Echte und betrügerische E-Mails erkennen

In den letzten Jahren haben wir immer wieder über betrügerische E-Mails berichtet, haben die Maschen der Kriminellen vorgestellt und vor neuen Tricks gewarnt. Dennoch erhalten wir beinahe täglich Nachrichten mit der Frage: “Ist diese E-Mail echt?” oder “Ist diese E-Mail eine Fälschung?”. Dabei ist uns aufgefallen, dass immer häufiger seriöse E-Mails für Betrug gehalten werden. Woher das kommt, ist nachvollziehbar: Es gibt so viele Betrugsversuche, dass man geneigt ist, alles zu hinterfragen. Daher wollen wir heute noch einmal anhand von Beispielen auf grundsätzliche Unterschiede zwischen “echten” und “gefälschten” Mails eingehen.

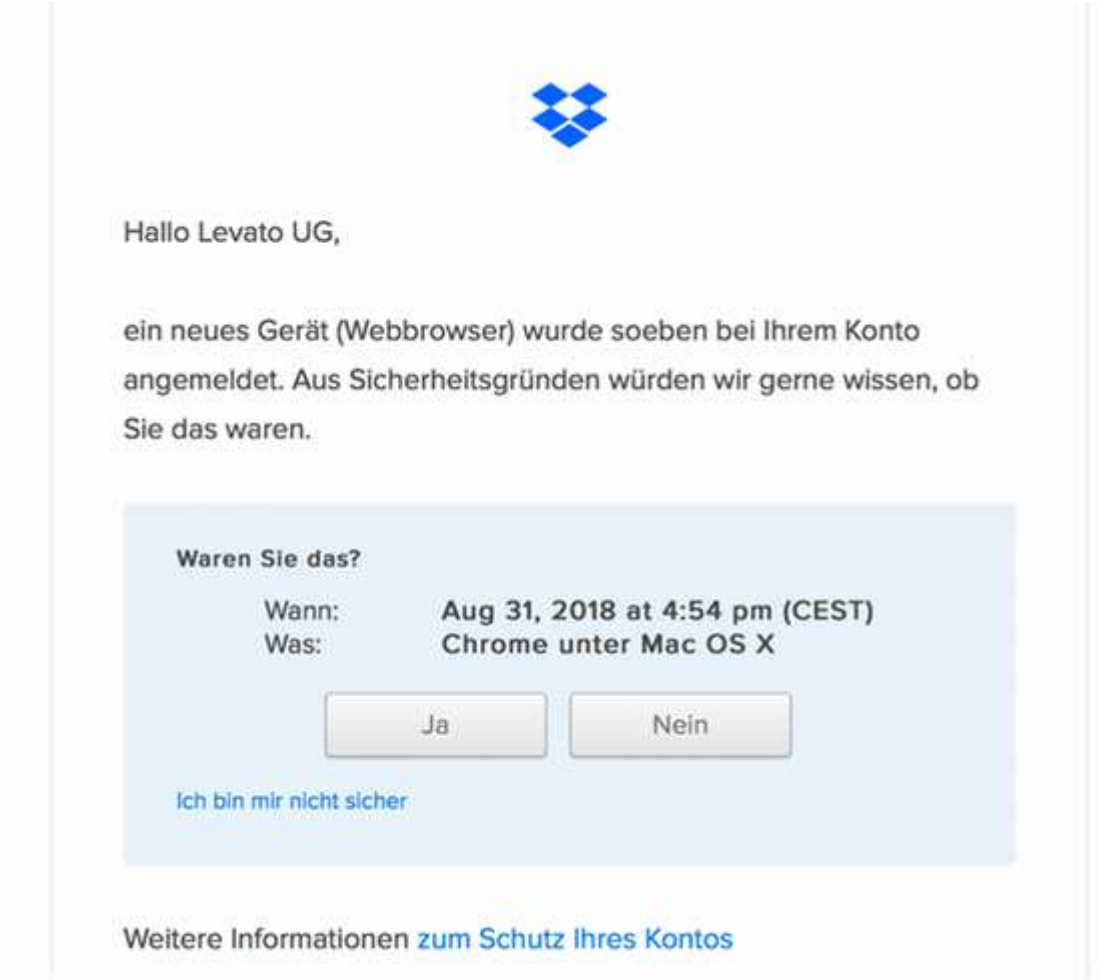
Diese Mails sind echt

Wir haben uns daran gewöhnt, den meisten E-Mails, die vermeintlich von Ebay, Amazon, Google oder PayPal kommen, zu misstrauen. Denn häufig versuchen die Betrüger, an unsere Anmeldedaten für genau diese Seiten zu kommen und ahmen dafür in gefälschten E-Mails das Erscheinungsbild der Firmen nach. Doch manchmal versenden Ebay, Amazon, Google, PayPal und Co. tatsächlich E-Mails an uns. Wie kann man also diese Mails erkennen, die tatsächlich von der echten Firma stammen? Am besten erkennt man echte Mails daran, dass diese uns über etwas informieren, dabei aber keinen Druck aufbauen, irgendetwas anzuklicken. Immer wieder kommt es vor, dass sich Nutzungsbedingungen geringfügig ändern. Darüber informieren die Firmen meist per Mail. Um diesen neuen Nutzungsbedingungen zuzustimmen, muss man aber nichts unternehmen. Vereinfacht gesagt funktioniert es so: Nutzt man die Dienste der Firma weiterhin, so akzeptiert man damit automatisch die neuen Nutzungsbedingungen. Man muss dafür also nirgendwo anklicken, man muss sich nirgendwo anmelden, man muss seine Daten nirgendwo erneut eingeben. Betrüger nutzen hier gerne den erfundenen Begriff “Datenabgleich”.

Beispiel #1: Kein Betrug, sondern echt – die Microsoft Nutzungsbedingungen

Schwerer zu erkennen sind die folgenden E-Mails. Es handelt sich um echte Mails von den Anbietern Dropbox und Google. Denn bei vielen Anbietern erhält man eine E-Mail, wenn es eine neue Anmeldung zu diesem Dienst von einem neuen Gerät aus gegeben hat. Wenn man beispielsweise das neue Google-Konto auf seinem Smartphone eingerichtet hat und sich nun das erste Mal mit seinem Computer bei Google mit diesem Google-Konto anmeldet. Die Benachrichtigungen dienen der eigenen Kontrolle und Sicherheit. Es könnte ja auch sein, dass eine neue Anmeldung bzw. der Versuch einer Anmeldung von einem fremden Computer durchgeführt wird, dann sind diese Benachrichtigungen ein Hinweis auf einen Hacker-Angriff. Manchmal wird man daher gefragt: “Waren Sie das?”