Kapitel 5

Unerwünschte E-Mails

Sie kennen das: Nach und nach füllt sich Ihr E-Mail-Account mit E-Mails der verschiedensten Art. Einmal schreibt Sie ein Bankhaus mit dem Hinweis an, dass Ihr Kreditrahmen gesprengt sei und Sie sich dringend über einen Link in der E-Mail auf Ihrem Konto einloggen sollen, um alles wieder in Ordnung zu bringen.

Ein anderes Kreditunternehmen hat unregelmäßige Kontenbewegungen festgestellt und möchte gern, dass Sie sich über einen in der E-Mail befindlichen Hyperlink an Ihrem Konto anmelden, um die Unregelmäßigkeiten zu überprüfen. In weiteren E-Mails bekommen Sie **kostengünstige Kreditangebote** ohne vorherige Schufa-Überprüfung offeriert. In wieder anderen E-Mails werden **exorbitant hohe Verdienstmöglichkeiten** versprochen oder aber romantische Liebesabenteuer in Ihrer Nachbarschaft oder Region.

Ein Paketdienst wiederum behauptet, Sie nicht angetroffen zu haben, und bietet an, dass Sie sich nun mithilfe der E-Mail um das weitere Vorgehen kümmern können. Mails von angeblichen Notaren und Anwälten fehlen genauso wenig wie Rechnungsmitteilungen von Telefonanbietern inklusive eines angehängten Dokuments, um sofort alles zu überprüfen.

Manche dieser E-Mails landen direkt im Posteingang Ihres E-Mails-Accounts, manche im Unbekannt- oder Unerwünscht-Ordner, einige auch im Junk-E-Mail-Ordner – je nach verwendetem Mailprogramm und ob Sie Ihre E-Mails direkt online abrufen (sich im Mailkonto über das Internet einloggen bzw. ein Add-on Ihres E-Mail-Anbieters in Ihrem Browser installiert haben) oder einen sogenannten Mailclient benutzen (Microsoft Outlook, Mozilla Thunderbird etc.).

In diesem Kapitel erfahren Sie mehr über Betrugsversuche durch **Phishing-E-Mails** und über die Methoden **CEO Fraud**, **Fake President** und **Fake Chef**.

Hat der Betrüger Zugang zu dem Sicherheitsbereich Ihres PayPal-Kontos, kann er hier Ihr Passwort ändern.

Nerviger Spam und gefährliche Phishing-E-Mails

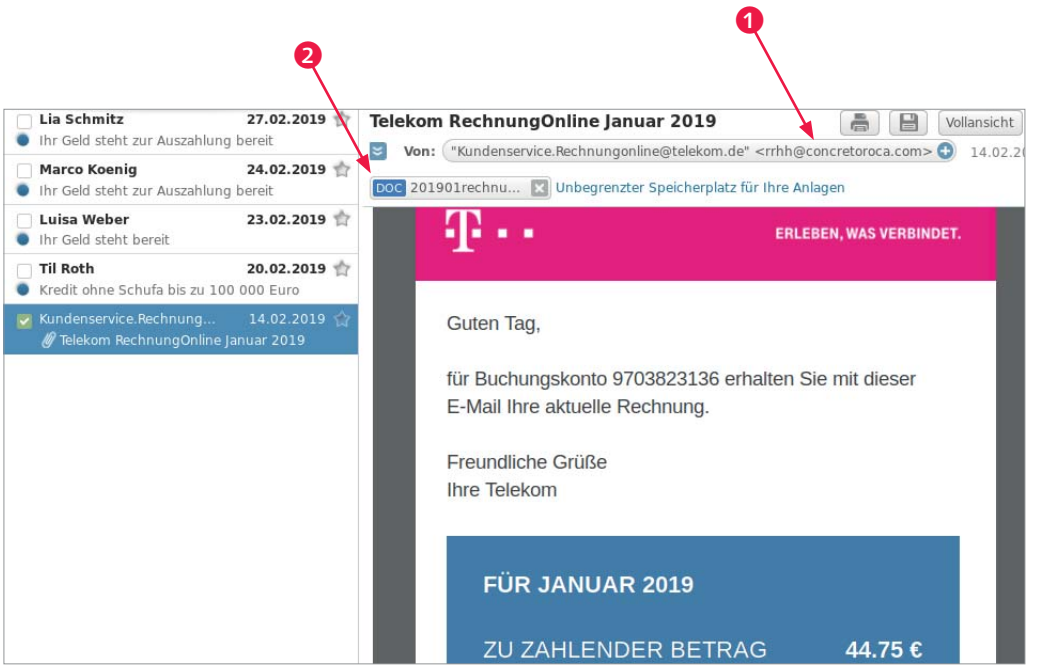
E-Mails, die massenhaft versendet werden, nennen sich **Spam-** oder **Junk-E-Mails**. Sie sind schlicht und ergreifend nervig, kommen sie doch unverlangt in Ihren E-Mail-Account. Der Großteil dieser E-Mails beinhaltet einfach nur Werbung und ist **eher harmlos**. Mittels eines oder mehrerer Hyperlinks werden Sie zu dem entsprechenden Werbetreibenden weitergeleitet.

