Phishing-Know-how: So entlarven Sie bösartige Mails

Jeder zweite Internetnutzer ist Opfer von Cybercrime. Wir zeigen, wie Sie solche Phishing-Attacken erkennen und sich schützen können.

Immer mehr Internetnutzer werden Opfer von Internetbetrügern. Die größte Bedrohung besteht auch heute noch durch Malware wie Viren, Trojanern und Erpressersoftware, gefolgt von Identitätsdiebstahl. Gegen die meisten PC-Viren hilft ein gutes Antivirentool (siehe dazu unseren Test ab **Seite 134**) und das sofortige Einspielen von Programmupdates für alle installierten Anwendungen. Damit Sie zudem kein Update gegen schlimme Sicherheitslücken verpassen, können Sie etwa das **Sumo** (*www.kcsoftwares.com/?sumo*) einsetzen. Auf Wunsch installiert es die meisten Updates sogar automatisch, bei den übrigen zeigt es eine Info an. Gegen den Identitätsdiebstahl durch betrügerische Mails und Webseiten hilft es, stets wachsam zu sein und bei Verdacht Mails auf die nachfolgend aufgezeigten Tricks zu analysieren.

Phishing-Angriffe per Mail: die unterschätzte Gefahr

Betrüger arbeiten mit psychologischen Tricks, damit ihr Opfer auch tatsächlich auf den Link in der Phishing-Mail klickt und später auf der gefälschten Website seine Daten preisgibt. Sie drohen etwa mit hohen Kosten, die entstehen, wenn der Empfänger nicht den Anweisungen gemäß handelt.

Immer noch stark verbreitet ist außerdem ein Trick bei Paypal-Kunden. Betrüger senden Mails, die von einer Kontensperrung berichten. Nur wer sich wieder einloggt, kann sein Konto auch wieder nutzen. Der Link zum Freischalten führt wie in allen Fällen von Phishing natürlich auf eine betrügerische Website.

So werden Phishing-Mails besonders glaubhaft manipuliert

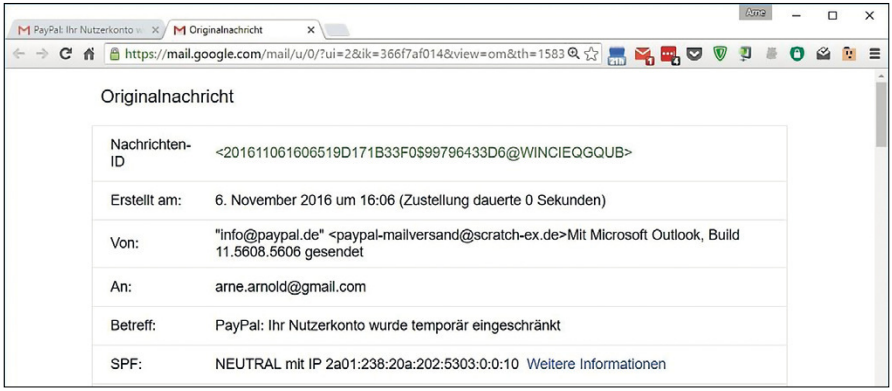
Die betrügerischen Mails müssen gar nicht perfekt gemacht sein, um möglichst viele Opfer zu finden. Wichtiger ist, dass das Opfer durch Zufall kurz vor der Mail etwas mit dem benannten Dienst zu tun hatte. Haben Sie etwa abends in einem Online-Shop per Paypal bezahlt und finden Sie morgens eine Nachricht von Paypal in Ihrem Postfach, dürfte Sie das naturgemäß interessieren. Steht dann etwas von Kontensperrung in der Nachricht, sind Sie wahrscheinlich alarmiert. Denn wer will schon als säumiger Zahler dastehen, nachdem man etwas gekauft hat? Wer in einem solchen Moment des Schreckens reagiert, der klickt wahrscheinlich auf den Link in der Mail und gibt in der Folge seine Daten preis.

