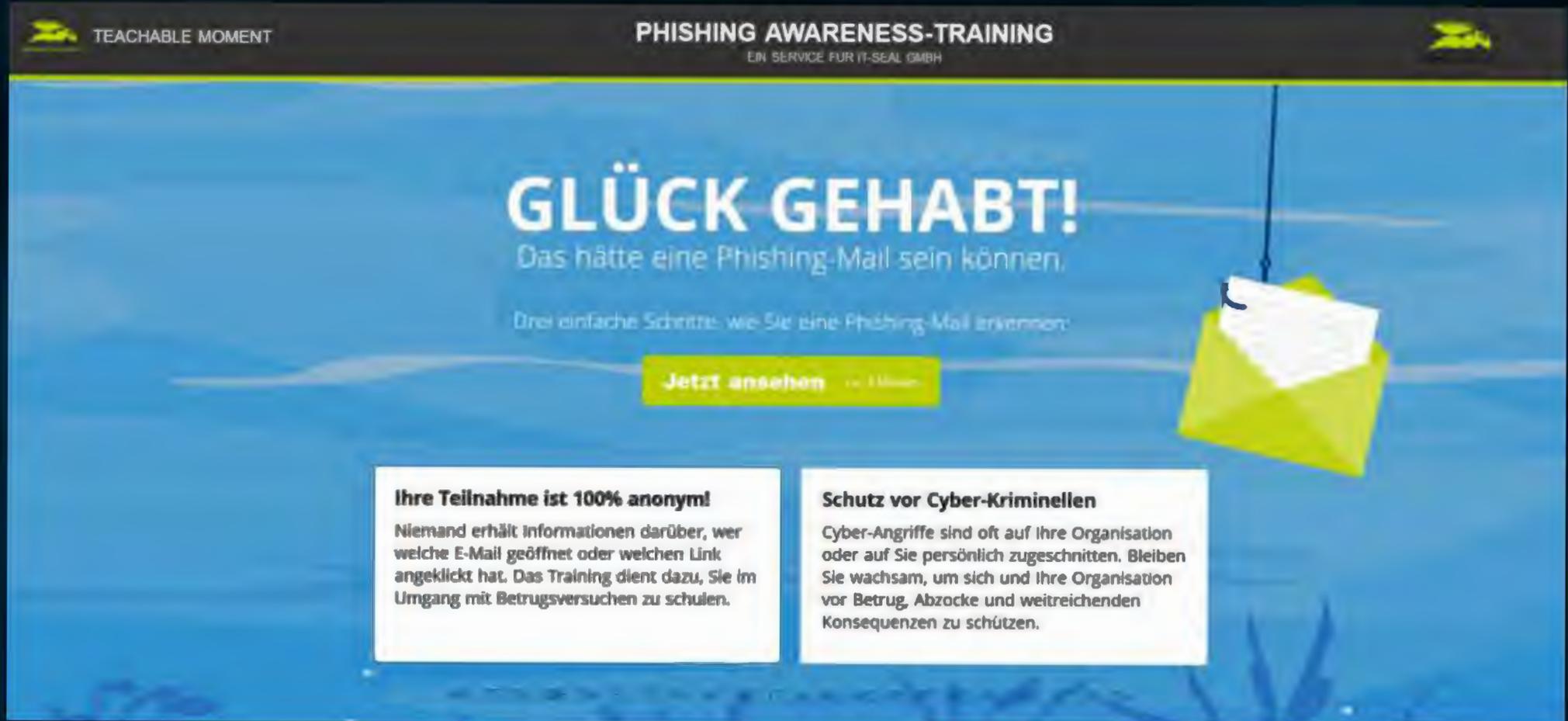
Wir freuen uns auf Ihren nächsten Besuch!  
**Amazon.de**



HORNETSECURITY

# PATENTIERTE SPEAR-PHISHING-ENGINE

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



TEACHABLE MOMENT

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](#) (10 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.



HORNETSECURITY

# PATENTIERTE SPEAR-PHISHING-ENGINE

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

TEACHABLE MOMENT PHISHING AWARENESS-TRAINING

Joachim Junghans <joachim.junghans@fissi.corn-de.org>  
Kooperationsanfrage IT S...

Sehr geehrter Herr Blume,

letzte Woche Dienstag habe ich  
sprachen über mögliche Synergi  
Frau Kamiar-Gilani meinte, ich si  
zusammengeschrieben, Sie finden...