Phishing-E-Mails wiederum sind darauf ausgelegt, an die Nutzerdaten des Adressaten zu gelangen, um ihm Schaden zuzufügen – sei es ihm persönlich oder seinem Computer.

Folgendes Szenario:

Sie erhalten eine E-Mail, die augenscheinlich vom Onlinebezahldienst PayPal stammt. Die Betrüger setzen darauf, dass ein Teil der Bevölkerung bereits Kunde bei PayPal ist und sich somit durch die E-Mail angesprochen fühlt. Ihnen wird vorgegaukelt, dass es zu unregelmäßigen Abbuchungsvorgängen gekommen sei und Sie sich mittels eines in der E-Mail befindlichen Hyperlinks in Ihrem PayPal-Account anmelden mögen, um entsprechende Überprüfungen vorzunehmen. Sie klicken auf den Hyperlink, landen auf einer gefälschten PayPal-Seite und loggen sich ein. Die Falle ist bereits zugeschnappt – **die Betrüger haben nun Ihre Zugangsdaten**, da Sie sich auf einer durch die Betrüger eigens erstellten Seite eingeloggt haben, die der PayPal-Seite täuschend ähnlich sieht.

Die Betrüger wiederum loggen sich jetzt mit Ihren Zugangsdaten auf der richtigen PayPal-Seite ein, nehmen Geldtransfers vor oder bezahlen hochwertige Waren, die sie sich bestellt haben. In der Abbildung links sehen Sie den Sicherheitsbereich eines PayPal-Kontos. Hier kann ein Betrüger Passwörter ändern und andere sicherheitsrelevante Einstellungen vornehmen.



Auf den ersten Blick eine Rechnung der Telekom,
doch der Absender verschickt gefährliche Schadsoftware.

Phishing-E-Mails mit Anhang

Oftmals ändern die Betrüger auch sofort Ihre Zugangsdaten und Sicherheitseinstellungen, um Sie von Ihrem eigenen Account »auszusperren«. Sie werden große Schwierigkeiten haben, das Ganze wieder in geordnete Bahnen zu lenken, was auch mit einem hohen Zeitaufwand verbunden ist, ganz zu schweigen von dem finanziellen Verlust.

Ein weiteres Beispiel: Sie erhalten eine E-Mail von der Telekom mit einer Rechnung. Auch hier gehen die Betrüger davon aus, dass es in Deutschland eine große Anzahl von Telekom-Kunden gibt, die sich angesprochen fühlen. Möglicherweise können Sie, wenn Sie genau hinschauen, an der Adresse erkennen, dass die Mail nicht von der Telekom stammt ❶. Dieser Rechnungsmitteilung ist ein **Anhang in Form eines DOC-Dokuments** ❷ beigefügt, mit dem Sie Ihre Telefonverbindungen angeblich sofort überprüfen können. Durch Öffnen dieses angehängten Dokuments wird, von Ihnen zunächst unbemerkt, **Schadsoftware auf Ihren Computer aufgespielt** und gestartet. Ihr PC ist nun möglicherweise mit einem **Virus** infiziert, in ein sogenanntes **Bot-Netzwerk** eingebunden, kann ferngesteuert, ausgelesen oder ganz gesperrt werden. Vielfältige Szenarien sind hier denkbar, und keines dieser Szenarien ist ungefährlich.

