FPM #1
GALAXUS FAKE MAIL

Report & Statistik

96	0	0	0
100%	**0%**	**0%**	**0%**
Email Sent	**Email Opened**	**Clicked Link**	**Submitted Data**
Alle geplanten Fake Emails wurden erfolgreich versendet.	Niemand hat die Fake Email geöffnet	Niemand hat auf dem im Fake Mail enthaltenen Link geklikt	Niemand hat Daten eingegeben

REASONS OF NO CLICKING

REASON 1
Absender "hallo@galaxus.ch" sehr Fragwürdig

REASON 2
"Jana Doe" als Verfasser ebenso fragwürdig

REASON 3
"Gratis Geschenk" hat viele abgeschreckt

REASON 4
Formatierung der Mail nicht Professionell & Schreibfehler

LOOKIN' GOOD!

Die Mitarbeiter sind für Auffällige Mails sensibel!

REPORTED EMAILS

In der folgenden Grafik kann eingesehen werden, wie mit den Fake Phishing Mail umgegangen wurde. Die Mitarbeiter können die Email bei sicherheit und unsicherheit der IT melden, oder direkt löschen. Erkennbar ist, dass es allen Aufgefallen ist, dass es SPAM war. Entweder wurde die Email direkt gelöscht, oder als "FYI SPAM" an die IT weitergeleitet.

EMAILS REPORTED "SPAM!"

13
Mitarbeiter erkannten die Mail sofort als SPAM

EMAILS REPORTED "SPAM?"

0
Mitarbeiter war sich unsicher ob das SPAM war

EMAIL DIRECTLY DELETED

83
Mitarbeiter löschten die Email direkt

Jana Doe (digitec.ch)

26. Mar. 2024, 16:41 MEZ

Hi Jessica

Erstmals Danke für Deine Treue!

Dank Deiner Jahrelanger treue haben wir für Dich ein Geschenk bereitgelegt!

Zögere nicht so schnell als möglich Dein Geschenk zu sichern! Äs het solangs het!

Klicke HIER um Dein Geschenk abzuholen!

