Soziale Netzwerke

Gängige Betrugsmaschen erkennen

Betrüger tummeln sich immer dort, wo sich auch potenzielle Opfer aufhalten. Das ist im Internet nicht anders als in der realen Welt. Bei über einer Milliarde Nutzern allein bei Facebook, ist es kein Wunder, dass sich Cyber-Piraten längst einen lukrativen Wirtschaftszweig in sozialen Netzwerken aufgebaut haben.

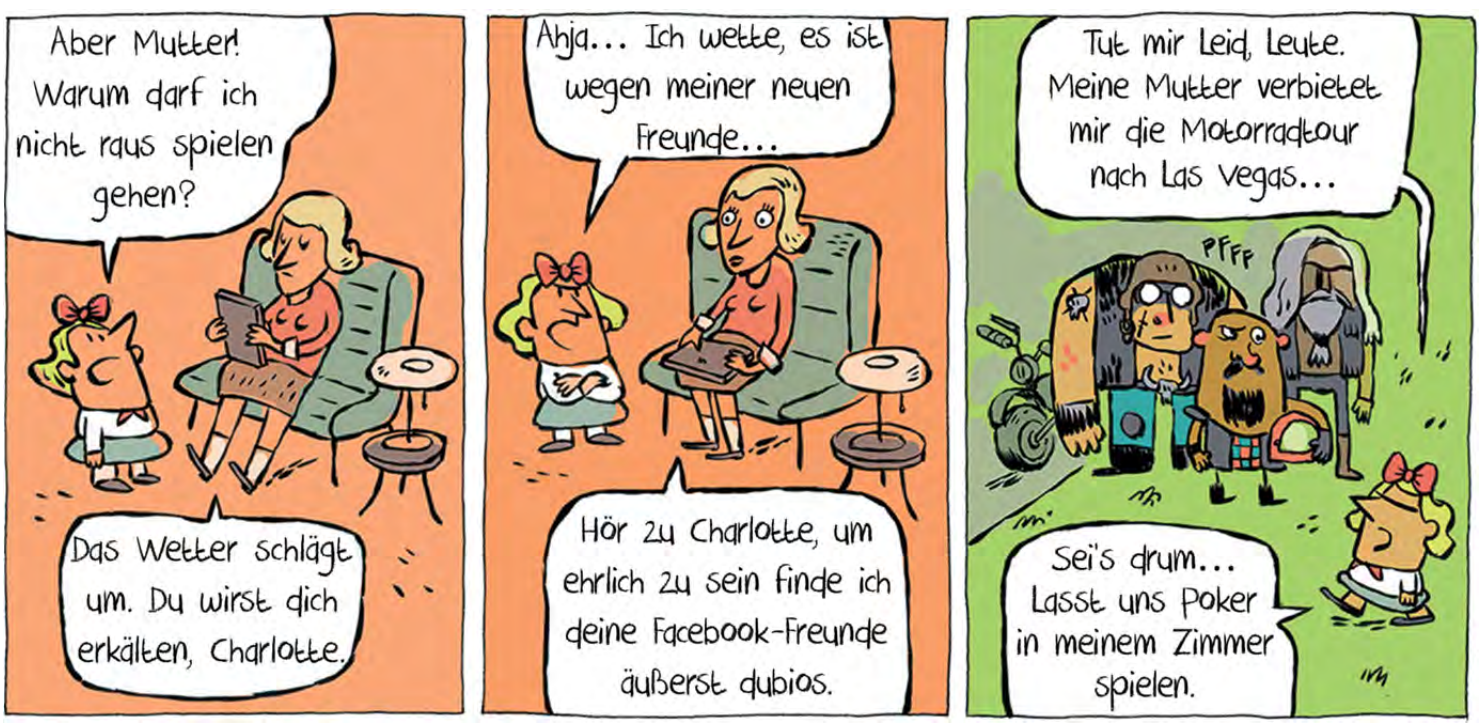
Die Maschen sind zum Teil die gleichen, wie auch beim regulären E-Mail-Verkehr. Der Vorteil für die Angreifer liegt bei Netzwerken wie Facebook & Co in der Anlage eines (Fake-)Profils, mit dem sie sich einfacher Gehör verschaffen, als mit einer anonymen Mail. Darüber hinaus können Kriminelle gezielte und auf ihre Opfer zugeschnittene Angriffe starten.