Tipp

Sie erkennen auf den ersten Blick meist nicht, ob es sich um eine harmlose E-Mail mit nur Werbeinhalt handelt oder um eine gefährlichere Variante. **Klicken Sie niemals auf einen Hyperlink und öffnen Sie nie einen Anhang**, wenn Sie den Absender nicht persönlich kennen und die E-Mail nicht erwartet haben. Auch wenn Sie tatsächlich ein Konto bei der Telefonfirma oder dem Versandhaus haben, löschen Sie die Mail sofort. Danach gehen Sie zum Portal Ihres Anbieters, loggen sich ein und schauen nach, ob dort eine Nachricht für Sie ablegt wurde.

Von: Amazon.de
Gesendet: Samstag, 13. Mai 2017 06:02
An: @web.de
Betreff: Benachrichtigung vom Sicherheitsdienst: #581-22676832-9521004

amazon.de

Meine Sicherheit Mein Konto Amazon.de

Sicherheitsmeldung

E-Mail Referenz: #876-3487551-6137710

Sehr geehrte/r Kunde/in,

bei Ihrem Amazon-Konto wurden verdächtige aktivitäten festgestellt. Wir bei Amazon.de nehmen die Kunden-Sicherheit äußerst ernst. aus Sicherheitsgründen müssen Sie bei Ihrem Nutzerkonto Ihre persönlichen Daten bestätigen. Bis dahin wurde Ihr Nutzerkonto eingeschränkt.

Diese Sicherheitsmaßnahme schützt Sie vor Missbrauch durch Dritte.

Bei der Bestätigung müssen Sie alle nötigen Informationen zu Ihrem Nutzerkonto und Zahlungsdaten eintragen, da Sie sonst nicht mehr in der Lage sind, weitere einkäufe durchzuführen.

Klicken Sie auf den unten angezeigten Link und folgen Sie den Anweisungen.
Wird festgestellt, dass Sie falsche Informationen / falsche Zahlungsdaten eingeben oder diese Bestätigung ignorieren, wird Ihr Nutzerkonto volständig gesperrt und Sie an unsere Sicherheitsabteilung gemeldet.

Weiter (über den Sicherheitsserver)

Nach der Bestätigung wird Ihr Account reaktiviert.
Wir danken Ihnen für Ihr Verständnis.

Mit freundlichen Grüßen
Ihr Amazon Kundenservice

Eine Phishing-E-Mail, mit der versucht wird, an Zahlungsdaten des Empfängers zu gelangen.

Merkmale einer Phishing-E-Mail

Anhand der typischen Merkmale, die auf dieser und der nächsten Seite erläutert werden, können Sie Phishing-Mails gut erkennen:

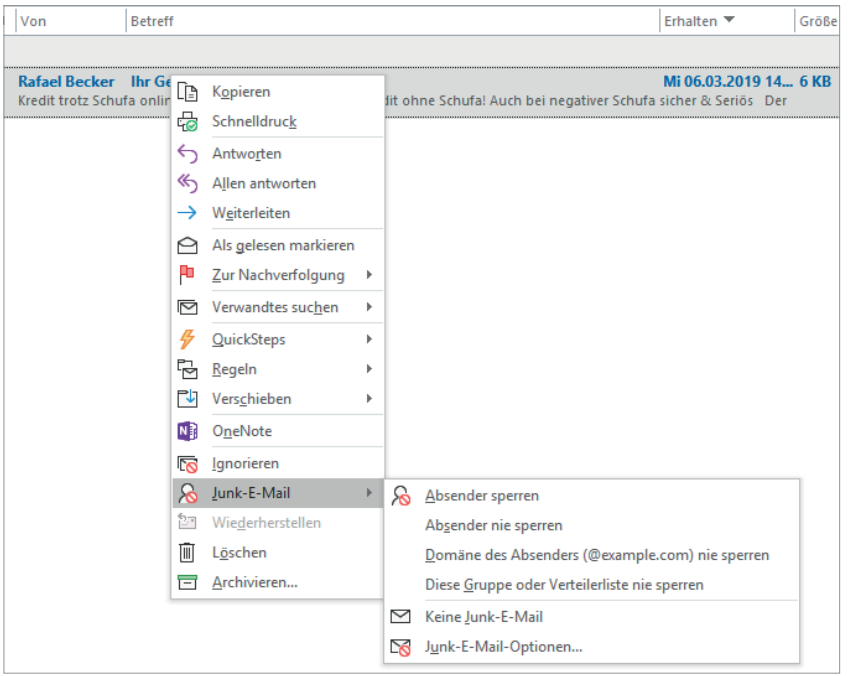
- **Die Absenderadresse entspricht nicht der offiziell bekannten Firmenadresse.**
  Oftmals sieht man es gleich: Der Absender der E-Mail verwendet nicht die »offizielle« E-Mail-Adresse der jeweiligen Firma (siehe Abbildung auf Seite 126, ❶).