Freundliche Grüsse

Janna Doe
After Sales Operations Expert

Für Fragen und Hilfe: https://helpcenter.digitec.ch/hc/de

Galaxus Mobile für Firmenkunden

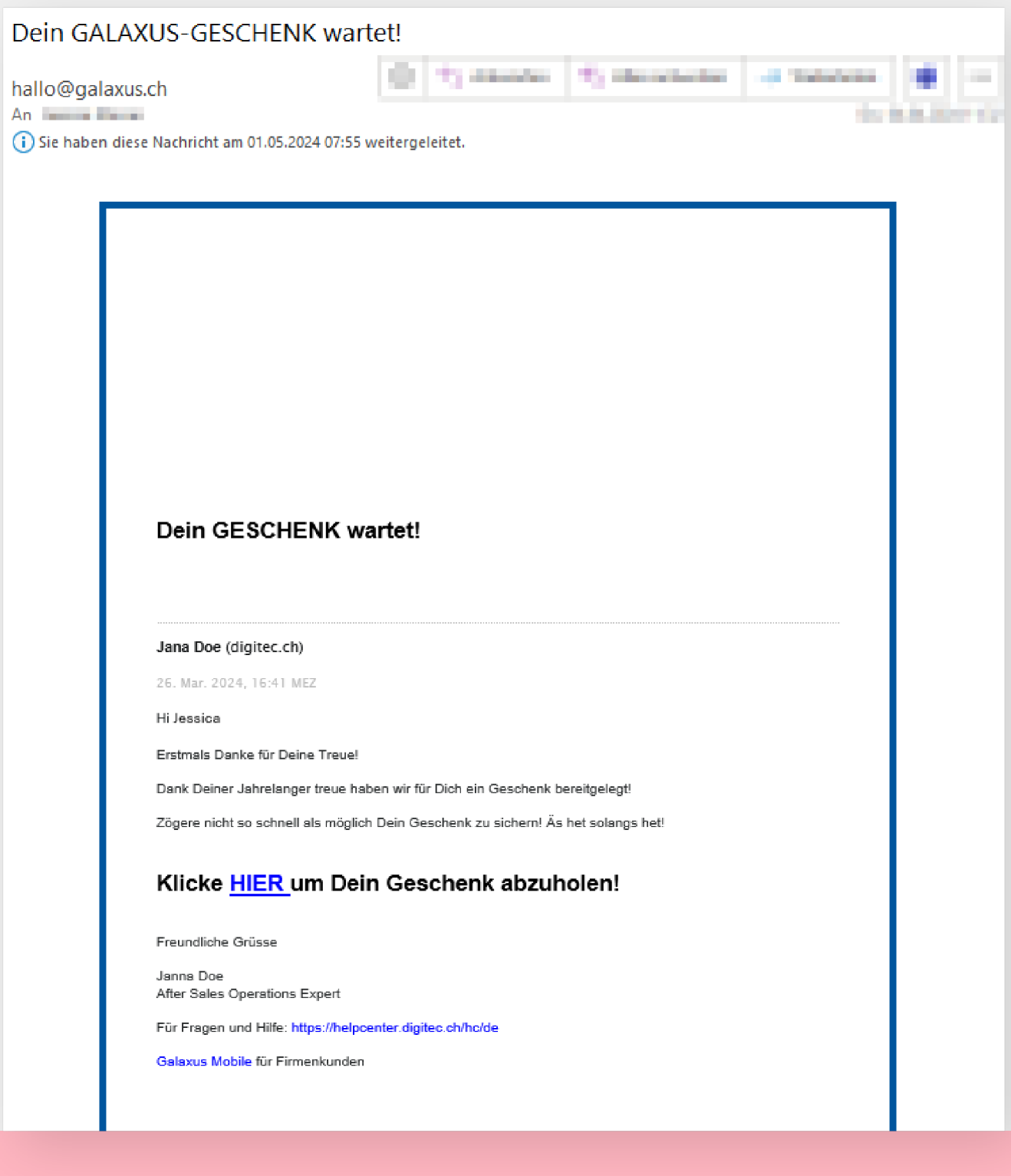
Fazit:

Auffällige Phishing-Mails zu erkennen sind für Mitarbeiter kein Problem!

FPM
Die drei Fake Mails

Erkennen & Handeln

Fake Phishing Mail #1
GALAXUS-FAKE



LOOKIN' WEIRD!

AUF WAS MUSS ICH ACHTEN?

Hier siehst Du die eingebauten Fehler in der Galaxus Fake Mail

Jana Doe (digitec.ch)

Jana Doe?

Sind wir hier in einem Kriminalfall?

Dein GALAXUS-GESCHENK wartet!

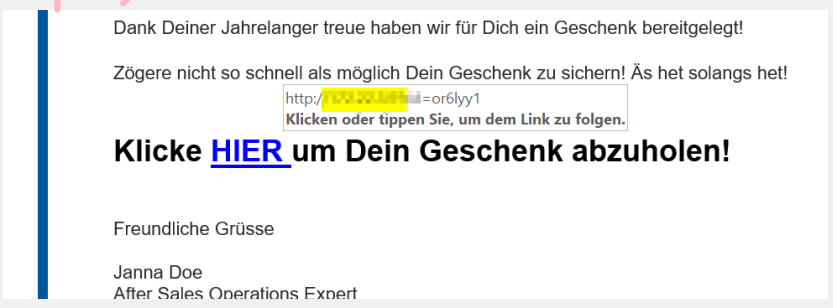
hallo@galaxus.ch
An Jessica Storrer

Galaxus hat wahrscheinlich keine solche Emailadresse..

