E-Mail

Gängige Betrugsmaschen erkennen

Betrugsmaschen – Sehr oft fangen sie mit einer E-Mail an. Kein Wunder, denn während auf offener Straße sich kaum jemand von einem Wildfremden in ein Gespräch verwickeln lässt, ist die Kommunikation über Internet der perfekte Köder: anonym, überzeugend und wirtschaftlich (mit nur einer E-Mail können Hunderttausende potenzielle „Opfer“ erreicht werden). Im Internet überwiegen auch oft die menschlichen Schwächen gegenüber der Skepsis. Zu diesen Charakteristika gehören zum Beispiel Neugierde, Mitleid, Angst oder Habgier. Sie werden ausgenutzt und bilden so das Fundament für eine Vielzahl an Betrugsstrategien im Online-Zeitalter:

Lotteriegewinne

Sie haben bei einer Lotterie gewonnen: Geld, ein Auto, einen Traumurlaub,… Weitere Details entnehmen Sie der E-Mail.

In der E-Mail könnten sich Links oder Dateianhänge befinden, die Sie auf schädliche Webseiten weiterleiten, bzw. Ihren Computer mit Malware infizieren. Auch ohne Links und Anhang ist der Lotteriegewinn eine Farce: Vermutlich werden Ihnen hohe „Bearbeitungsgebühren“ in Rechnung gestellt. Vom eigentlichen Gewinn sehen Sie nichts!

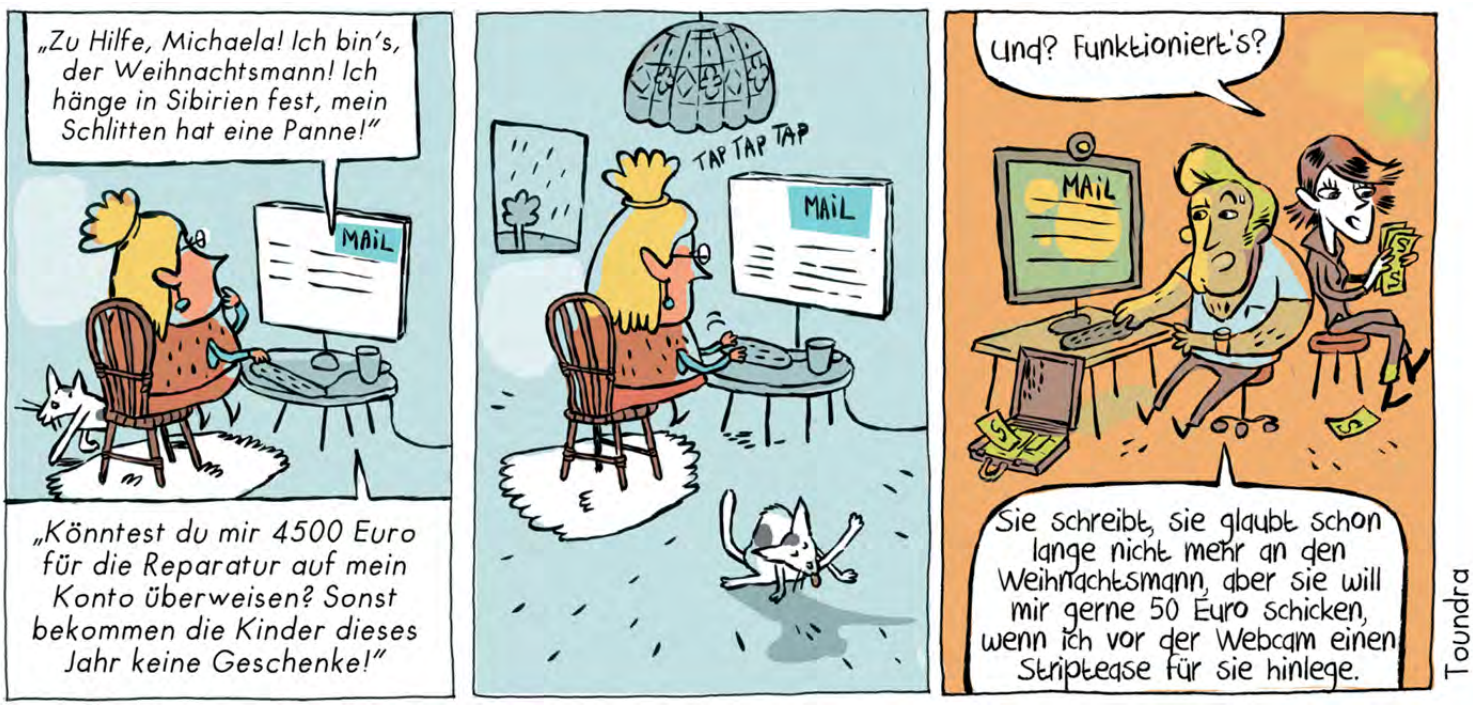
Ihr gesunder Menschenverstand sagt Ihnen bereits, dass da etwas faul sein muss. Ignorieren Sie solche Angebote. Sie können sie im Mailserver auch als Spam markieren.