- **Rechtschreib- und Grammatikfehler.**
  Diese finden sich immer noch in vielen Phishing-E-Mails, wie auch im Beispiel links. Hintergrund ist, dass viele Betrüger im Ausland sitzen, der deutschen Sprache kaum mächtig sind und sich den in ihrer Sprache erstellten E-Mail-Text durch ein Programm ins Deutsche übersetzen lassen. Typisch ist z. B. auch, dass die Umlaute ä, ö und ü falsch dargestellt werden. Oftmals findet sich nur der Grundvokal (a, o, u) oder die Umschreibung ae, oe, ue in den Texten.

- **Die persönliche Anrede fehlt.**
  In den meisten Fällen fehlt die persönliche Anrede, oder Ihre E-Mail-Adresse ist als Anrede eingesetzt. Gewiefte Betrüger schreiben Sie jedoch persönlich an (falls Ihr Name bekannt ist), um somit eine höhere Seriosität vorzugaukeln.

- **Anhänge.**
  An der E-Mail befinden sich Anhänge zum Öffnen, zumeist in den Formaten **.pdf**, **.zip** oder **.doc(x)** (siehe Abbildung auf Seite 126, ❷). Öffnen Sie einen solchen Anhang keinesfalls! Entweder befindet sich darin ein Schadprogramm oder ein Formular, das Sie mit persönlichen Daten (Bankzugangsdaten, PINs, TANs oder Ähnliches) ausfüllen und übermitteln sollen.

Fortsetzung ⟶



Bei Verdacht auf Phishing können Sie den Absender sperren, hier unter Outlook 365.

Merkmale einer Phishing-E-Mail (Fortsetzung)

- **Drohgebärden, dringender Handlungsbedarf.**
  »Wenn Sie nicht, dann …«. »Handeln Sie sofort, sonst verpassen Sie …«. Finden Sie solche oder ähnliche Sätze in einer E-Mail, werden Sie bitte stutzig. Beispielsweise wird Ihre Hausbank, falls Sie überhaupt E-Mails von dort erhalten, niemals solche Formulierungen innerhalb einer E-Mail verwenden.

- **Keine Geschäftsbeziehung.**
  Falls Sie zum Absender keinerlei Geschäfts- oder sonstige Beziehungen pflegen oder gepflegt haben, löschen Sie die E-Mail getrost.

Tipp

Besteht auch nur der leiseste Verdacht, eine Phishing-Mail bekommen zu haben, empfehle ich, **sie sofort zu löschen**. E-Mail-Programme kann man dahin gehend sogar anlernen: So können offensichtliche Phishing- und Spam-E-Mails beispielsweise als **Spam** oder **Junk** gekennzeichnet werden, und natürlich können Sie den Absender gleich ganz sperren (siehe Abbildung links – hier am Beispiel von Microsoft Outlook 365). Ebenso ist es möglich, Regeln zu erstellen. Enthält die Betreffzeile oder der Text einer E-Mail ein bestimmtes Wort oder kommt die E-Mail von einem bestimmten Absender, kann man diese E-Mail zum Beispiel automatisch löschen oder durch das E-Mail-Programm in einen von Ihnen vorgegebenen Ordner automatisch verschieben lassen. Denken Sie auch daran, den Inhalt des Papierkorbs Ihres E-Mail-Programms regelmäßig zu löschen.

Hallo!

Wie Sie vielleicht bemerkt haben, habe ich Ihnen eine E-Mail von Ihrem Konto aus gesendet.
Dies bedeutet, dass ich vollen Zugriff auf Ihr Konto habe.

Selbst wenn Sie es andern passwort, spielt es keine Rolle. Mein Trojaner wird und copien es abfangen.

Ich habe dich jetzt seit ein paar Monaten beobachtet.
Tatsache ist, dass Sie uber eine von Ihnen besuchte Website fur Erwachsene mit Malware infiziert wurden.

Wenn Sie damit nicht vertraut sind, erklare ich es Ihnen.
Der Trojaner-Virus ermoglicht mir den vollstandigen Zugriff und die Kontrolle uber einen Computer oder ein anderes Gerat.
Das heiBt, ich kann alles auf Ihrem Bildschirm sehen, Kamera und Mikrofon einschalten, aber Sie wissen nichts davon.

Ich habe auch Zugriff auf alle Ihre Kontakte und Ihre Korrespondenz.

Warum hat Ihr Antivirus keine Malware entdeckt?
Antwort: Meine Malware verwendet den Treiber.
Ich aktualisiere alle vier Stunden die Signaturen, damit Ihr Antivirus nicht verwendet wird.

Ich habe ein Video gemacht, das zeigt, wie du befriedigst dich... in der linken Halfte des Bildschirms zufriedenstellen,
und in der rechten Halfte sehen Sie das Video, das Sie angesehen haben.
Mit einem Mausklick kann ich dieses Video an alle Ihre E-Mails und Kontakte in sozialen Netzwerken senden.
Ich kann auch Zugriff auf alle Ihre E-Mail-Korrespondenz und Messenger, die Sie verwenden, posten.

Wenn Sie dies verhindern mochten, ubertragen Sie den Betrag von 377€ an meine Bitcoin-Adresse
(wenn Sie nicht wissen, wie Sie dies tun sollen, schreiben Sie an Google: "Buy Bitcoin").

Meine Bitcoin-Adresse (BTC Wallet) lautet: 1PFMWGRdex7KCYGxLvAZaBdpQHjkebSzvH

Nach Zahlungseingang losche ich das Video und Sie werden mich nie wieder horen.
Ich gebe dir 48 Stunden, um zu bezahlen.

Jetzt bekomme ich Angst

Auf der linken Seite sehen Sie eine E-Mail, die mich während des Schreibens dieses Buchs erreicht hat. Mir wird gedroht, ein Schmuddelvideo über mich im Internet zu veröffentlichen, wenn ich nicht einen gewissen Bitcoin-Betrag bezahle. Der Clou: Der Absender dieser E-Mail bin ich selbst!

Was ist passiert? Wie Sie links nachlesen können, behauptet der Absender, einen Virus auf meinen PC geschleust zu haben, da es ihm nunmehr gelungen ist, mir E-Mails mit meiner eigenen Absender-E-Mail-Adresse übersandt zu haben.

Es ist technisch einfach, E-Mails mit jedweder Absenderkennung zu versenden.

Der Versender ist lediglich – wie auch immer – an meine E-Mail-Adresse gelangt. Mehr nicht. Diese hat er dann zum massenhaften Versenden seiner E-Mails missbraucht. Kopiere ich nun eine beliebige Zeile aus dieser E-Mail und recherchiere damit im Internet (durch Einfügen in eine Suchmaschine), komme ich sogleich zu einem eindeutigen Ergebnis:

Es handelt sich um einen frei erfundenen E-Mail-Text, der jeglicher Grundlage entbehrt. Somit **ab in den Papierkorb** bzw. **gleich ganz löschen**. Sollte ein Hyperlink in einer solchen E-Mail vorhanden sein, bitte nicht anklicken oder sonstigen Kontakt aufnehmen! Und natürlich auch nichts überweisen!

Für die technisch etwas Versierteren der folgende Hinweis: Nach einer Überprüfung des erweiterten E-Mail-Headers wird es sofort klar, dass diese E-Mail nicht vom eigenen E-Mail-Account stammen kann.

Informationen der Polizei zu CEO Fraud, zu finden unter
https://www.polizei-beratung.de/themen-und-tipps/gefahren-im-internet/ceo-fraud/

CEO Fraud, Fake President, Fake Chef

Unterschiedliche Begriffe – eine Bedeutung. Als **CEO** (Chief Executive Officer) bezeichnet man das geschäftsführende Vorstandsmitglied (Geschäftsführer/-in) bzw. den Vorstandsvorsitzenden eines Unternehmens. Das englische Wort **Fraud** bedeutet ins Deutsche übersetzt »Betrug«. Der Begriff **Fake** kommt ebenso aus dem englischen Sprachgebrauch und bedeutet »Fälschung«.

Es läuft auf ein und dasselbe hinaus: Der Betrüger gibt sich als Chef aus und versucht, die Mitarbeiter per E-Mail zu **Geldtransfers auf meist ausländische Konten zu veranlassen**. Hierbei sind oft diejenigen Mitarbeiter Ziel der Attacken, die auch tatsächlich an exponierter Stelle sitzen und die Ermächtigung haben, Geldtransfers zu tätigen. So können z. B. fingierte Rechnungen der Anlass für eine Zahlung sein, oder ein ausländischer Kooperationspartner muss kurzfristig monetär unterstützt werden – Gründe lassen sich viele finden.

Meist haben die Betrüger auf irgendeine Art und Weise **Kenntnisse über die Firmenstrukturen** derjenigen Firmen, auf die sie es abgesehen haben. Die E-Mails werden gezielt versandt, und die darin enthaltenen Rechnungen oder Texte erregen zunächst beim Empfänger keinen Verdacht. Es sieht tatsächlich so aus, als käme die Anweisung der Überweisung von der Firmenspitze.

Zahlungen werden veranlasst, das Geld ist weg. Diese Betrugsmasche hat ahnungslosen Mitarbeitern schon den Job gekostet, da sie ja tatsächlich in gutem Glauben gehandelt haben. Durch CEO Fraud werden in Deutschland ansässigen Unternehmen jährlich Millionenschäden zugefügt.

Auch Vereine bleiben nicht verschont

Dreister geht es kaum: Die Kassiererin eines Vereins erhält eine E-Mail von Ihrem Vereinsvorsitzenden. Die Form der E-Mail gibt keinen Anlass zu Bedenken. Stutzig macht sie jedoch der Inhalt: Demnach soll sie **über das Vereinskonto einen hohen vierstelligen Eurobetrag an eine Privatperson überweisen**. Nach persönlicher Rücksprache mit dem Vereinsvorsitzenden entpuppt sich diese E-Mail als Fälschung.

Dass diese Masche mittlerweile auch bei örtlichen Vereinen versucht wird, ist erschreckend. Darum: Machen Sie diese Betrugsmasche publik! Leiten Sie diese Informationen an die Verantwortlichen Ihres Vereins und auch an die Firma, in der Sie tätig sind, weiter.

Dieser Betrugsmasche geht voraus, dass sich die Gauner mit den Firmen- und mittlerweile auch **Vereinsstrukturen** vertraut gemacht haben (wer Vorstand ist oder das Rechnungsbuch führt). Diese Informationen sind sehr leicht im Internet zu finden.

Einen entsprechenden Zeitungsartikel dazu können Sie hier nachlesen: *https://www.rnz.de/nachrichten/region/polizeibericht-region_artikel,-meckesheim-das-muessen-sie-ueber-die-betrugsmasche-ceo-fraud-wissen-_arid,431334.html*.

Mehr über das Thema finden Sie auf der Seite von *www.polizeiberatung.de* unter *https://www.polizei-beratung.de/themen-und-tipps/gefahren-im-internet/ceo-fraud/*.