Sonst: **Via offizieller Website eine Anfrage machen ob Email legitim ist**

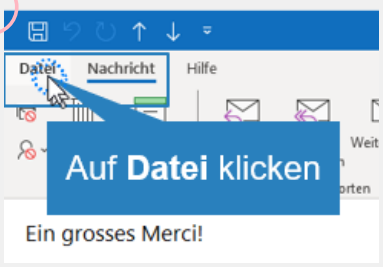
Komische Internetseite..?

(Fahre mit der Maus über den Link -nicht klicken, nur fahren - um zu sehen wo der hinführt)

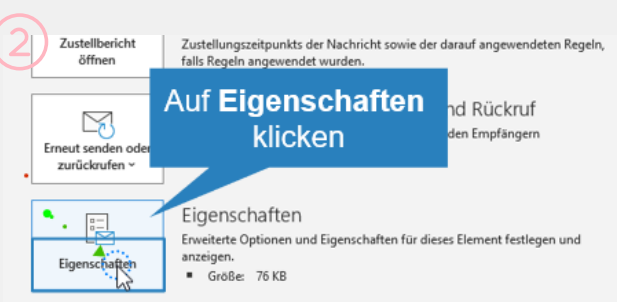


Absenderadresse genau überprüfen:

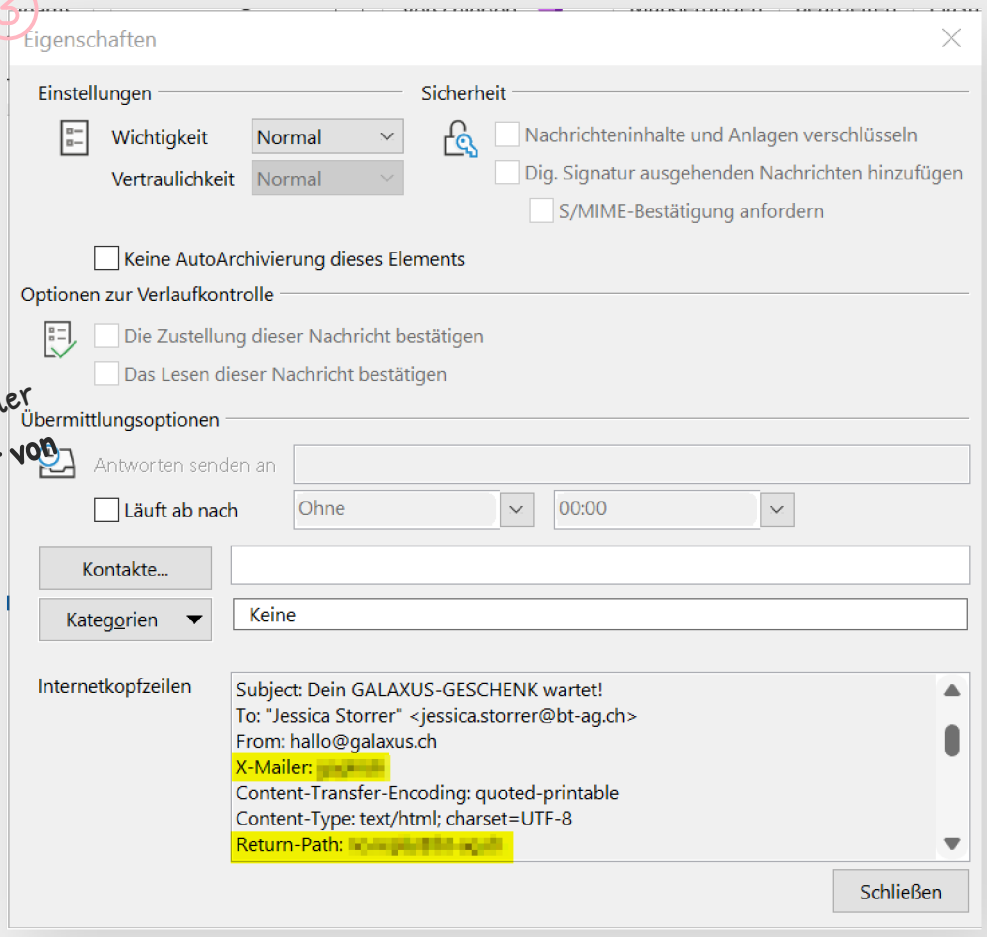
1. Auf **Datei** klicken



2. Auf **Eigenschaften** klicken



3. Hier kann unter ReturnPath und X-Mailer eingesehen werden, dass der Absender von einer komischen Adresse war!



FPM #2
Microsoft FAKE MAIL

Report & Statistik

56	1	1	0
100%	**1%**	**1%**	**0%**
Email Sent	**Email Opened**	**Clicked Link**	**Submitted Data**
Alle geplanten Fake Emails wurden erfolgreich versendet.	Jemand hat das Email geöffnet	Diese Person klickte ebenso auf den Link	Aber es wurden keine Daten eingegeben! Bravo!

REASONS OF NO CLICKING