Geklontes Profil

In Ihrem Namen legt ein Betrüger eine Kopie Ihres Facebook-Profils an. Dazu kopiert er Ihr Profilbild sowie alle Fotos von Ihnen, die, sofern es die Privatsphäre-Einstellungen erlauben, zugänglich sind. Schnell entsteht ein Profil, das dem Ihrem täuschend ähnlich sieht. Schritt zwei der Betrugsmasche: Freundschaftsanfragen an alle Personen schicken, die sich auch in Ihrer Liste befinden. Die Erfolgsquote wird hoch sein, wenn Ihre Freunde glauben, dass es sich tatsächlich um Ihr rechtmäßiges Profil handelt. Der entscheidende letzte Schritt: Per Privatnachricht bittet der Betrüger in Ihrem Namen seine neugewonnenen Freunde, ihm mit etwas Geld aus einer prekären Situation zu verhelfen, oder aber ihn dringend unter einer bestimmten (und natürlich überteuerten!) Telefonnummer anzurufen. Noch perfider: Er fordert Ihre Freunde dazu auf, einen infizierten Phishing-Link zu klicken.

Der Betrüger benutzt Sie als Trittbrettfahrer, um auf illegale Weise an Geld zu gelangen.

Seien Sie streng bei der Einstellungen Ihrer Privatsphäre. Je weniger Außenstehende (und auch Freunde) von Ihnen sehen, umso weniger kann geklaut und für illegale Zwecke missbraucht werden. Seien Sie auch skeptisch, wenn Sie eine Freundschaftsanfrage von Jemandem erhalten, mit dem sie bereits befreundet sind. Vielleicht wurde sein Profil geklont?



Gehacktes Profil

Sie erhalten eine Nachricht von einem Freund, der in der Klemme steckt und dringend etwas Geld von Ihnen borgen will? Ein Facebook-Freund möchte Sie unbedingt von einer Super-Diät überzeugen und hat gleich einen Link für Neueinsteiger mitgeschickt? Ihre beste Freundin schickt Ihnen eine Chatnachricht mit der Buchstabenkombi „lol“ und hängt ein Video daran, das Sie sich anschauen sollen?

Das stinkt nach Betrug! Wenn ein Betrüger ein Facebook-Profil hackt, hat er es nicht nur auf die darauf befindlichen Daten abgesehen, sondern wird vor allem versuchen, das Vertrauensverhältnis des Opfers zu seinen Facebook-Freunden finanziell auszunutzen, beziehungsweise Schadsoftware in Umlauf zu bringen.

Wenn Sie ungewöhnliche Benachrichtigungen von einem Freund erhalten, seien Sie vorsichtig und fragen Sie lieber einmal nach, ob diese wirklich von ihm stammen. Spätestens, wenn Ihr luxemburgischer Freund Ihnen eine Nachricht auf Englisch schreibt, und eine Datei zum Downloaden daran hängt, sollten Ihre Alarmglocken läuten: Auf keinen Fall auf die Datei oder den Link klicken! Freunde, die scheinbar Geldprobleme haben, sollten Sie, wenn Sie helfen wollen, am besten telefonisch kontaktieren.

Gefälschte Facebook-Mail

Sie erhalten eine E-Mail von Facebook, in der Sie dazu aufgefordert werden, sich über den mitgeschickten Link mit Ihrem Facebook-Konto zu verbinden, um z.B. Fotos zu sehen, auf denen Sie markiert wurden, oder die Benachrichtigung eines Freundes zu lesen.

Hierbei könnte es sich um eine Phishing-Mail handeln. Kriminelle versuchen, Sie mit täuschend echt aussehenden Mails und Phishing-Webseiten zum Eingeben Ihrer persönlichen bzw. Ihrer Login-Daten zu bewegen, oder Ihnen ein Schadprogramm unterzujubeln.

Wenn Sie gar nicht bei Facebook angemeldet sind, löschen Sie diese E-Mail. Klicken Sie nicht auf mitgeschickte Links oder Dateianhänge. Besser ist es, sich direkt über ein neues Browserfenster bei Facebook anzumelden (Adresse manuell eingeben) und sich selbst davon zu überzeugen, was es alles Neues gibt.

Falsche Gewinnspiele, falsche Gutscheine und vermeintliche Gratis-Angebote

Ein Gutschein im Wert von 30 Euro von Ihrer Lieblings-Bekleidungskette? Und das ganz ohne Eigeninitiative? Sie klicken auf die verlockende Werbeanzeige im Facebook-Newsfeed und gelangen auf eine Webseite, wo Sie ein Formular nach dem anderen ausfüllen müssen…

Auf Facebook wimmelt es nur so von Werbeanzeigen. Einige davon sind nicht legitim: Mit Logos bekannter Marken wird Seriosität vorgegaukelt, tatsächlich aber geht es darum, möglichst vielen Opfern private Daten zu entlocken oder sie in eine kostspielige Abo-Falle zu locken. Von vermeintlichen Gewinnen, Gutscheinen oder Gratis-Produkten sehen die Opfer nichts.

Auf Facebook schenkt Ihnen niemand etwas. Vertrauen Sie Ihrem gesunden Menschenverstand und lassen Sie sich nicht von illusorischen Versprechen blenden. Spätestens wenn Sie zur Eingabe persönlicher Daten oder zum Herunterladen eines spezifischen Programms aufgefordert werden, sollten Sie schnell einen Schlussstrich ziehen! Ansonsten riskieren Sie, Opfer eines Phishing-Betrugs zu werden, bzw. ungewollt ein teures Produktabonnement zu unterschreiben.

Love-Scam

Sie scheinen im sozialen Netzwerk Ihren Traumpartner gefunden zu haben… Getroffen haben Sie sich zwar noch nie, aber so wie er/sie schreibt, müssen Sie seelenverwandt sein. Die Gefühle sind stark, und auch die Bilder Ihrer neuen Bekanntschaft sind überzeugend attraktiv. Über Wochen oder sogar Monate hinweg schreiben Sie sich fast täglich. Treffen wollen Sie sich auch, aber leider ist Ihr(e) Liebste(r) gerade im Ausland auf Geschäftsreise und kann wegen gestohlenem Portemonnaie nicht zu Ihnen kommen. Klar, dass Sie ihm/ihr mit einigen tausend Euro aus der Patsche helfen, damit er/sie die nötigen Dokumente beantragen und ein neues Flugticket kaufen kann, oder?

Professionelle Liebes-Betrüger wickeln meist mehrere Bekanntschaften gleichzeitig um den Finger. Sie sind Experten darin, mit Geduld ein Vertrauensverhältnis aufzubauen, infolge dessen dann eine auf den ersten Blick logische Geschichte mit der Bitte nach finanzieller Unterstützung auf den Tisch kommt. Sie sind einzig und allein auf das Geld Ihrer Opfer aus.

Spätestens wenn Ihre Online-Bekanntschaft Sie um Geld bittet, sollten Ihre Alarmglocken läuten. Beenden Sie das Verhältnis und schicken Sie keine Nacktbilder oder sonstige private Informationen, mit denen die Betrüger Sie erpressen könnten.

Sextortion

Sextortion bedeutet Erpressung mit sexuellem Inhalt. Das typische Szenario in sozialen Netzwerken ist Folgendes: Als Mann werden Sie von einer überaus attraktiven unbekannten Frau kontaktiert. Diese kommt schnell zum Wesentlichen: Sie hat Lust auf mehr…ganz unverbindlich natürlich… und Sie sollen mitmachen, indem Sie Ihre Webcam einschalten und sich bei sexuellen Handlungen filmen.

Die Webcam wird Ihnen zum Verhängnis. Hinter der attraktiven Verführerin stecken Betrüger, die Ihre vermeintlich private Webcam-Einlage aufzeichnen und drohen, damit an die Öffentlichkeit zu gehen. Es sei denn, Sie bezahlen Ihren Erpressern ein happiges Lösegeld.

Man kann es nicht oft genug sagen: Nacktbilder im Internet sind tabu! Falls es Sie doch einmal erwischt hat, denken Sie daran: Auch wenn Sie das Lösegeld zahlen, haben Sie keine Garantie, dass Ihr Video gelöscht wird, und es nicht noch zu weiteren Erpressungen kommt.

Erstatten Sie schnellstmöglich Anzeige bei der Polizei. Werden Ihre Bilder in sozialen Netzwerken oder auf anderen Webseiten veröffentlicht, fordern Sie die Seitenbetreiber dazu auf, diese sofort zu entfernen.

Als Video/Status getarnte Links

„Sie werden nicht glauben, was dieses schwangere Mädchen tut…!“ „Unglaublich…das muss man sehen, um es zu glauben!“ Solche oder ähnliche Schlagzeilen sollen neugierig machen und den User dazu verleiten, auf das Video in der Facebook-Timeline zu klicken. Komisch nur, dass man überhaupt kein Video sehen kann, sondern auf eine Webseite weitergeleitet wird.

Bei solchen vermeintlichen Schocker-Beiträgen handelt es sich um Links, die als Video getarnt wurden, um so möglichst viele Klicks zu erhaschen. Die Konsequenzen für den Benutzer hängen von der Art der Webseite ab, auf die er weitergeleitet wird. Im günstigsten Fall landet er „nur“ auf einer unbedeutenden Seite, für die geworben werden soll. Oft steht auch das Sammeln von Daten im Vordergrund, unter dem Vorwand, zum Anschauen des Videos müsse man volljährig sein und zur Überprüfung des Alters die persönlichen Daten angeben. Im schlimmsten Fall handelt es sich dabei um eine schädliche Webseite, die zum Herunterladen einer mit Malware infizierten Datei aufruft.

Seien Sie skeptisch bei allzu schockierenden Schlagzeilen, oder bei Videos, bei denen der Titel nichts über den tatsächlichen Inhalt aussagt. Wenn Sie auf eine Webseite weitergeleitet werden, führen Sie dort keine Downloads durch und geben Sie keine persönlichen Daten ein.

Über aktuelle Falschmeldungen und Betrugsmaschen informiert das österreichische Portal Mimikama (www.mimikama.at).

Infizierte Statusmeldungen

Sie erhalten eine Benachrichtigung, dass ein Freund Sie in einem Video oder einer Statusmeldung markiert hat. Klar, dass Sie sehen wollen, um welchen Beitrag es sich dabei handelt.

Wollen Sie das Video anschauen, laden Sie sich unbemerkt ein Schadprogramm auf Ihren Computer. Gleichzeitig postet der Trojaner in Ihrem Namen den infizierten Link auf der Facebook-Pinnwand weiter und markiert automatisch Freunde darin – die nächsten Opfer und Katalysatoren, die dafür sorgen, dass die Malware im Umlauf bleibt und ihren Infektionsradius vergrößern kann.

Seien Sie skeptisch bei Video-Posts. Wenn Ihr Freund keinen Kommentar dazu geschrieben hat, sondern nur Buchstaben- und Zahlenkombinationen wie z.B. „WTFF……f6h7qr" oder ähnlich, handelt es sich mit Sicherheit um einen Trojaner, der die Runde macht, und dem auch Ihr Freund zum Opfer gefallen ist. Halten Sie Ihr Antivirenprogramm stets auf dem neusten Stand und informieren Sie sich auf Seiten wie dem österreichischen Portal Mimikama (www.mimikama.at) über aktuelle Betrugsmaschen.

Gefälschte Fanseiten

Gefälschte Fanseiten sind auf den ersten Blick oft gar nicht als solche zu erkennen. Sie profitieren von der Bekanntheit und Beliebtheit einer bestehenden Marke (z.B. Apple oder Mc Donalds), um schnell viele Likes zu sammeln. Anschließend verleiten Sie mit vermeintlichen Gewinnspielen, Gutscheinen oder anderen Inhalten zum Klicken.

Wer klickt, landet wahrscheinlich auf einer externen Webseite, die nichts mehr mit Facebook zu tun hat. Hier warten weder Gratis-Angebote, noch Gewinnspiele. Stattdessen wird der User wahrscheinlich zur Eingabe persönlicher Daten aufgefordert (die anschließend weiterverkauft werden), oder ihm wird im schlimmsten Fall ein Trojaner auf den Computer installiert.

Bevor man einer Fanseite auf Facebook beitritt, sollte man überprüfen, ob es sich auch um die richtige handelt. Dazu geht man am besten auf die offizielle Webseite der Marke und sucht nach dem Link zur Facebook-Seite. Bei Angeboten, die zu schön sind, um wahr zu sein, sollten die Alarmglocken läuten. Großkonzerne wie Apple und Co haben keine Smartphones zu verschenken – auch wenn diese angeblich durch fehlende Verpackung nicht mehr verkäuflich sind…

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

Unveränderte nichtkommerzielle Vervielfältigung und Verbreitung ist ausdrücklich erlaubt.
http://creativecommons.org/licenses/by-nc-nd/3.0/de/

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