. Überlegen Sie genau, ob Sie sich kürzlich irgendwo neu angemeldet haben, wenn Sie eine solche Mail erhalten. Echte Mails erkennt man auch hier wieder daran, dass man nicht sofort dazu gedrängt wird, seine Anmeldedaten erneut anzugeben. Zwar gibt es auch in echten E-Mails eine Möglichkeit, etwas anzuklicken. Nicht jeder Klick führt also sofort ins Verderben. Aber: Wichtig ist, was danach passiert, nach dem Klick, welche Seite sich öffnet und was auf dieser Seite behauptet wird.

Beispiel #2 und #3: Seriöse Mails von Google und Dropbox mit Sicherheitshinweisen



Diese Mails sind gefälscht

Gefälschte Mails erkennt man fast immer daran, dass man unter irgendeinem Vorwand dazu gebracht wird, seine kompletten Anmeldedaten inklusive Passwort erneut einzugeben, d.h. zu **bestätigen**, **abzugleichen** oder zu **verifizieren**. Diese drei Varianten deuten nahezu immer auf einen Betrugsversuch hin. Der Vorwand ist dabei meistens, dass es angeblich irgendwelche “Unregelmäßigkeiten” gab und dass der Zugang aus Sicherheitsgründen gesperrt sei. Zum Aktivieren soll man dann erneut die Daten eingeben. Dies ist ein feiner, aber wichtiger Unterschied zu den obigen Beispielen.

Da es manchmal in der Tat sehr schwer ist, diesen Unterschied zu erkennen, kontrollieren Sie im Zweifelsfalle auch folgendes:

a) Bin ich bei dem Anbieter überhaupt registriert?

b) Passt die Absenderadresse auch zum Anbieter?

c) Enthält die E-Mail auffällige Rechtschreibfehler?

d) Werden Sie mit Ihrem echten Namen angeschrieben?

e) Wird Druck aufgebaut, dass man schnell irgendwo anklicken soll oder informiert die Mail nur?

f) Kommen die Begriffe "**Datenabgleich**" oder das Satz "**Verifizieren Sie Ihr Konto**" vor? Dann ist es ein Betrug!

g) Gibt es die gleiche Nachricht auch auf der Internetseite des Anbieters?

Viele Anbieter wie Amazon, PayPal, eBay oder die Bank fürs Online-Banking haben nämlich auf deren Internetseite auch ein eigenes Postfach, indem alle E-Mails, die Sie erhalten haben, mit einer Kopie gespeichert sind. Wenn Sie sich auf der Internetseite des Anbieters anmelden (ohne vorher den Link in der Mail anzuklicken) und dann in das Postfach schauen, so sehen Sie dort die gleichen Nachrichten, die auch per Mail verschickt wurden. Auf diese Weise können Sie optimal kontrollieren, ob eine Nachricht echt ist.

Hier sehen Sie eine gefälschte E-Mail: