Gib Phishing-Mails keine Chance!

So entlarvst Du Cyberkriminelle

Phishing-E-Mails ähneln Nachrichten von Eurer Bank, Arbeitskollegen, Lieferanten, Freunden oder sogar von Deinem Chef. Auch wenn sie vertrauenswürdig aussehen, enthalten sie oft Hinweise, die ihre wahren oder bösartigen Absichten verraten.

Wenn Du eine E-Mail erhältst, die mehrere der folgenden Phishing-Indikatoren enthält oder sich einfach **nicht «richtig» anfühlt, wende Dich umgehend an den USKA Webmaster** – bevor noch mehr Leute betroffen sind...

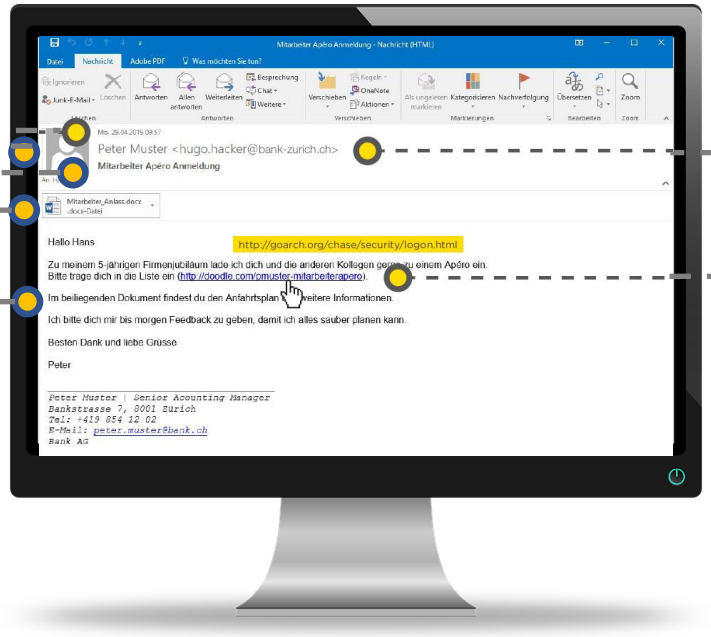
Datum
Wurde die E-Mail zu einer ungewöhnlichen Uhrzeit geschickt (Nacht, Wochenende)?

Empfänger
- Wurde die E-Mail noch an andere Personen geschickt?
- Falls ja: Kennst Du diese Personen?
- Sind es ungewöhnlich viele?

Betreff
Stimmt der Betreff mit dem Inhalt überein?
- Ist es eine Antwort auf eine E-Mail, die Du geschickt oder angefordert hast?
- Ist der Betreff persönlich oder eher allgemein formuliert?

Anhang
Erwartest Du eine entsprechende Datei?
Falls der Absender von intern stammt:
- Stimmt der Dateiname mit den bei Deinen üblichen Bezeichnungen überein?
- Wirkt der Dateiname vertrauenswürdig?
- Ist es ein üblicher Dateityp?
- Hat der Virenscanner die Datei gemeldet?
- Beinhaltet das Dokument Makros? (Nicht aktivieren!)

Inhalt
- Ist die Ansprache unpersönlich?
- Wird eine Aktion von Ihnen verlangt (Herausgabe/Eingabe Logindaten, Zahlungsaufforderung etc.)?
- Wird mit Konsequenzen gedroht, beispielsweise bei Nichtreaktion (Geldverlust, Strafanzeige, Konto- oder Kartensperrung etc.)?
- Hat der Text Rechtschreib-/Grammatikfehler oder eine unübliche Formatierung?
- Sieht die Signatur/der Footer vertrauenswürdig aus?
- Werden verschiedene Schriftgrössen, -formatierungen, -farben etc. verwendet?



Absender
- Kennst Du den Absender?
- Falls ja: Ist es dieselbe E-Mail-Adresse wie beim letzten E-Mail-Kontakt?
- Wurde die E-Mail von einem Bekannten, Partner oder Lieferanten geschickt, ist inhaltlich aber ungewöhnlich resp. uncharakteristisch?
- Stimmt die E-Mail-Adresse mit dem Anzeigenamen des Absenders überein? (Peter Muster → <hugo.hacker@bank-zurich.ch>)
- Handelt es sich bei der E-Mail-Adresse um eine gefälschte Domain? (@bank-zurich.ch → @bank.ch)

Hyperlinks
Wenn Du mit der Maus über den Link fährst (s. links in gelb):
- Wird dieselbe Zieladresse angezeigt? (Achtung: Auf keinen Fall klicken!)
- Ist der Link ungewöhnlich lang?
- Wird im Text Bezug zum Link genommen?
- Ist die Zieladresse des Hyperlinks fehlerfrei? (z.B. www.apple.com → www.appple.com)

Allgemeine Tipps
Höre auf Dein Bauchgefühl: Wenn Du nicht sicher bist, ob die E-Mail echt oder ein Betrug ist, lass die E-Mail lieber durch unseren Web-Master überprüfen.

Klicke bei Unsicherheiten niemals auf einen Link und öffne auf keinen Fall die Datei.

Wenn Du vermeintlich sichere Anhänge öffnest und eine Warnmeldung erscheint, lass die E-Mail durch unseren Web-Master.

Im Zweifelsfall in einer neuen, separaten E-Mail oder telefonisch beim Absender nachfragen, ob er/sie tatsächlich diese E-Mail geschickt hat.

ONE STEP AHEAD

SIDLER
Information Security
www.sidler-security.ch

USKA, 29.7.2021