REASON 1
Anfrage nach Passwortänderung sah suspicious aus

REASON 2
Datum des verlangten Passwortwechsels war in der Vergangenheit

REASON 3
Fehler in der Rechtschreibung der Email

REASON 4
Domain Schreibefehler miCORsoft statt miCROsoft

LEARN MORE!
mjcybersecurity.com

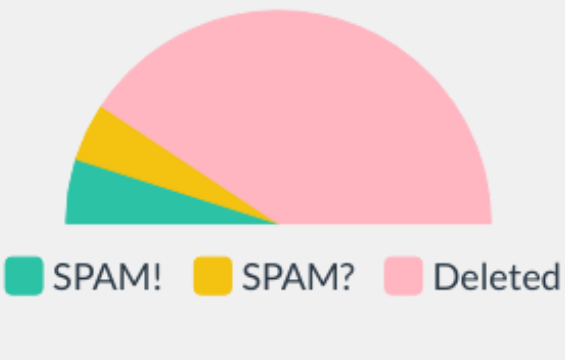
LOOKIN' GOOD!

Die Mitarbeiter haben keine Daten eingegeben!

REPORTED EMAILS

In der folgenden Grafik kann eingesehen werden, wie mit den Fake Phishing Mail umgegangen wurde. Die Mitarbeiter können die Email bei Sicherheit und unsicherheit der IT melden, oder direkt löschen. Erkennbar ist, dass bei dieser Fake Phishing Mail die Mitarbeiter schon unsicherer waren.

Die Mitarbeiter fragen nach wenn sie unsicher sind!



EMAILS REPORTED "SPAM!"

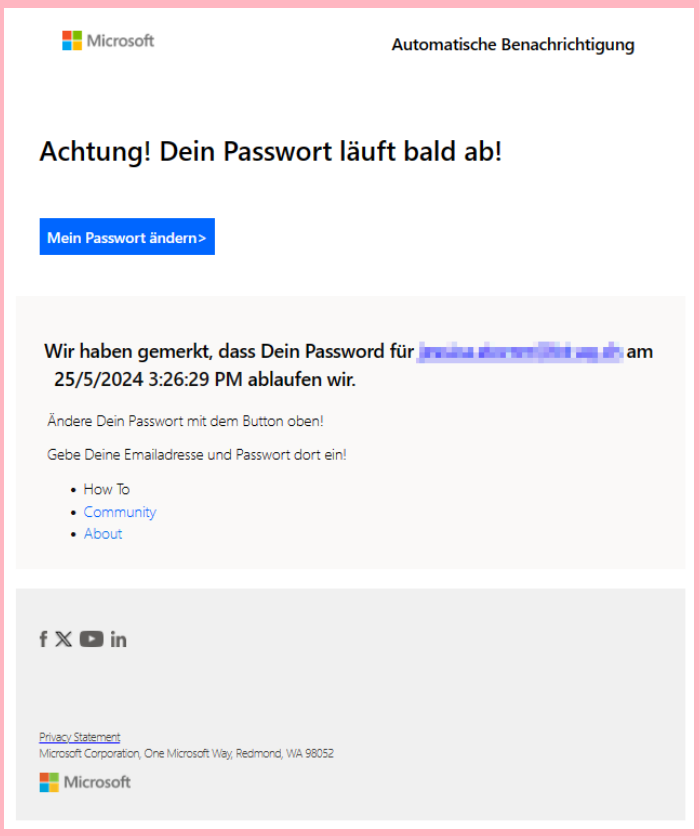
10
Mitarbeiter erkannten die Mail sofort als SPAM

EMAILS REPORTED "SPAM?"