Angebote, die zu schön sind, um wahr zu sein

Ein Job, der super bezahlt ist, und den Sie von zu Hause aus erledigen können, tolle Reisen zu Schnäppchenpreisen oder Ihr Geld als Kapitalanlage mit unglaublich hohen Zinsen… Im Internet gibt es unzählige verlockende Angebote. Praktisch, dass Sie per E-Mail direkt zu Ihnen nach Hause kommen…

Bei Angeboten, die zu schön sind, um wahr zu sein, lauern hohe „Bearbeitungsgebühren“, und Nebenkosten. Geld, das Sie im Voraus für eine zu erbringende Leistung gezahlt haben, werden Sie wahrscheinlich nie wieder sehen.

Ignorieren Sie E-Mails, die Ihnen das Blaue vom Himmel versprechen. Lesen Sie bei Angeboten generell immer das Kleingedruckte und seien Sie skeptisch, wenn im Vorfeld Gebühren von Ihnen verlangt werden, oder Sie persönliche (auch finanzielle) Daten angeben sollen



„Nigerianer“ (Vorschussbetrug)

Sie gelten als extrem vertrauenswürdig, weshalb Sie der Erbe eines verstorbenen Millionärs als Partner ausgewählt hat, ihm beim Geldtransfer zu helfen und dabei eine dicke Provision als Belohnung zu erhalten.

Wenn Sie zustimmen, müssen Sie vorab für „Bearbeitungsgebühren“ (z.B. Anwaltskosten oder Zoll) aufkommen. Vom „Erbe“ erhalten Sie keinen Cent. „Nigerianer“ werden übrigens so genannt, weil sie ihren Ursprung in Nigeria (ausgehend von der sogenannten „Nigeria Connection“) haben. Sie schildern die unterschiedlichsten Szenarien, laufen aber immer darauf hinaus, dass Ihnen für eine kleine Gefälligkeit eine riesen Belohnung versprochen wird.

Auch hier werden instinktiv Ihre Alarmglocken läuten… Niemand verschenkt einfach so eine Menge Geld. Ignorieren Sie die Anfrage. Wenn Sie andere, gutgläubige Menschen vor dem Trickbetrug warnen möchten, können Sie die E-Mail auch in einem Forum veröffentlichen.

Bestätigung/Aktualisierung von Daten

Ihre Bank fordert Sie über E-Mail auf, einen Link zu klicken, um anschließend Ihren Benutzernamen und Ihr Kennwort einzugeben. Grund dafür sei eine Aktualisierung bzw. Überprüfung der Sicherheitseinstellungen Ihres Kontos. Täten Sie dies nicht, würde Ihr Konto gesperrt.

Luxemburgische Banken kommunizieren nicht über E-Mail! Ihre Bank würde Sie niemals per E-Mail auffordern, Ihre Login-Daten einzugeben und Ihnen auch nicht mit der Schließung des Kontos drohen. Die E-Mail stammt von Betrügern, die Sie auf eine gefälschte Webseite leiten, Ihre eingegebenen Login-Daten dort ablesen und diese anschließend benutzen, um Zugang zu Ihrem Konto zu erlangen.

Gehen Sie keinesfalls den Anforderungen nach, die in der E-Mail von Ihnen gefordert werden. Wenn Sie sichergehen wollen, dass es sich nicht doch um eine legitime Nachricht Ihrer Bank handelt, rufen Sie diese an und fragen Sie direkt nach.

Falsche Zahlungsaufforderungen

Ein bekannter Online-Shop schickt Ihnen eine E-Mail mit Zahlungsaufforderung. Wie es scheint, haben Sie eine offene Rechnung für eine Bestellung. Wenn Sie nicht unverzüglich die (meist hohe) Summe zahlen, wird eine ebenfalls beachtliche Strafe hinzukommen. Für weitere Details sollen Sie entweder die angehängte Datei öffnen, oder auf einen Link klicken.