Einfacher Schutz gegen Phishing-Mails

Diesen Tipp kennen Sie: Klicken Sie nicht auf Links in verdächtigen Mails von Ihrer Bank oder von Bezahldiensten. Und genau genommen, können Sie hier das Wort „verdächtigen" streichen! Denn wenn Ihnen Ihre Bank, Amazon, DHL, Paypal oder Ebay etwas Wichtiges mitzuteilen hat, dann werden Sie diese Information fast immer auch in Ihrem Kundenkonto auf der jeweiligen Website finden. Statt auf den Link in einer Mail zu klicken, starten Sie einfach Ihren Internetbrowser, geben eigenhändig die Adresse des Dienstes ein und melden sich an. Viele Dienste zeigen nach dem Einloggen neue Mitteilungen an. Bei anderen sind Probleme im Kontenverlauf leicht zu erkennen, etwa bei Paypal. Sollte bei einem fraglichen Dienst kein Mitteilungspostfach vorhanden sein und sich auch sonst nichts Erhellendes aus dem eigenen Kundenkonto ergeben, dann suchen Sie auf der Website die Hotline-Nummer oder die Support-Mail. Melden Sie sich dort, um die in der Mail genannten Probleme anzusprechen. Wenn Sie den Weg per Mail wählen, dann können Sie auch die fragliche Phishing-Mail dorthin weiterleiten und um Stellungnahme bitten.

So enttarnen Sie gefälschte Links in Phishing-Mails

Wenn Sie eine Phishing-Mail selbst analysieren möchten, dann sehen Sie sich zunächst die enthaltenen Links an. Interessant ist der zentrale Link in der Mail, der auch inhaltlich hervorgehoben ist. Verlinkungen oben oder unten in der Mail rufen meist die echte Website auf, um so die Glaubwürdigkeit zu erhöhen.



› Wenn Sie sich etwa bei Gmail den Header zu einer Mail anzeigen lassen, erkennen Sie einfache Absendermanipulationen sofort: Hier etwa, dass nicht „info@paypal.de" stimmt, sondern „paypal-mailversand@scratch-ex.de.

Die Kriminellen verstecken den Link in einer Mail meist hinter harmlosen Text oder einer Textgrafik. Der Text kann etwa *„www.paypal.com"* lauten, oder in der Grafik steht *„Informationen aktualisieren"*. Um an den tatsächlichen Link dahinter zu kommen, führen Sie die Maus darüber, aber ohne zu klicken. Es öffnet sich dann entweder ein kleines Pop-up mit dem Link, oder das Mailprogramm zeigt den Link unten in der Infozeile an. Dort gibt es aber oft zu wenig Platz, um den kompletten Link anzuzeigen. Es ist dann übersichtlicher, wenn Sie sich den Link kopieren und etwa in einen Editor oder eine Textverarbeitung einfügen. Klicken Sie dafür mit der rechten Maustaste auf den Text oder die Grafik mit dem dahinterliegenden Link und wählen Sie *„Link kopieren"*.

Aufbau einer Webadresse: Um einen Link analysieren zu können, müssen Sie den Aufbau einer Webadresse kennen. Die Adresse besteht aus einer Domain und einer Top Level Domain (TLD). Davor steht eine Angabe zum verwendeten Protokoll. Bei Webseiten ist das http:// oder https://, wobei http:// oft nicht mit angezeigt wird, meist aber die Angabe www. Also im Prinzip https://www.domain.TLD oder etwa https://www.paypal.com. Die Domain kann man sich als Website-Betreiber frei aussuchen, sofern sie nicht bereits vergeben ist. Als TLD sind oft die Länder-Domains (englisch: Country Code Top-Level-Domains, CCTLD) üblich. In Deutschland also .de. Daneben gibt es einige generische TLD (GTLD), etwa .com für commercial, .gov für government oder .org für organization. Außerdem gibt es seit etwa 2014 etliche weitere Domains, etwa. ag, .berlin, .bio, .cash, .center .club, .tips, oder .versicherung. Sie können also auch auf eine Internetadresse wie diese stoßen: www.beste.versicherung.

Analyse eines Phishing-Links an zwei Beispielen

Leicht zu erkennen sind IP-Adressen wie hier: *„http://181.41.219.174/zj0lmRV7t"*.
Er stammt aus einer Phishing-Mail für 1und1-Kunden. Aber kein seriöser Dienst versendet Links auf IP-Adressen. Sie sind also schon fertig mit der Analyse.