9
Mitarbeiter war sich unsicher ob das SPAM war

EMAIL DIRECTLY DELETED

36
Mitarbeiter löschten die Email direkt


Microsoft

Automatische Benachrichtigung

Achtung! Dein Passwort läuft bald ab!

Mein Passwort ändern>

Wir haben gemerkt, dass Dein Password für [redacted] am 25/5/2024 3:26:29 PM ablaufen wir.

Ändere Dein Passwort mit dem Button oben!

Gebe Deine Emailadresse und Passwort dort ein!

- How To
- Community
- About

Privacy Statement
Microsoft Corporation, One Microsoft Way, Redmond, WA 98052

Microsoft

Fazit:

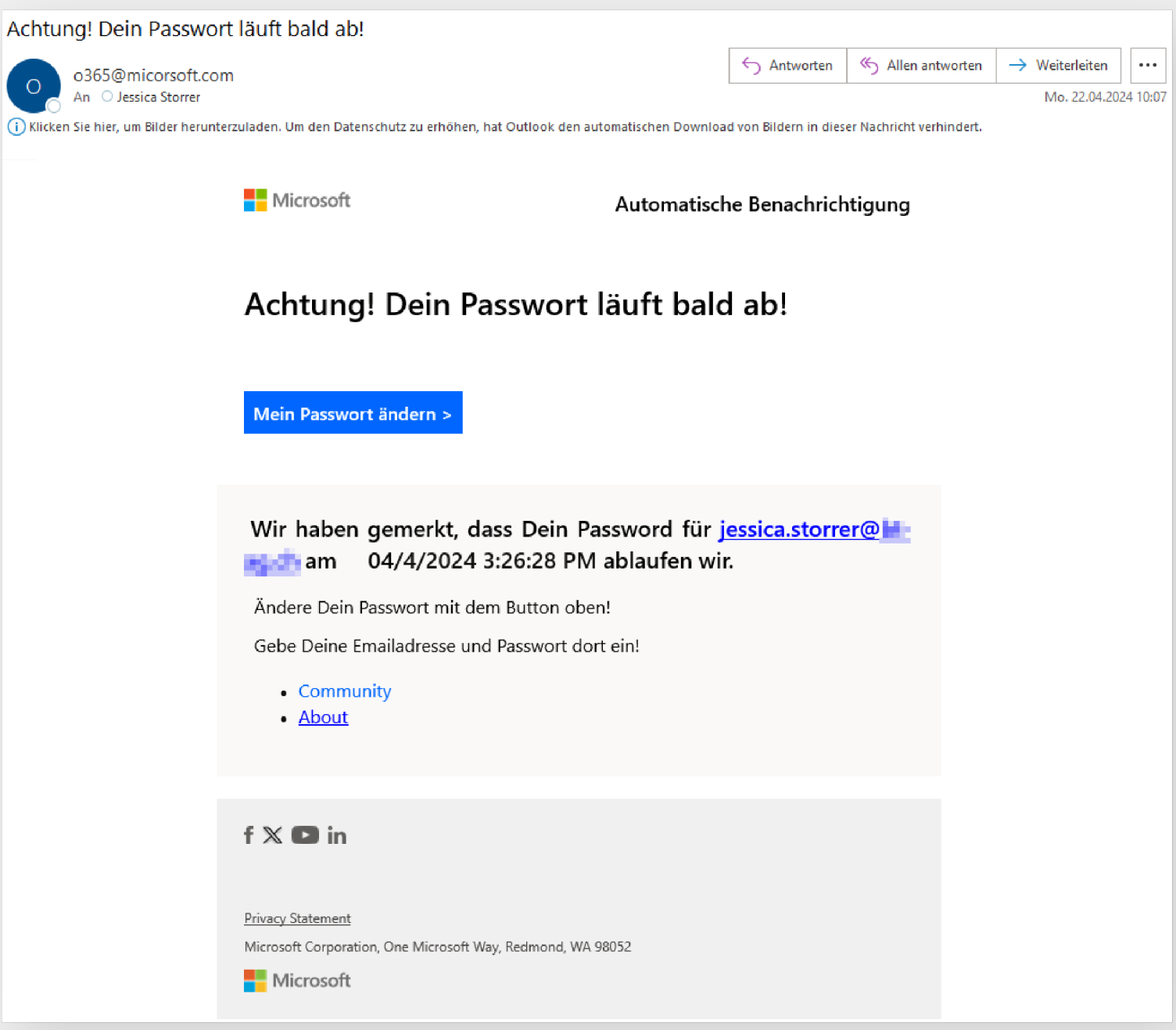
Mitarbeiter reagieren sensibel und fragen nach, ob es sich um SPAM handelt!

