Spam

Ermittelt für jedes Szenario, ob es sich bei der Nachricht um Spam handelt und ob man Informationen mit dieser Person teilen sollte. Notiert bei jeder Frage eure Antwort in dem dafür vorgesehenen Feld.

Szenario 1

Ihr erhaltet eine E-Mail von einem Rechtsanwalt, der euch darüber in Kenntnis setzt, dass ein entfernter Verwandter euch als Erbe einer größeren Geldsumme benannt hat. Ihr werdet zu Folgendem aufgefordert: „ Um das Geld zu erhalten, senden Sie mir bitte Ihre Kontonummer und Ihre Bankleitzahl, damit wir die Zahlung vornehmen können.“

Szenario 2

Ein Freund schreibt euch per SMS, dass er ein Foto sucht, das ihr ihm einmal gezeigt habt, er aber keine Berechtigung hat, um es anzusehen. Ihr habt gerade keinen Zugriff auf euren Computer, um ihm das Foto zu senden. Er antwortet: „Ich könnte mich kurz über dein Konto anmelden, um das Foto herunterzuladen. Wie lautet dein Passwort?“

Szenario 3

Ihr erhaltet eine an euch adressierte E-Mail von eurer Schule, die euch mitteilt, dass die Konten einiger Schüler gehackt wurden. Der Absender schreibt: „Wir haben vor Kurzem festgestellt, dass die Sicherheit einiger Schülerkonten beeinträchtigt wurde. Wir entschuldigen uns für diese Unannehmlichkeit und arbeiten mit Hochdruck daran, das Problem zu beheben. Um Ihr Konto zurückzusetzen, antworten Sie bitte mit Ihrem Benutzernamen und Ihrem Passwort auf diese E-Mail.“

Szenario 4

Ihr erhaltet eine E-Mail von einer Bank, bei der ihr tatsächlich ein Konto habt. Die E-Mail besagt, dass die Bank gehackt wurde und dass ihr euch so bald wie möglich bei eurem Konto anmelden solltet, um euer Passwort zu ändern. Zudem solltet ihr das Passwort aller Konten ändern, bei denen ihr das gleiche Passwort verwendet.

Spam: Exemplar für den Kursleiter

Ermittelt für jedes Szenario, ob es sich bei der Nachricht um Spam handelt und ob man Informationen mit dieser Person teilen sollte. Notiert bei jeder Frage eure Antwort in dem dafür vorgesehenen Feld.

Szenario 1

Ihr erhaltet eine E-Mail von einem Rechtsanwalt, der euch darüber in Kenntnis setzt, dass ein entfernter Verwandter euch als Erbe einer größeren Geldsumme benannt hat. Ihr werdet zu Folgendem aufgefordert: „Um das Geld zu erhalten, senden Sie mir bitte Ihre Kontonummer und Ihre Bankleitzahl, damit wir die Zahlung vornehmen können."

Bei dieser E-Mail handelt es sich sehr wahrscheinlich um Spam. Selbst wenn der Name eures Verwandten korrekt ist, ist der Absender möglicherweise nicht der, für den er sich ausgibt. Er könnte auch auf anderen Wegen über euer Verwandtschaftsverhältnis zu dieser Person erfahren haben. Fremden Personen eure Kontodaten mitzuteilen, ist immer riskant und sollte sorgfältig bedacht werden. Sendet eure Daten niemals an eine fremde Person, bevor ihr sie nicht selbst kontaktiert habt – und auch dann seid sehr vorsichtig! Es ist beispielsweise keine gute Idee, eure Kontodaten per E-Mail zu versenden, da der Versand unverschlüsselt erfolgt. Aus diesem Grund haben viele Krankenhäuser, Rechtsanwaltskanzleien und Banken spezielle Webseiten für die Kommunikation mit ihren Kunden eingerichtet.

Szenario 2

Ein Freund schreibt euch per SMS, dass er ein Foto sucht, das ihr ihm einmal gezeigt habt, er aber keine Berechtigung hat, um es anzusehen. Ihr habt gerade keinen Zugriff auf euren Computer, um ihm das Foto zu senden. Er antwortet: „Ich könnte mich kurz über dein Konto anmelden, um das Foto herunterzuladen. Wie lautet dein Passwort?"

Hier handelt es sich nicht um Spam, aber ihr solltet euer Passwort trotzdem nicht mit anderen Personen teilen. Sobald diese Person euer Passwort hat, könnte sie euch aus eurem Konto aussperren oder auf andere Onlinekonten mit dem gleichen Passwort zugreifen. Falls außerdem Dritte oder Hacker eure Nachricht mitlesen, könnten weitere Personen ohne euer Wissen auf euer Konto zugreifen.

Szenario 3

Ihr erhaltet eine an euch adressierte E-Mail von eurer Schule, die euch mitteilt, dass die Konten einiger Schüler gehackt wurden. Der Absender schreibt: „Wir haben vor Kurzem festgestellt, dass die Sicherheit einiger Schülerkonten beeinträchtigt wurde. Wir entschuldigen uns für diese Unannehmlichkeit und arbeiten mit Hochdruck

daran, das Problem zu beheben. Um Ihr Konto zurückzusetzen, antworten Sie bitte mit Ihrem Benutzernamen und Ihrem Passwort auf diese E-Mail.“

Es ist nicht üblich, Benutzer um diese Informationen zu bitten. Auch wenn der Absender legitim erscheint, solltet ihr davon ausgehen, dass E-Mails, in denen ihr nach eurem Passwort gefragt werdet, Spam sind.

Szenario 4

Ihr erhaltet eine E-Mail von einer Bank, bei der ihr tatsächlich ein Konto habt. Die E-Mail besagt, dass die Bank gehackt wurde und dass ihr euch so bald wie möglich bei eurem Konto anmelden solltet, um euer Passwort zu ändern. Zudem solltet ihr das Passwort aller Konten ändern, bei denen ihr das gleiche Passwort verwendet.

Das korrekte Vorgehen ist in diesem Fall, ein neues Browserfenster zu öffnen und wie üblich auf die Webseite zuzugreifen. Eine solche Mitteilung (d. h. dass Konten gehackt wurden) wird üblicherweise auch im Kundenportal des Unternehmens oder der Bank bekanntgegeben. Die Anweisungen im Portal können ohne Bedenken befolgt werden. Wie schon in Szenario 3 beschrieben wurde, wird kein legitim Handelnder in einer E-Mail um eure Konto- oder Zugriffsdaten bitten.