



IT-Awareness Schulung.

MARVIN EQUIT • ESCHBORN, DEN 23. FEBRUAR 2024

AGENDA.

- 1 Grundlagen & Motivation
- 2 Social Engineering
- 3 Bedrohungen für Microsoft 365
- 4 Praktische Übungen
- 5 Schutzmaßnahmen
- 5 Q&A



01

GRUNDLAGEN & MOTIVATION.

WARM-UP.

Join at [menti.com](https://www.menti.com) | use code **7708 4683**

Mentimeter

Go to
www.menti.com

Enter the code

7708 4683

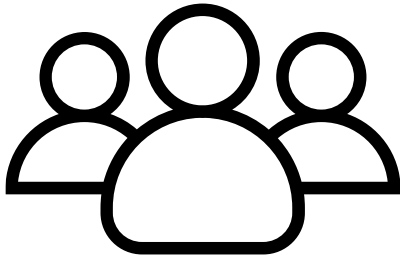


Or use QR code

DIE 3 SÄULEN VON CYBER-SECURITY.

DER MENSCH IM FOKUS

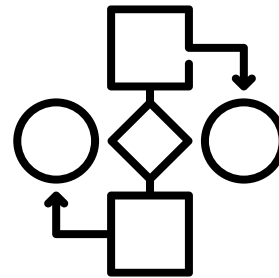
Menschen



Mitarbeiter, die in folgenden Bereichen geschult wurden:

- Erkennen und Vermeiden von Cyber-Bedrohungen, Phishing-E-Mails und andere Social-Engineering-Taktiken.

Prozesse



- Geschäfts- und IT-Prozesse, die ein Unternehmen transparenter und gesetzeskonformer machen können.
- Strategien zur proaktiven Vorbeugung für eine schnelle und effektive Reaktion im Falle eines Cybersicherheitsvorfalls.

Technology



- Tools, Software, Hardware usw. - die eingesetzt, integriert und automatisiert werden, um die schnelle Erkennung und Eindämmung von Bedrohungen zu erleichtern.

DESHALB IT-AWARENESS (1 | 2).

ES GEHT NICHT IMMER NUR UM SOFTWARE UND DATEN

Durch die einfachsten Fehler oder Unaufmerksamkeiten im Umgang mit der IT können wir schon erheblichen Schaden anrichten. Dabei schaden wir allerdings nicht unbedingt nur uns selbst:

3 Bereiche im Fokus

Kunde

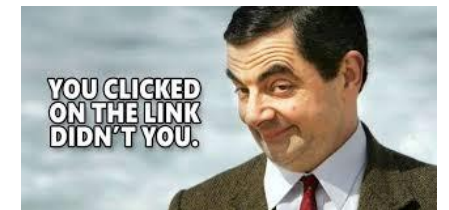
„Mitarbeiter:in verliert gesicherten Kundenlaptop von Bundesbehörde. Beiliegend: Zugangsdaten und Authentifizierungskarte“

grandega

„Mitarbeiter:in lässt Laptop ungesichert stehen und verlässt den Arbeitsplatz während die Bafin beim Kunden im Haus ist“

Mitarbeitende

„23 Personen haben ihre Privatadresse durch eine Sammel-E-Mail verraten und sich damit automatisch zu IT-Awareness Schulung angemeldet“

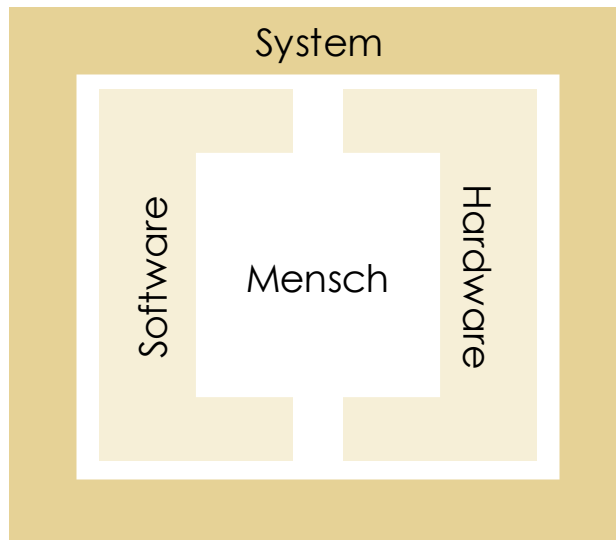


! So nutzen auch Hacker die einfachsten Unaufmerksamkeiten aus.

DESHALB IT-AWARENESS (2 | 2).

DER MENSCH IM FOKUS

Cyber-Security dreht sich nicht immer nur hochspezialisierte Hacker die Schwachstellen in einer Software ausnutzen. Der einfachste Weg in ein System zu kommen, geht über Menschen, die mit dem System arbeiten.



48% der Unternehmen erlebten ca. 4-9 erfolgreiche Phishing Angriffe 2021¹

74 % aller Sicherheitsverletzungen werden durch Menschen verursacht, entweder durch Fehler, Missbrauch von Berechtigungen, Verwendung gestohlener Zugangsdaten oder durch Social Engineering.²

90 % der Cyberangriffe zielen auf die Mitarbeiter eines Unternehmens ab.³

! Für menschliches Versagen, müssen zwei Faktoren vorhanden sein: Gelegenheit und Entscheidung.

