WWU MÜNSTER

IT SICHERHEIT WWU MÜNSTER

Checkliste: Betrügerische E-Mails erkennen

8 Punkte, um Phishing-, Spam- und andere schädliche E-Mails zu erkennen

Ist die absendende Person unbekannt? Ist die E-Mail-Adresse unpassend? 1

- Betrügerische E-Mails werden häufig von unpassenden oder unplausiblen E-Mail-Adressen verschickt.
- Seien Sie wachsam, wenn Sie die absendende Person nicht kennen.
- Prüfen Sie, ob die E-Mail-Adresse zur absendenden Person passt, wie z. B. "...@uni-muenster.de" für E-Mails von WWU-Angehörigen.
- Prüfen Sie, ob eine gültige digitale Signatur vorliegt. Betrügerische E-Mails sind i. d. R. **nicht** signiert.

Werden unrealistische Vorteile versprochen? 2

- Für Werbe- und Betrugszwecke werden häufig unrealistische Gewinne, Rabatt- oder Gutscheinkarten (z. B. Amazon oder Paysafecard) versprochen.
- Misstrauen Sie Gratisdienstleistungen. Oftmals verstecken sich hinter solchen Diensten illegale Angebote oder Ihre Anmeldedaten werden weiterverkauft.

Erzeugt die absendende Person Druck? 3

- Aufforderungen zu sofortigem Handeln deuten auf Betrug hin, z. B. umgehendes Einloggen auf einer Internetseite oder eine Geldüberweisung.
- Auch Androhungen von negativen Konsequenzen können Teil von Betrugs-Versuchen sein (z. B. Sperrung des Zugangs).
- Überprüfen Sie vermeintliche Handlungs-aufforderungen durch die WWU IT. Legitime Meldungen der IT finden Sie auch unter den Betriebsmeldungen auf der WWU IT-Internetseite.

Werden vertrauliche Informationen verlangt? 4

- Betrügerische E-Mails verlangen häufig die Preisgabe vertraulicher Daten per E-Mail oder auf einer verlinkten Internetseite (z. B. Passwörter).
- Prüfen Sie vor der Eingabe vertraulicher Daten auf einer Internetseite, ob die Adresse plausibel und die Verbindung verschlüsselt ist (https statt http).
- Geben Sie Zugangsdaten der WWU nur auf Webseiten der WWU ein.

Ist die Anrede unpersönlich? 5

- In betrügerischen E-Mails ist die Anrede oft unpersönlich, fehlt oder weicht von der üblichen Form ab.
- Die meisten Unternehmen werden in der Anrede Ihren vollen Namen verwenden. In gefälschten Nachrichten ist die Anrede häufig allgemeingültig, wie z. B. “Lieber Kunde”.

Soll ich auf einen Link klicken? 6

- Bei Links ist nicht immer erkennbar wohin sie führen. Klicken Sie bei unbekannten Absendern **nie** unbedacht auf Links.
- Überprüfen Sie die Internetadresse, indem Sie mit dem Mauszeiger über den Link fahren: Links aus betrügerischen E-Mails sind oft zum Verwechseln ähnlich (z. B. "uni-meunster.de" oder "uni-muenster.de.com" anstatt "**uni-muenster.de**").

Enthält die E-Mail unerwartete Anhänge? 7

- Öffnen Sie keine unbekannten oder unerwarteten Dateianhänge.
- Sollte die E-Mail von einer bekannten Person stammen, erkundigen Sie sich im Zweifelsfall vor dem Öffnen auf anderem Wege (Telefon, Mattermost), ob diese Person die E-Mail tatsächlich verschickt hat.
- Aktivieren Sie bei unbekannten Office Dateien nicht den Bearbeitungsmodus und keine Makros.

Enthält die E-Mail Fehler? 8

- Texte aus betrügerischen E-Mails werden häufig mit Hilfe von Übersetzungstools generiert, sodass die Grammatik oder Rechtschreibung fehlerhaft sind (v. a. Umlaute).

Sollten ein oder mehrere Punkte zutreffen, handelt es sich womöglich um einen Betrugsversuch. Sollten Sie eine betrügerische E-Mail mit WWU-Bezug erhalten, melden Sie diese dem Computer Emergency Response Team unter:
spam@uni-muenster.de