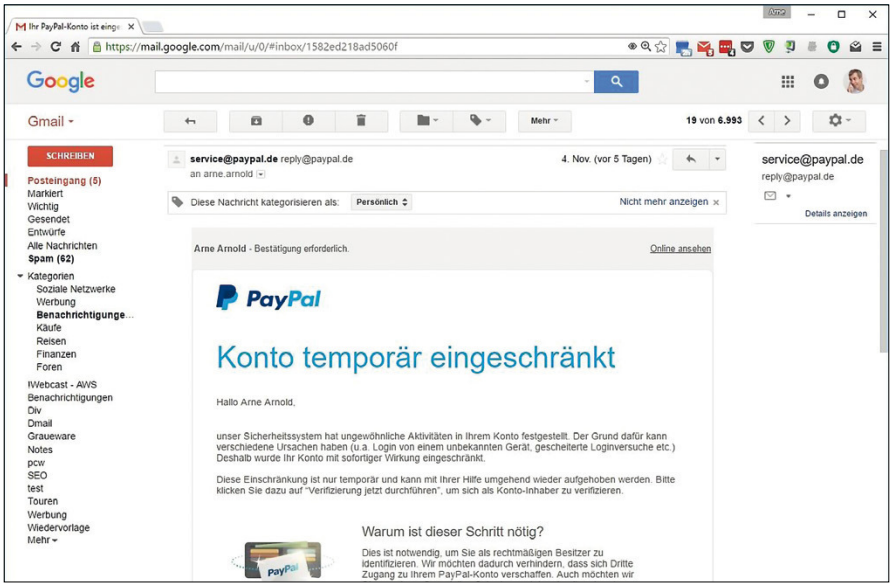
Möchten Sie dennoch weiterforschen, dann geben Sie die IP-Adresse in das Eingabefeld auf *https://network-tools.com* ein und drücken auf *„Go"*. Nach kurzer Zeit wird Ihnen rechts unter *„Domain Name"* die zugehörige Domain genannt. In diesem Beispiel ist das „advicecenterrevise.com". Diese Adresse ist nicht grundsätzlich verdächtig, es lässt sich aber auch kein Zusammenhang zu 1und1 herstellen.

Auf den ersten Blick etwas undurchschaubar erscheint der Link hinter dem Verifizierungsfeld in einer Phishing-Mail an Paypal-Kunden. Er beginnt so: *http://megaurl.co/d9d4r3wh5zf7foer7bp9845dg697jfszlsprd591j7vfew09bkbllwb0oya5ocycha5g6mcinhj7hx2mah4wlgf622d5g2 qjlmfxs2zxuhm4jtjz8j0zmc3itc1iss2p7zmmdrbflbjr45k-8g0oaokbf0yz1h9smhnsuvkddfsgh9igteg-2eu9z78dpirxnham5bzoz6ypogs7vmbv.*

#foyaw2g6t1fkdicraps7arx62nq2f57wretpdm8ycritel0d5u9wp-154fkvj3trdqh8mypf rinssaacocme39231. Allerdings hört er nicht bei der *„1"* auf, sondern geht noch fast 700 Zeichen weiter.

Doch mit dem Wissen um den Aufbau einer URL kommen Sie ganz leicht an die tatsächliche Domain. Streichen Sie gedanklich die zwei Schrägstriche nach *„http:"*. Jetzt suchen Sie den ersten Schrägstrich oder das erste Fragezeichen von links und prüfen das Wort davor, um die Top Level Domain zu finden. Es ist *„.co"*. Die Domain seht immer links davor. Es ist somit *„megaurl."*. Der ganze Text nach *„.co"* dient nur der Verwirrung. Wenn Sie megarurl.co in den Browser eingeben, gelangen Sie zu einem Dienst, der eine vorhandene URL verlängert. Er macht also genau das Umgekehrte von URL-Verkürzern wie Bit.ly oder Tiny-URL. In allen Fällen lassen sich die letztendlichen Ziel-Adressen nicht sofort erkennen.