Sie haben diese Bestellung nicht getätigt. Diese E-Mail stammt von Betrügern, deren Ziel es ist:

- **Das Geld für die „Bestellung“ einzuheimsen, falls Sie sich von der Strafankündigung so unter Druck gesetzt fühlen, dass Sie zahlen,**
- **Ihnen durch Klicken auf den Anhang einen Trojaner unterzujubeln, bzw. Sie durch Klicken auf den Link auf eine schädliche Webseite zu lotsen, auf der sich Ihr Computer mit Malware infiziert, oder Sie zum Eingeben persönlicher Daten aufgefordert werden, die dann von den Kriminellen mitgelesen werden.**

Falls Sie unsicher sind, was diese Rechnung betrifft, dann nehmen Sie telefonischen Kontakt mit dem Online-Shop auf. Wichtig: Entnehmen Sie die entsprechende Telefonnummer nicht der E-Mail, denn auch die hier angegebenen Kontaktdaten sind wahrscheinlich gefälscht. Sie können auch den Online-Shop generell darüber in Kenntnis setzen, dass in seinem Namen betrügerische Mails im Umlauf sind. Die Rechnung sollten Sie auf jeden Fall ignorieren. Lassen Sie sich von der Androhung negativer Konsequenzen nicht unter Druck setzen und öffnen Sie die mitgeschickte Datei gar nicht erst.

Ransomware

Ihr Computer ist blockiert. Eine Warnmeldung erscheint auf dem Bildschirm: Alle Ihre Daten wurden verschlüsselt und befinden sich nun in der Hand von Erpressern. Sie müssen ein Lösegeld (englisch: „ransom“) zahlen, falls Sie wieder Zugriff auf Ihren Computer haben wollen.

Ransomware ist ein Schadprogramm, das Ihre Daten als Geisel nimmt. Ihr Computer wurde, zum Beispiel beim Klicken auf einen Link in einer E-Mail, oder beim Besuchen einer schädlichen Webseite, mit der Malware infiziert.

Wenn Sie Opfer einer Ransomware wurden, sollten Sie der Zahlungsaufforderung nicht nachkommen. Wer das Lösegeld bezahlt, unterstützt die kriminellen Machenschaften im Internet. Leider kann es in einigen Fällen vorkommen, dass Ihnen nichts anderes übrig bleibt, als die geforderte Summe doch zu zahlen. Nämlich dann, wenn die chiffrierten Daten sehr wichtig für Sie sind, und Sie keine Kopie davon besitzen. Benutzt die Ransomware ein sehr leistungsstarkes Chiffrier-System, wie zum Beispiel CryptoLocker, sind Sie den Erpressern ausgeliefert, falls Sie Ihre Daten zurück haben wollen.

Glücklicherweise genügt es oft, die Zahlungsaufforderung zu ignorieren, und Ihren PC zu säubern, um die Ransomware loszuwerden. Dieser Säuberungs-Vorgang kann sich mehr oder minder komplex gestalten, je nachdem, welche Art von Schadprogramm Ihren Computer infiziert hat. Als erstes sollten Sie versuchen, den Computer im abgesicherten Modus neu zu starten, um schädliche Elemente zu löschen. Allerdings kann es vorkommen, dass der abgesicherte Modus auf einem infizierten Gerät nicht funktioniert. Dann müssen Sie den PC mit Hilfe einer Live-CD neu starten.

Präventive Schutzmaßnahmen:

Sparsam mit Daten umgehen:

Geben Sie Ihre E-Mail-Adresse nicht bedenkenlos weiter und veröffentlichen Sie sie auch nicht im Internet. Computerprogramme auf der ganzen Welt suchen rund um die Uhr das Internet nach Kontaktdaten ab, die dann weiterverkauft und oft für kriminelle Zwecke missbraucht werden.

Wenn Sie Ihre E-Mail-Adresse trotzdem veröffentlichen wollen oder müssen, können Sie statt „@“ auch eine kreative Buchstabenkombination oder ein Sonderzeichen angeben, z.B. [ät] oder *. Solche Adressen werden von den Suchcomputern weniger erkannt.

Geben Sie niemals persönliche oder finanzielle Daten über E-Mail preis. Seriöse Firmen werden Sie nie dazu auffordern.

Eingehende Mails kritisch prüfen

Um auszuschließen, dass eine E-Mail aus einer kriminellen Quelle stammt, die sich die Identität ihres Opfers angeeignet hat, oder sich mit täuschend echten Mitteln als offizieller Kontakt (z.B. Bank oder Behörde) ausgibt, sollten Sie sich folgende Fragen stellen: Ist es normal, dass ich eine Nachricht von diesem Absender erhalte? Entspricht der Inhalt dieser Mail dem, was ich von diesem Absender erwarte (inhaltlich und sprachlich)? Sind die Maßnahmen, um die ich ggf. gebeten werde, gerechtfertigt ungefährlich?

Hören Sie auch auf Ihren gesunden Menschenverstand. Absurde Geschichten und vielversprechende Angebote gibt es im Internet wie Sand am Meer. Was sich zu schön anhört um wahr zu sein, ist in der Regel eine Lüge.