¹ Quelle: Statista <https://www.statista.com/statistics/1149219/share-organizations-worldwide-phishing-attack-country/>, ² Quelle: Verizon: <https://www.verizon.com/business/resources/reports/dbir/>

³ Quelle: Arctic Wolf: <https://arcticwolf.com/state-of-cybersecurity-2022-trends/>

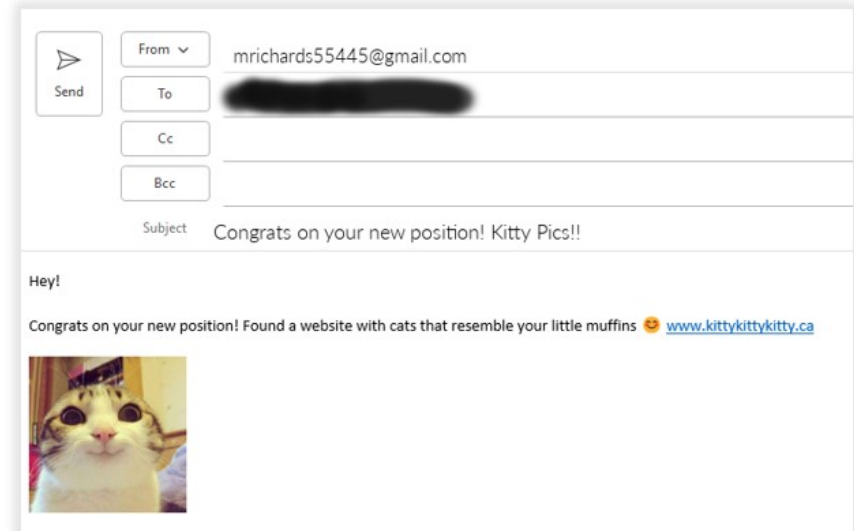
BELIEBTE ANGRIFFE (1 | 4).

HACKEN FUNKTIONIERT ANDERS ALS IM FILM

Vorstellung



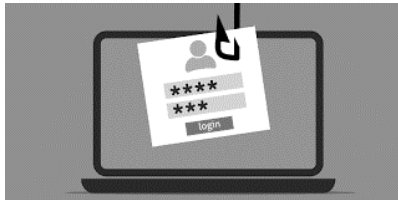
Realität



BELIEBTE ANGRIFFE (2 | 4).

DIE TOP 3

Phishing



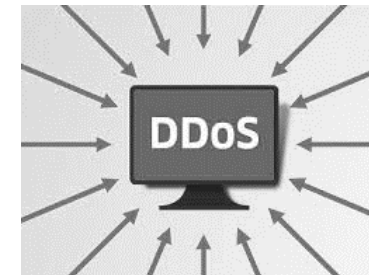
Phishing-Angriffe sind eine Form des Social Engineering, bei der Angreifer versuchen, sensible Informationen wie **Anmeldeinformationen** oder **Finanzdaten** durch Täuschung zu erlangen

Ransomware



Ransomware ist eine Art von Malware, die **Daten** auf dem Computer eines Opfers **verschlüsselt** und ein **Lösegeld** für die Entschlüsselung fordert.

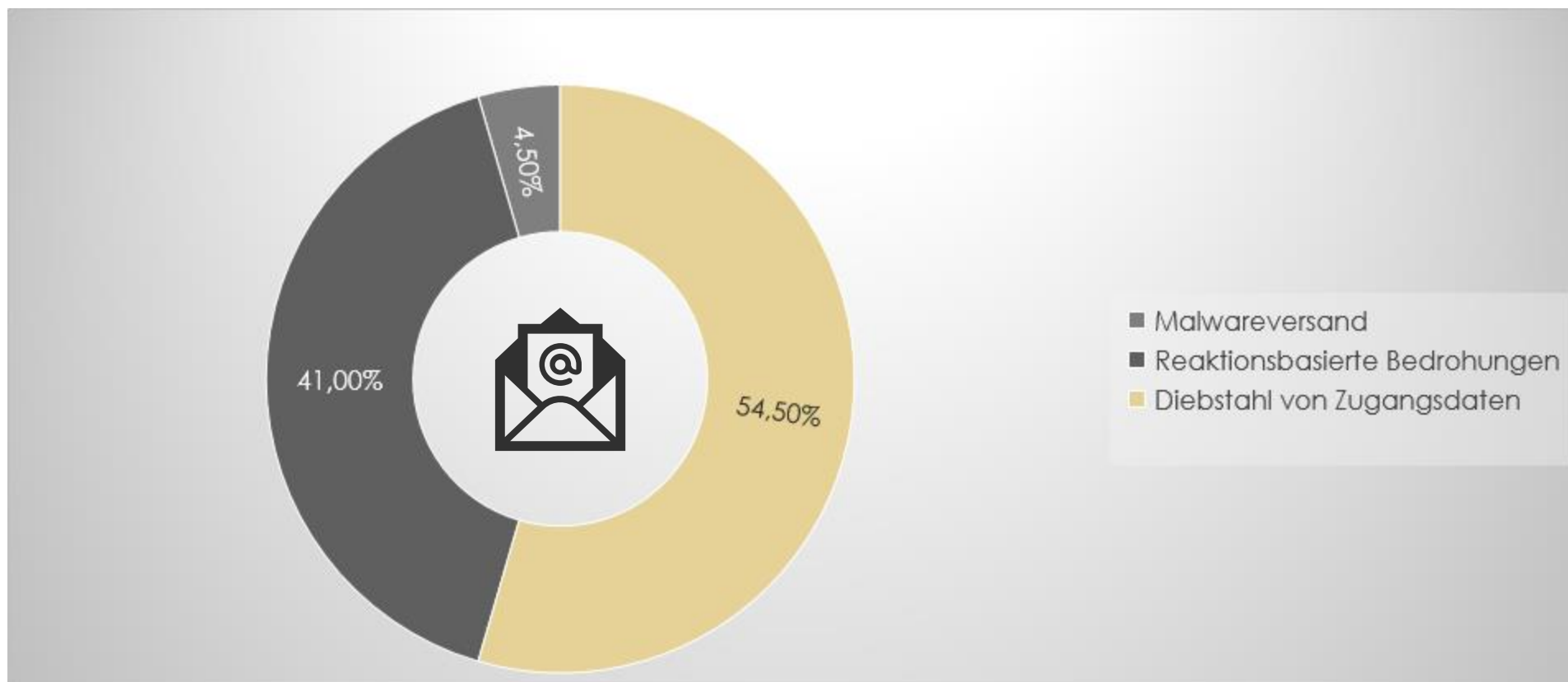
DDos-Attacken



Distributed Denial of Service (DDoS)-Attacken sind Cyberangriffe, bei denen zahlreiche kompromittierte Systeme genutzt werden, um ein einzelnes Ziel, typischerweise einen Server oder eine Website, mit einer **Flut von Anfragen zu überlasten**.

BELIEBTE ANGRIFFE (3 | 4).

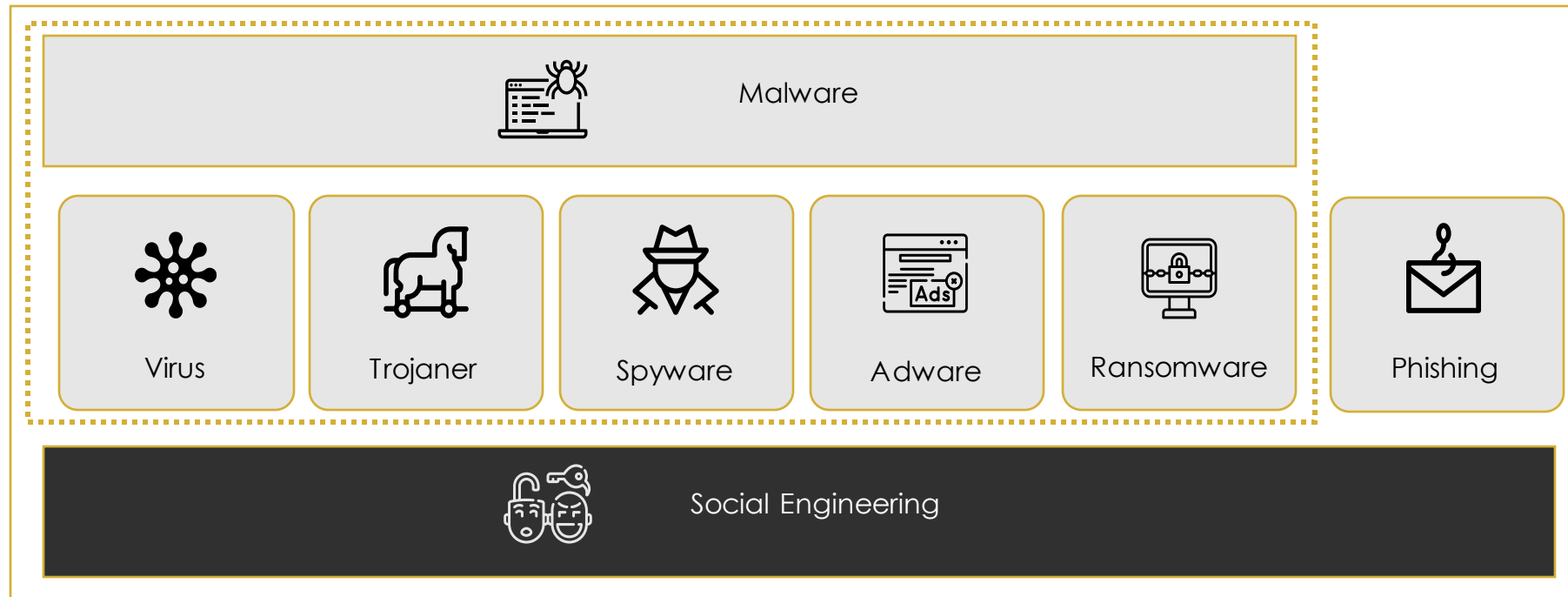
DER DREH UND ANGELPUNKT IST UND BLEIBT DIE E-MAIL



 **Diebstahl von Zugangsdaten macht weiterhin den Größten Sektor an Bedrohungen aus.**

BELIEBTE ANGRIFFE (4 | 4).

MALWARE UND SOCIAL ENGINEERING KOMMEN SELTEN ALLEIN



! Mit Hilfe von Social Engineering kann Malware in Unternehmen oder in Organisationen verbreitet werden.

02

SOCIAL ENGINEERING.

SOCIAL ENGINEERING.

DIE EFFEKTIVSTE METHODE FÜR HACKS

Durch verschiedene Methoden wird versucht, das Vertrauen einer bestimmten Person zu erhalten. Bei einer erfolgreichen Attacke wird das Opfer wichtige Daten (Login-Namen und Passwörter sind ein zentrales Beispiel) preisgeben.



Social Engineering

Social Engineering ist ein Verfahren, um Vertrauen zu schaffen oder relevante Daten durch Ausnutzung menschlicher Komponenten in Erfahrung zu bringen.

Menschliche Eigenschaften, die oft beim Social Engineering ausgenutzt werden

Hilfsbereitschaft

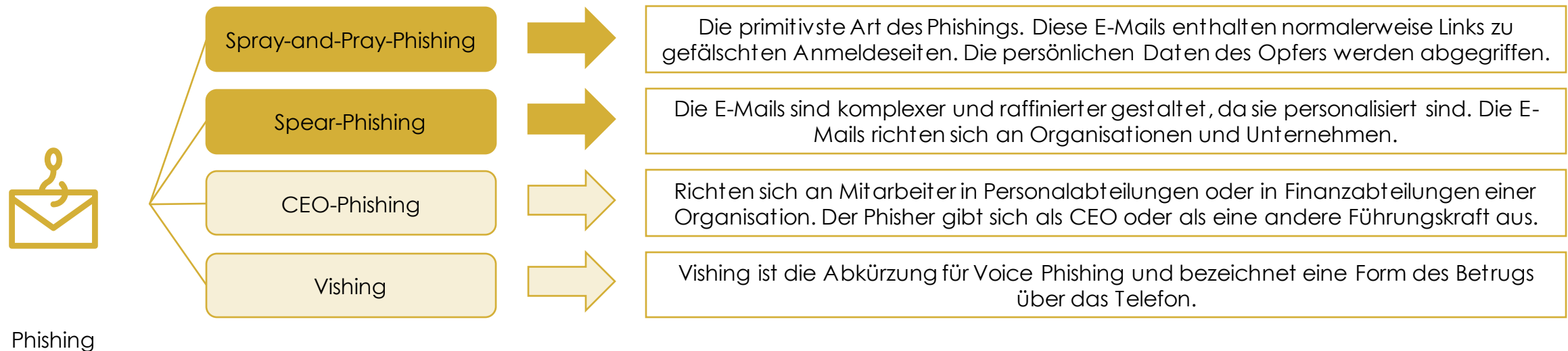
Neugier

Autorität

PHISHING (1 | 2).