LEARN MORE!
mjcybersecurity.com

FPM
Die drei Fake Mails

Erkennen & Handeln

Fake Phishing Mail #2
MICROSOFT-FAKE



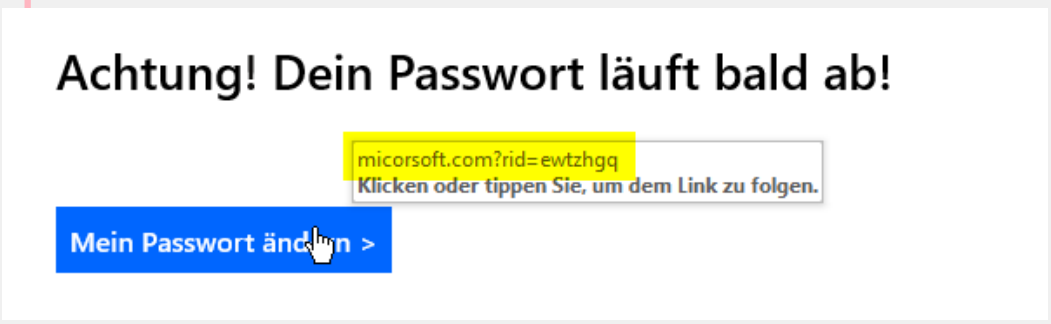
LOOKIN' WEIRD!

AUF WAS MUSS ICH ACHTEN?

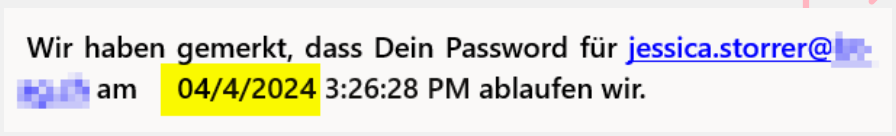
Hier siehst Du die eingebauten Fehler in der Microsoft Fake Mail

Komische Internetseite..?
(Fahre mit der Maus über den Link -nicht klicken, nur fahren - um zu sehen wo der hinführt)

Fiese Falle:
miCORsoft statt miCROsoft!