Ich freue mich auf Ihre Gedanken zu meinem Entwurf. Wenn Sie telefonisch Rücksprache halten möchten, erreichen Sie mich am besten mobil unter; 0173/14159265

Beste Grüße  
Joachim Junghans

Joachim Junghans  
Projektmanagement



HORNETSECURITY

# Awareness Trainings Module

## Anstehende E-Trainings

Hier finden Sie alle E-Trainings, die Sie noch nicht begonnen haben



Schutzklassen

## Abgeschlossene E-Trainings

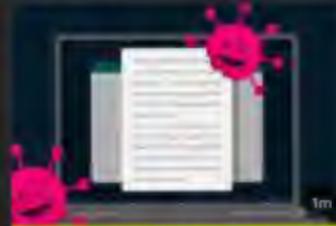
Hier finden Sie alle E-Trainings, die Sie abgeschlossen haben. Sie können sie erneut starten, um Ihr Wissen aufzufrischen.



Gift Card Scams



Adware & Malvertising



Gefährliche Makros – Emotet und die Makrovirenpandemie



Social Engineering



IT und Ich: Einführung



Nicht anbeißen – Login-Seiten als Köder



E-Mail-Sicherheit



Vishing



HORNETSECURITY

# Awareness / Phishing Simulator



## Machen!

- Cybersicherheit ist Chefsache
- Notfallplan erstellen
- Verhalten im Cybervorfall üben
- Updates & Patches immer aktuell halten
- Starke Passwörter, MFA
- Rollen- & Rechtemanagement
- Verschlüsselte Kommunikation
- Phase 1 Schwachstellenmanagement
- Phase 2 Pentesting
- Zeit und Geld in Sicherheit investieren



HORNETSECURITY

# 365 TOTAL PROTECTION

NEXT-GEN MICROSOFT 365 SECURITY

PLAN



PLAN



PLAN



PLAN



BUSINESS

ENTERPRISE

BACKUP

COMPLIANCE & AWARENESS



SPAM & MALWARE PROTECTION



ADVANCED THREAT PROTECTION



BACKUP & RECOVERY OF MAILBOXES, PLANNER & TEAMS



PERMISSION MANAGEMENT



PHISHING & ATTACK SIMULATION



COMMUNICATION PATTERN ANALYSIS



OMARC REPORTING & MANAGEMENT



EMAIL ENCRYPTION



EMAIL ARCHIVING



BACKUP & RECOVERY OF ONEDRIVE & SHAREPOINT



PERMISSION ALERTS



SECURITY AWARENESS



AI RECIPIENT VALIDATION



ENHANCED EMAIL REPUTATION & DELIVERY



EMAIL SIGNATURES & DISCLAIMERS



EMAIL CONTINUITY



BACKUP & RECOVERY OF ENDPOINTS



PERMISSION AUDIT



ESI<sup>®</sup> REPORTING



SENSITIVE DATA CHECK



EASY DNS MANAGEMENT & OPTIMISATION



HORNETSECURITY

# NEUE WÖCHENTLICHE WEBINARE



Montags

11:00 Uhr



<https://register.gotowebinar.com/rt/1465132659176518752?source=Ditpro>



Donnerstags

11:00 Uhr



<https://register.gotowebinar.com/rt/4668118882539976537?source=Ditpro>



Donnerstags

11:00 Uhr



<https://register.gotowebinar.com/rt/8193558884850603872?source=Ditpro>



HORNETSECURITY

# Titeltext

PLAN 4 PROMO-AKTION | 07.10.2024 - 31.12.2024

## 365 TOTAL PROTECTION PLAN 4

MONATLICH 8,00 € JE NUTZER IN DEN ERSTEN 12 MONATEN\*

### 365 TOTAL PROTECTION

AI-POWERED, ALL IN ONE M365 SECURITY, BACKUP & GRC

#### \*Rahmenbedingungen:

- Gilt für New Business und Cross-Sell
- Ausgenommen sind Kunden, die bereits Plan 3 (TPEB) und zusätzlich einen in Plan 4 enthaltenen Services verwenden (SAS, 3PIM, AIRV).
- Die Vertragszeitraum beträgt mindestens 12 Monate
- Dein Händler-Einkaufspreis (HEK) reduziert sich entsprechend während der initialen Promo-Laufzeit.
- Ab dem 13. Monat 10,00 € monatlich je Nutzer.

## E-MAIL SECURITY BUNDLE FÜR ON-PREMISES KUNDEN

VOM 01.10.24 BIS 31.12.24

### VORAUSSETZUNGEN

- ✓ Nur gültig für Neukunden.
- ✓ Mindestens 12 Monate Vertragslaufzeit ab Vertragsstart

### ENTHALTENE SERVICES

**ENDKUNDENPREIS: 4,50 €\***

THANK YOU!



HORNETSECURITY