Nicht blind auf Links klicken oder Dateien herunterladen

Generell sollten Sie es vermeiden, in E-Mails auf mitgeschickte Links zu klicken. Hierüber können Sie auf Phishing-Seiten landen, auf denen Ihre Daten ausspioniert werden, oder aber Sie können Ihren Computer mit einem Schadprogramm infizieren. Letzteres gilt auch für Dateianhänge.

Tätigen Sie generell keine Downloads und klicken Sie nicht auf Links in E-Mails, deren Absender Sie nicht kennen, oder deren Empfang Sie nicht erwartet haben. Auch wenn der Absender bekannt ist, so könnte sich jemand in dessen System gehackt und in seinem Namen die E-Mail verschickt haben. Viren und Trojaner verbreiten sich schnell unter Verwendung der E-Mail-Adressbücher. Im Zweifelsfall lieber dem Absender anrufen und sich erkundigen, besonders dann, wenn der Anhang unerwartet kommt.

Geben Sie Links lieber manuell in die Adresszeile Ihres Browsers ein, oder suchen Sie im Internet nach der offiziellen Webadresse. Oft sehen mitgeschickte Links auf den ersten Blick offiziell aus, stellen Sich dann aber als Fälschungen heraus (z.B. www.luxenburg.lu anstelle von www.luxemburg.lu). Außerdem kann sich hinter einer korrekten Internetadresse ein korrupter Link zu einer gefälschten Webseite verstecken.

Der Umgang mit Spam

Richten Sie sich für nicht offizielle Anlässe, z.B. für Online-Einkäufe oder die Teilnahme an Gewinnspielen eine zweite Mailadresse ein. Auf diesem Konto landen mit Sicherheit jede Menge Werbemails und Spam. So können Sie Ihr professionelles, bzw. offizielles E-Mail-Konto bestmöglich „sauber“ halten.

Antworten Sie nicht auf Spam. Auch wenn die E-Mails noch so nervig sind, wenn Sie darauf reagieren, weiß der Absender, dass Ihre Adresse aktiv ist, was Ihnen eine noch größere E-Mail-Flut bescheren wird. Achtung: Spam-Mails sind keine Newsletter. Während man letztere einfach abbestellen kann, bestätigt man beim Klicken des „Abbestellen“-Buttons bei Spam nur, dass das Konto aktiv ist.

Quellen überprüfen

Wenn Sie einen Trickbetrug hinter einer E-Mail erahnen, sich aber nicht ganz sicher sind, dann können Sie auch eine Online-Recherche starten. Geben Sie dazu einfach die entsprechenden Schlagworte oder Teile der Mail in die Suchmaschine ein. Die Wahrscheinlichkeit ist groß, dass bereits Andere vor Ihnen dieselbe Mail erhalten haben, und in Foren davor warnen. Es gibt auch eine Reihe von Webseiten, die sich der Entlarvung von Betrugsmaschen im Internet gewidmet haben.

Sollten Sie Fragen zum Thema Online-Betrug oder zur Internetnutzung generell haben, kontaktieren Sie die **BEE SECURE Helpline**:

BEE SECURE HELPLINE
BERATUNG & HILFE
8002-1234

Union Luxembourgeoise des Consommateurs (ULC)

Wenn Sie online bei einem in Luxemburg ansässigen Unternehmen einkaufen und sich über Ihre Rechte informieren oder über einen Betrug beschweren möchten, kontaktieren Sie die ULC.

www.ulc.lu

Centre Européen des Consommateurs (CEC)

Wenn Sie online in einem anderen Land der EU einkaufen und sich über Ihre Rechte informieren oder über einen Betrug beschweren möchten, kontaktieren Sie das CEC.

Tel. 26 84 64-1 www.cecluxembourg.lu

Institut Luxembourgeois de Régulation (ILR)

Wenn Sie bei Ihrem Telekommunikationsanbieter eine Beschwerde eingereicht haben, können Sie sich, bei einer nicht zufriedenstellenden Lösung des Problems, kostenfrei an die Schlichtungsstelle des ILR wenden.

www.ilr.lu/consommateurs

Police Grand-Ducale

Sie wollen Anzeige wegen Betrugs erstatten?

Schreiben Sie eine E-Mail an contact@police.etat.lu und informieren Sie sich über die genaue Prozedur.

www.police.lu

Herausgeber: BEE SECURE · B.P. 707 · L-2017 Luxembourg
Tel.: (+352) 247-86427 · Fax.: (+ 352) 46 41 86
bee-secure@snj.lu · www.bee-secure.lu

Co-funded by the European Union