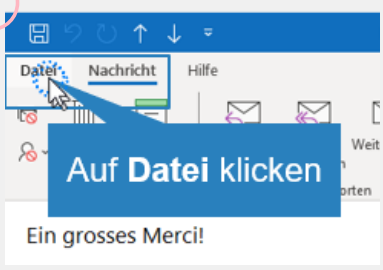


Der Passwortwechsel lag in der **Vergangenheit**

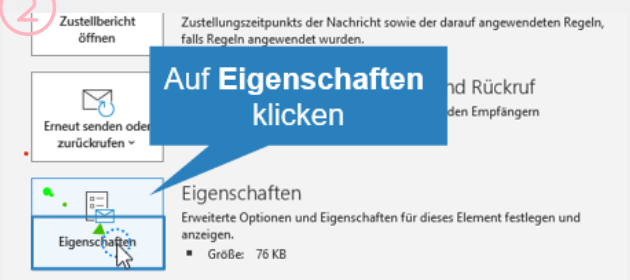


Absenderadresse genau überprüfen:

1

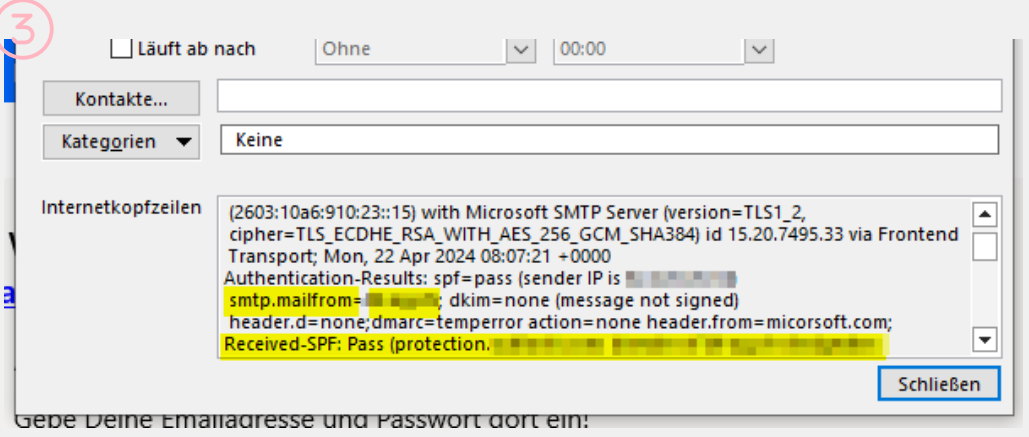


2



Hier kann unter smtp.mailfrom und Received-SPF **eingesehen werden, dass der Absender von einer komischen Adresse** war!

3



FPM #3
QR CODE FRAUD

Report & Statistik

80	8	8	6
100%	**10%**	**10%**	**7.5%**
Email Sent	**Email Opened**	**Clicked Link**	**Scanned QR**
Alle geplanten Fake Emails wurden erfolgreich versendet.	Niemand hat die Fake Email geöffnet	Niemand hat auf dem im Fake Mail enthaltenen Link geklikt	Niemand hat Daten eingegeben

REASONS OF *CLICKING/SCANNING*

REASON 1
Absender sah auf den ersten Blick nach einer wahren, bekannten Person aus

REASON 2
QR Code Sensibilisierung noch nicht bei den Mitarbeiter angekommen

REASON 3
"Ist ja nur mein Handy" - was wenn es in unsrem WLAN ist?

REASON 4
Keine typische SPAM Mail gewesen

LEARN MORE!
mjcybersecurity.com

GETTIN' BETTER!

QR-Phishing ist noch nicht bei den Mitarbeiter angekommen

REPORTED EMAILS

In der folgenden Grafik kann eingesehen werden, wie mit den Fake Phishing Mail umgegangen wurde. Die Mitarbeiter können die Email bei Sicherheit und unsicherheit der IT melden, oder direkt löschen. Erkennbar ist, dass viele die Emailadrese nicht genau angeschaut haben, sonst wäre aufgefallen, dass die Email nicht von der Person ist. Zudem wurde der QR Code gescannt, weil sie es ja "mit Ihrem Handy" machen.

Viele der Mitarbeiter haben es aber als SPAM abgetan!

EMAILS REPORTED "SPAM!"

7
Mitarbeiter erkannten die Mail sofort als SPAM

EMAILS REPORTED "SPAM?"

1
Mitarbeiter war sich unsicher ob das SPAM war

EMAIL DIRECTLY DELETED

64
Mitarbeiter löschten die Email direkt


Von:
[redacted]
Betreff: QR Code scannen für Infos, Tipps & Tricks

Hi

Bitte Scanne doch den unteren QR Code für weitere Tipps & Tricks! Oder klicke hier:

Gruess

Jessica Storrer
[redacted]
E-mail Address

Fazit:

QR-Code Phishing und Sensibilisierung auf Absender muss gestärkt werden!

LEARN MORE!
mjcybersecurity.com

FPM
Die drei Fake Mails

Erkennen & Handeln

Fake Phishing Mail #3
QR-FRAUD

QR Code scannen für Infos, Tipps & Tricks

JA jessica.storrrer@[redacted]
An Jessica Storrer

Antworten | Allen antworten | Weiterleiten | ...

Di. 30.04.2024 10:59

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

Hi

Bitte Scanne doch den unteren QR Code für weitere Tipps & Tricks! Oder klicke hier:

Gruess

Das ver knü of...
Jessica Storrer
IT
Fon [redacted]
Fon [redacted]
E-mail [redacted]
Address [redacted]

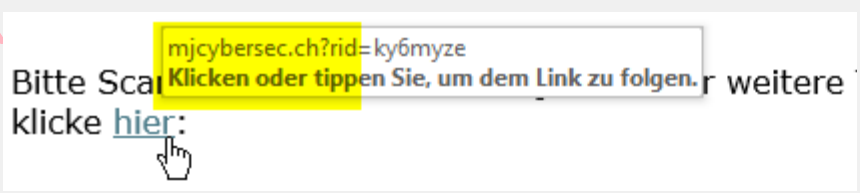
LOOKIN' WEIRD!

AUF WAS MUSS ICH ACHTEN?

Hier siehst Du die eingebauten Fehler in des QR-Frauds

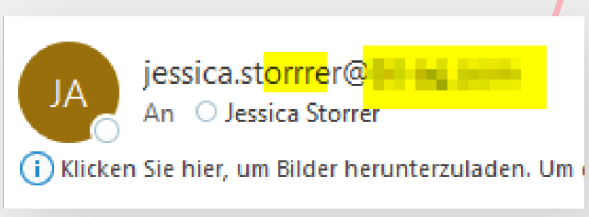
Komische Internetseite..?

(Fahre mit der Maus über den Link -nicht klicken, nur fahren - um zu sehen wo der hinführt)



Fiese Falle:

Ähnlichkeiten mit einem "echten" Mitarbeiter. Immer genau auf Namen und Adresse achten!



Komisch aussehende Signatur

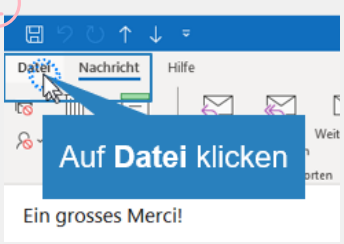
Wenn die Signatur komisch aussieht, zweimal hinschauen!

"Ich scanne es ja mit meinem Handy" -> Sobald Du in einem WLAN bist, kanns sich verbreiten!

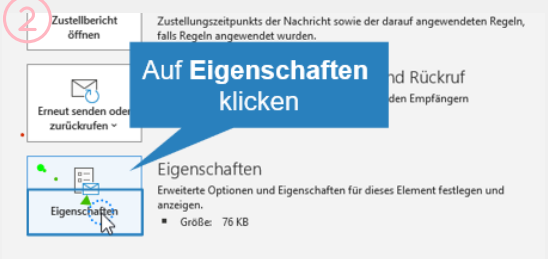
QR-Code Scans können **direkt zu einem Download** führen. Überprüfe, wo der Link hingeht und passe auf mit "gekürzten" Links -> bit.ly....

Absenderadresse genau überprüfen:

1.



2.



3.

Hier kann unter smtp.mailfrom und Received-SPF **eingesehen werden, dass der Absender von einer komischen Adresse war!**