DIE PHISHING-ARTEN ZUR BESCHAFFUNG VON ZUGANGSDATEN

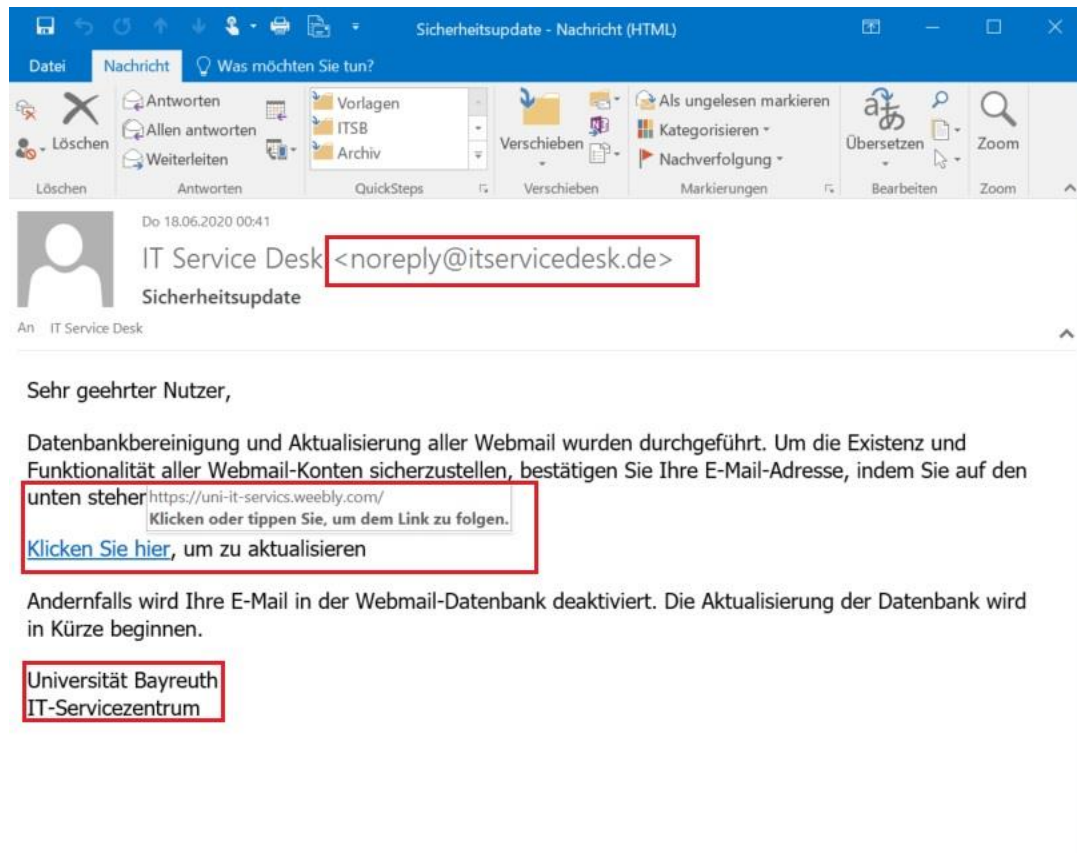
Ziel ist die illegale Beschaffung von Zugangsdaten. Dabei verwenden Angreifer Phishing-E-Mails, um präparierte Links oder Anhänge zu verbreiten



 Die meisten Phishing Angriffe brauchen keine 10 Minuten zur Vorbereitung.

PHISHING (2 | 2).

PRAXISBEISPIEL



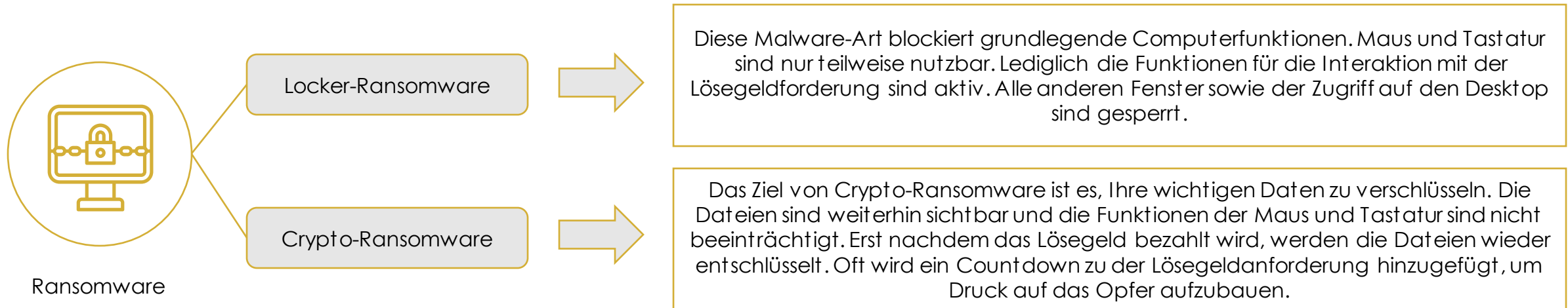
Genereller Aufbau von Phishing Mails:

- Anrede
- Grund der Mailv erschickung
- Notwendigkeit zum Handeln
- Link oder alternativ Dateianhang.
- Zeitdruck
- Konsequenzen, wenn ihr nicht handelt
- Angeblicher Absender

RANSOMWARE (1 | 3).

DIE AM HÄUFIGSTE VERWENDETE MALWARE

Ransomware sind Schadprogramme, die den Computer sperren oder darauf befindliche Daten verschlüsseln. Die Täter erpressen ihre Opfer, in dem sie den Bildschirm oder die Daten des Opfers nur nach einer Lösegeldzahlung wieder freigeben.



 Bei der Ransomware Attacke werden die Daten des Opfers „gekidnappt“ und erst nach Bezahlung eines Lösegelds freigegeben.

RANSOMWARE (2 | 3).

PRAXISBEISPIEL

Die BKA-Trojaner sind zahlreiche verschiedene Trojaner, die aber alle nach demselben Muster arbeiten. Die Ransomware sperrt den Rechner und blendet ein Bild mit einer angeblich von der Bundespolizei (ehemals Bundesgrenzschutz) oder dem Bundeskriminalamt (BKA) stammenden Nachricht ein



! Ransomware läuft in der Regel immer nach diesem Muster ab.

RANSOMWARE (3 | 3).

PRAXISBEISPIEL

WannaCry war ein Ransomware-Angriff, der sich im Jahr 2017 in über 150 Ländern ausbreitete. Er war so konzipiert, dass er eine Sicherheitslücke in Windows ausnutzte, die von der NSA erschaffen und durch die Hackergruppe Shadow Brokers geleakt wurde. Die Nutzer wurden ausgesperrt und es wurde ein Lösegeld in Form von Bitcoin verlangt.



KEY FACTS

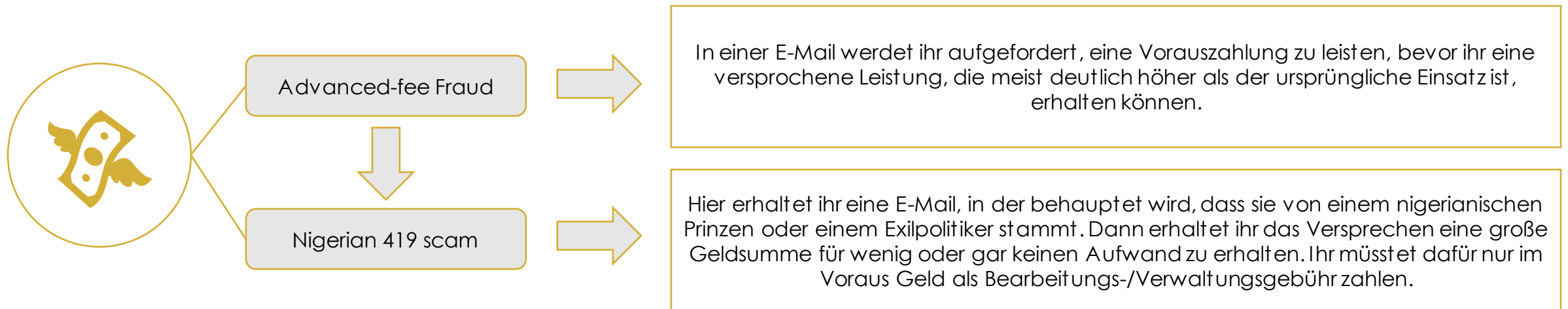
- Infektion von mehr als 230.000 Windows-PCs in über 150 Ländern an einem Tag
- WannaCry die am meisten verbreitete Ransomware-Angriffe bisher.
- Mai 2017 veröffentlicht
- Der weltweite finanzielle Schaden durch WannaCry betrug ca. 4 Milliarden US-Dollar.

! WannaCry verursachte allein bei der National Health Service (NHS) einen Schaden von über 107 Millionen Euro

REAKTIONS-BASIERTE ANGRIFFE.

DER VORSCHUSS-BETRUG

Bei einer reaktionsbasierten Bedrohung reagieren Opfer über einen ausgewählten Kommunikationskanal auf verschiedene Methoden wie Advance Fee Scams (Vorschussbetrug), bei dem Opfer vorab eine Zahlung leisten, um eine größere Geldsumme zu erhalten – auch bekannt als 419- oder nigerianischer Betrug.



! Durch den immensen Unterschied zwischen der Anzahlungs- und versprochenen- Summe ist der Scam so erfolgreich.

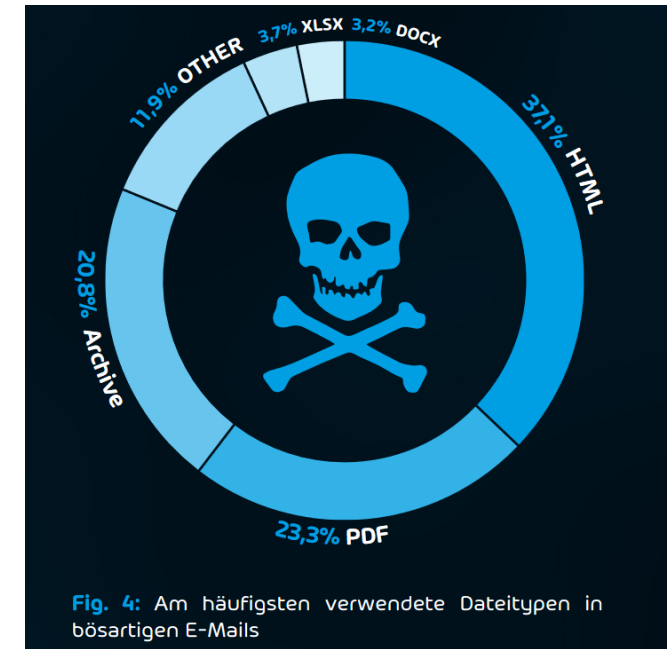
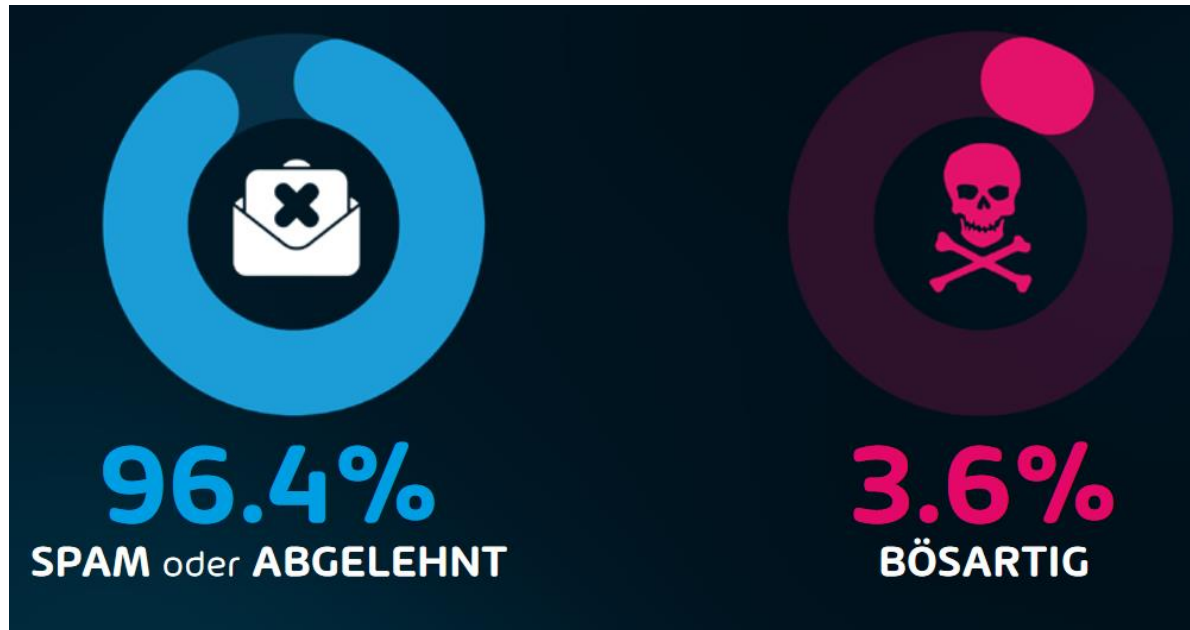


BEDROHUNGEN FÜR MS 365.

E-MAILS.

MICROSOFT KANN LEIDER NICHT ALLE SCHÄDLICHEN MAILS BLOCKIEREN

Auch wenn Microsoft verschiedene Sicherheitsmaßnahmen einsetzt, um verdächtige E-Mails zumindest in den SPAM-Ordner zu werfen, klappt eine Kategorisierung leider nicht immer.

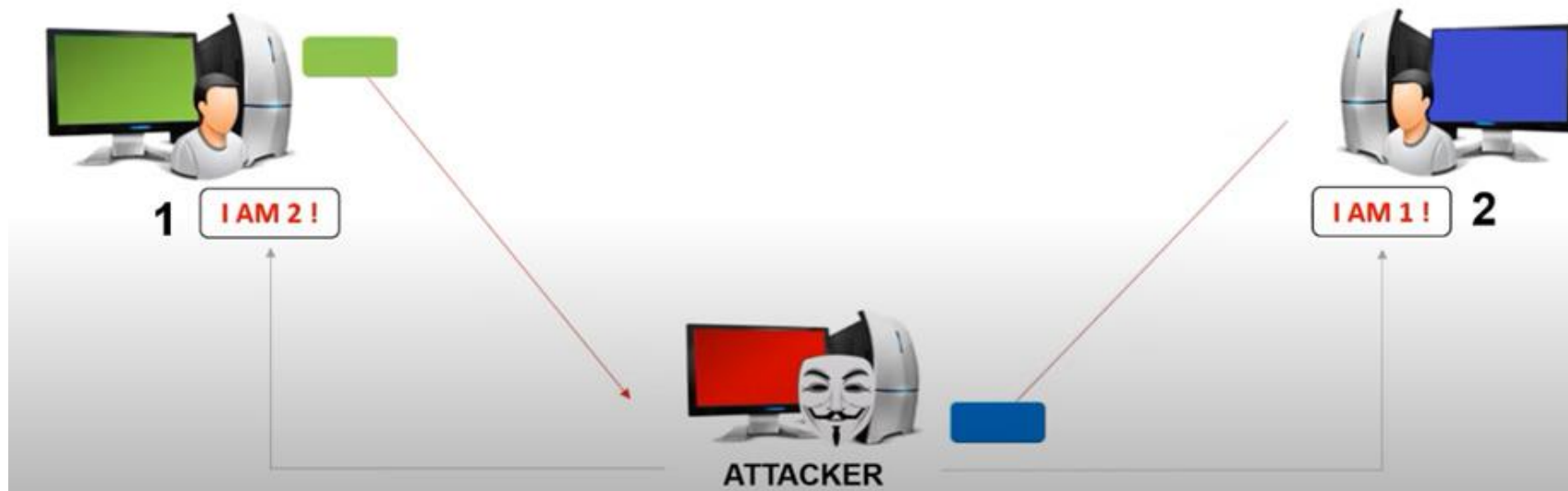


 **Behaltet deshalb eure E-Mails immer im Blick.**

MFA-BYPASS-ANGRIFFE.

MIT EINER ZWEI-FAKTOR-AUTHENTIFIZIERUNG IST EIGENTLICH ALLES TUTTI FRUTTI ODER?

Diese Art von ALTM-Angriff überwacht die MFA-Abfrage nahtlos, fängt dann den Antwortcode des Benutzers ab und leitet ihn an die eigentliche Anmeldeseite weiter. Das Endergebnis ist, dass der Benutzer nicht weiß, dass er kompromittiert wurde, während der Angreifer nun vollen Zugriff auf das Benutzerkonto hat.



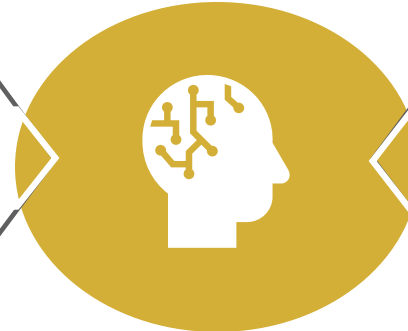
! Anfällig sind hier vor allem öffentliche WLAN- Netzwerke.

DIE ROLLE VON KI.


ALLES HAT SEINE VOR- UND NACHTEILE



- Weniger erfahrene Angreifer nutzen generative KI nicht nur für Angriff, sondern können von ihr sogar lernen, WIE man solche Angriffe durchführt
- Darkweb-Varianten von ChatGPT werden Teile von Angriffsketten verbessern & automatisieren.
- Unerfahrene Angreifer erhöhen Ihre Geschwindigkeit von Cyberangriffen.
- Die Fähigkeit von LLMs, Texte glaubwürdig in andere Sprachen zu übersetzen, eröffnet Kriminellen auch „neue Märkte“.



- Generative KI ist kein Allheilmittel
- Unerfahrene Angreifer, die Tools wie ChatGPT für Angriffe nutzen wollen, müssen immer noch viel Zeit investieren, um die gesamte Angriffskette für einen bestimmten Angriff zu verstehen
- Sicherheitsexperten und Anbieter setzen generative KI auch für die Verteidigung ein

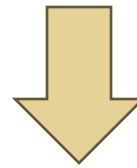
 **Durch ein frühzeitiges Alignment von Vorstellungen können spätere Konflikte vermeiden werden.**

CLOUD SERVICES.

EIN SYSTEM FÜR ALLE

Wenn es um die Ihre Systeme geht, bietet Microsoft hervorragende Sicherheitsmaßnahmen an, allerdings macht die Größe und der Umfang der Microsoft Cloud sie zu einem besonders lukrativen Ziel für Cyberkriminelle.

Angreifer wissen, dass das Überlisten der Exchange Online Protection eines einzelnen Kunden höchstwahrscheinlich bedeutet, dass mit der gleichen Methode ALLE M365-Kunden überlistet werden können.



So gab es im Mai 2023 einen Zugriff auf die Microsoft Cloud (Exchange Online) durch die mutmaßlich staatsnahe chinesische Hackergruppe Storm-0558. Offiziell bekannt ist, dass dabei E-Mail-Konten von 25 Organisationen gehackt wurden, darunter auch das US-Außenministerium.



ÜBUNGEN.

Join at [menti.com](https://www.menti.com) | use code 7708 4683

 Mentimeter

Go to
www.menti.com

Enter the code

7708 4683



Or use QR code



KERNPUNKTE.

WAS WIR AUS DEN ÜBUNGEN MITNEHMEN

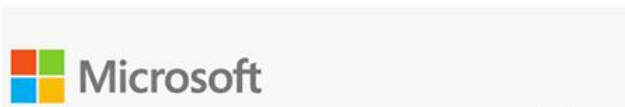
- Achtet bei Emails immer auf den Roten Balken „Externe E-Mail-Adresse“ => ist bei „internen“ E-Mails schonmal schlecht
- Microsoft sendet euch keine E-Mails zu Account-Daten
- Bei Websites immer auf die URL achten
- Achtet auf die tatsächlichen Links und Buttons

Hi User,

There are some pending new files shared with you by a contact and you need to retrieve them to enable you view it.

<https://x.co/f4zbq4u/?z=<<email>%3hdo>
Click or tap to follow link.

Retrieve New Document



From: Microsoft Team Brand Impersonation <MSteam@emailsupport.co>

To: Jim Halpert <jhalpert@paperco.com>

Subject: Urgent action required Urgency



Hi Jim,

Your mailbox size has been exceeded.

To continue using your mailbox you must upgrade Content: Account Restriction to your extra 10GB plan without any charges.

Just click here

Upgrade Mailbox Size

Suspicious Link

Thanks,
Microsoft 365 Team

EXKURS: SAFE-LINKS.

OUTLOOK ÜBERPRÜFT LINKS AUCH AUTOMATISCH

Wenn ihr Nachrichten mit Links zu Webseiten erhaltet, überprüft Outlook.com, ob die Links im Zusammenhang mit betrügerischen Phishing-Versuchen stehen oder ob sie wahrscheinlich Viren oder Schadsoftware auf Ihren Computer herunterladen

Wir haben leider Unstimmigkeiten in den aktuellen Adressen im System, wäre gut wenn deine Daten kurz hier eintragen und schicken könntest;

<https://eur03.safelinks.protection.outlook.com/?url=https%3A%2F%2Fforms.office.com%2F%2FrF25PS0fin&data=05%7C02%7Cmarvin.equity%40grandega.de%7C115d5501d31947a0103208dc17655da6%7C559ebc091a394ca28d7cd67cd4f14962%7C0%7C0%7C638410971344030107%7CUnknown%7CTWFpbGZsb3d8eyJWljoIMC4wLjAwMDAiLCJQIjoiV2luMzliLCJBTil6lk1haWwiLCJXVCi6Mn0%3D%7C3000%7C%7C%7C&sdata=XWzr%2BxVQtbVle7gShAuKvPha%2FFF8ZXL8vo5Rzb6SbXk%3D&reserved=0>

Danke!

Grüße
Stefan

 Aber auch das funktioniert nur begrenzt.

05

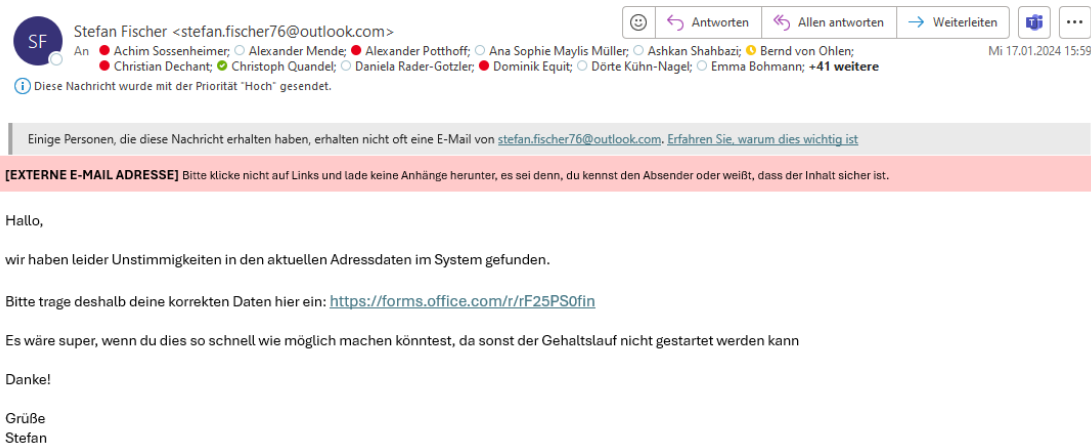
SCHUTZMAßNAHMEN.

VERHALTENSWEISE BEI PROBLEMEN (1 | 2).


E-MAILS

Der Hauptpunkt in dem Angreifer in unser System kommen können und auf den ihr am meisten achten solltet, sind die guten alten E-Mails.

Fehlende Adressdaten im System



- Öffnet keine Anhänge
- Fragt über Teams nach, ob der Absender wirklich die E-Mail geschrieben habt
- Gebt Stefan Bescheid wenn euch etwas merkwürdig vorkommt

 Keine E-Mail ist so dringend, um nicht zweimal hinschauen zu können

VERHALTENSWEISE BEI PROBLEMEN (2 | 2).

COMPUTER VERHÄLT SICH KOMISCH

Nach einem Virus treten meist Punkte auf, an denen sich euer Computer merkwürdig verhält.

Merkmale

- Euer Gerät wird langsamer
- Häufiges abstürzen oder einfrieren
- Unerwartete Pop-up-Fenster
- Fehlende oder infizierte Dateien
- Unbekannte Anwendungen und Programme
- E-Mail-Konto sendet Nachrichten, die nicht von euch sind

Verhaltensweise

- Beendet eure OneDrive
- Startet einen System-Scan mit unserem Anti-Virus Programm „Bitdefender“
- Gebt Stefan Bescheid



 Manche Viren zeigen sich jedoch nicht immer, deshalb ist ein regelmäßiger System-Scan wichtig.

MÖGLICHKEITEN SICH ZU SCHÜTZEN.

JEDER KANN ETWAS DAZU BEITRAGEN SICH UND grandega ZU SCHÜTZEN



Update



Passwort

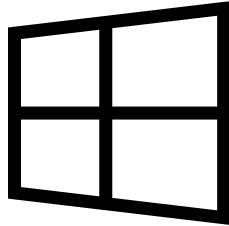


Aufmerksam sein

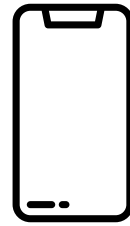
UPDATE.

NEU IST IMMER BESSER (AUßER ES IST WINDOWS 11)

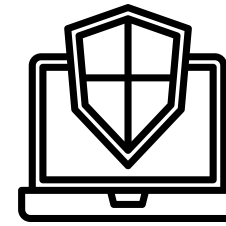
Alle Anwendungen auf einem PC oder auf einem Endgerät sollten aktuell gehalten werden. Aktuelle Software trägt maßgeblich zur Verbesserung der IT-Sicherheit bei. Updates von Betriebssystemen, Endgeräten, Antiviren Programmen sowie Firewalls werden oft als Belästigung gesehen und deshalb oft vernachlässigt. Mit diesem Verhalten ist die Wahrscheinlichkeit höher ein Opfer eines Cyberangriffs zu sein.



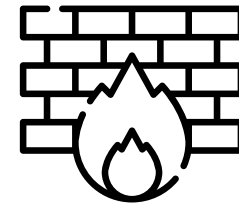
Betriebssysteme




Endgeräte



Antivirus



Firewall

 Bei der Vernachlässigung von Updates einzelner Personen, werden ganze Unternehmen und Organisationen gefährdet.

PASSWORT.

AUCH PASSWORT-MANAGER KÖNNEN HILFREICH SEIN

Stellen Sie sicher, dass Sie starke Passwörter verwenden, die niemand erraten oder abschauen kann. Am besten, Sie benutzen gleich einen seriösen Passwortgenerator, um nach dem Zufallsprinzip starke Passwörter zu generieren und sicher zu speichern.

Do's

- Passwörter sollten mindestens acht Zeichen lang sein
- Groß- und Kleinbuchstaben verwenden
- Sonderzeichen wie ?, !, %, +, _, etc. nutzen
- Mehrere Ziffern hinzufügen

Dont's

- Passwörter Kombinationen vermeiden, die Geburtstage bzw. Namen des Haustiers enthalten oder in einem Wörterbuch stehen.
- Auf gängige Wiederholungs- und Tastaturmuster wie asdf, 1234, abcd, 666, etc. verzichten.
- Nicht ein simples Passwort wählen, das nur um ein Sonderzeichen am Wortanfang oder -ende ergänzt ist, zum Beispiel: !Pizza.

Tipp

Unter folgende Portale ist es möglich zu überprüfen, ob eure Zugangsdaten im Netz kursieren:

<https://sec.hpi.de/ilc/>
<https://haveibeenpwned.com/>

 **Zugangsdaten werden von Cyber-Kriminelle, nach Angriffen, oft im Internet veröffentlicht oder zum Kauf angeboten.**

AUFMERKSAM SEIN.

MANCHMAL SIND ES NUR KLEINIGKEITEN



E-Mails hinterfragen, ob sie wirklich valide sind, wenn sie eine Aktion verlangen



Verwendet keine externen Medien, die ihr nicht kennt.



Vermeidet möglichst öffentliche WLAN-Netzwerke



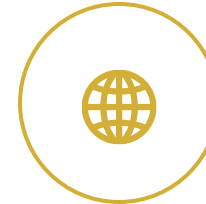
Fragt Stefan wenn euch was komisch vorkommt



Benutzt die Zweifaktor-Authentifizierung



Beim verlassen des Arbeitsplatzes, sollte das Arbeitsgerät gesperrt werden.



In den sozialen Netzwerken sollen keine sensiblen Informationen gepostet werden.



Lasst keine Zugangsdaten offen oder an eurem Laptop herumliegen

 **Jeden Nutzer sollte bewusst sein, dass er zu jederzeit ein Angriffsziel sein kann.**

DAS MACHT grandega.

WIR VERSUCHEN VIEL, ABER ALLES KLAPPT LEIDER NICHT IMMER

Technik

- Alle E-Mails außerhalb des Unternehmens werden mit einem **roten Banner** versehen.
- E-Mails die mit einem Namen von einem unserer Mitarbeiter:innen gesendet werden, werden größtenteils direkt **blockiert**
- Back-up der grandega Dokumente
- Updates sind nicht mehr optional und müssen nach 3 Tagen durchgeführt werden
- Bitdefender versendet automatisch E-Mails an die IT wenn eine Bedrohung festgestellt wurde
- **Zweifaktor-Authentifizierung**
- Safe-Links in Outlook



Menschen


- Phishing-Simulationen zum Erkennen von böartigen E-Mails
- Prozesse für Verhaltensweisen bei Problemen
- Schulungen
- IT-Support der immer zur Stelle ist
- Wir verschicken nur Links und keine Anhänge

 Bis ist grandega noch vor größeren Attacken verschont geblieben, aber dennoch: Vorsicht ist besser als Nachsicht.



OFFENE FRAGEN.

grandega

 Rahmannstraße 11
D-65760 Eschborn

 info@grandega.de

 www.grandega.de

DANKE. 