Achtung: Wollen Sie die Domain absolut gefahrlos in einem Browser eingeben, empfiehlt es sich, einen Browser in einem virtuellen PC zu nutzen. Denn sollte hinter der Webadresse keine Phishing-Website, sondern eine virenverseuchte Site warten, sind Sie in einer virtuellen Maschine gut geschützt. Am einfachsten bekommen Sie mit dem Tool **Bitbox** (*https://cybersecurity.rohde-schwarz.com/de/produkte/endpoint-sicherheit-management/rsrbrowser-box*) einen virtuellen Browser.



› Hier sehen Sie eine gut gemachte Phishing-Mail. Der Absender scheint plausibel, das Layout ist vertraut, und auch der Text fordert eine scheinbar durchaus nachvollziehbare Verifizierung.

So ermitteln Sie den Absender einer Mail

Eine Phishing-Mail verrät sich aber nicht nur durch die enthaltenen Links, sondern auch durch den gefälschten Absender. Diese Fälschung ist unter Umständen allerdings nur schwer zu durchschauen und die nötige Analyse etwas aufwenig. Dazu ein einfaches Beispiel. Eine Mail gibt vor, von Payback zu stammen. Nachrichtentext und enthaltene Bilder sind so gut gemacht, dass sie tatsächlich von Payback stammen könnten. Der Mailabsender lautet auf „payback@punkte.payback-de.pw". Eine genaue Untersuchung der Mail würde ergeben, dass die Mail tatsächlich von dieser Adresse stammt. Der Grund dafür ist einfach: Die Adresse gehört den Kriminellen. Eine Header-Analyse bringt Ihnen also nur etwas, wenn es einen Unterschied zwischen vorgeblichem Original und tatsächlicher Mailadresse gibt.

Von woher stammt eine Mail wirklich? Lassen Sie sich nicht von der Adresse täuschen, die Ihr Mailprogramm oder Browser als Mailabsender anzeigt. Diese Angabe lässt sich leicht fälschen. Möchten Sie sich den echten Absender genauer ansehen, benötigen Sie die Infos aus dem Mail-Header, auch Internetkopfzeilen genannt. Das ist der Teil der Mail, in dem die Protokolldaten der Übermittlung gespeichert sind. Alle gängigen Mailprogramme und Webmailer verbergen diese Infos allerdings zunächst.

So kommen Sie bei gängigen Mailclients an den Mail-Header:

Outlook 2013/2016: Öffnen Sie die Mail und wählen Sie *„Datei / Eigenschaften"*. Markieren Sie den kompletten Text im Feld *„Internetkopfzeilen"* und kopieren Sie ihn mit der Tastenkombination Strg-C.

Thunderbird: Markieren Sie die Mail, und wählen Sie *„Ansicht / Nachrichten-Quelltext"*. Markieren Sie im neuen Fenster alles bis einschließlich *„to: "*, und kopieren Sie den Text mit dem Hotkey Strg-C.

Gmail (Webmail): Lassen Sie sich die Mail anzeigen, und klicken Sie rechts oben auf den kleinen Pfeil gleich neben dem Antwortenpfeil. Wählen Sie dort *„Original anzeigen"*. Markieren Sie im neuen Fenster alles bis einschließlich *„to: "*, und kopieren Sie den Text mit der Tastenkombination Strg-C.

GMX (Webmail): Öffnen Sie die Mail und klicken Sie rechts oben auf das kleine *„i"* neben der Uhrzeit. Markieren und kopieren Sie den Text aus dem neuen Fenster.

Mail-Header aufbereiten und analysieren

Die besten Hinweise über die Herkunft der Mail stecken in den Received-Zeilen. Jeder Server, der die Mail an Sie weiterleitet, fügt oben eine neue „Received:"-Zeile mit den Infos *„from"* (Absender) und *„by"* (Serveradresse) ein. Beim Mailversand sind mindestens zwei Mailserver beteiligt. Es können aber auch eine ganze Reihe von Servern die Mail weitergeleitet haben. Vertrauenswürdig ist nur der letzte Eintrag, denn das ist die Received-Zeile Ihres eigenen Mailproviders. Alle Zeilen davor können gefälscht sein.

Dennoch lohnt sich ein Blick auch auf die untersten Zeilen, da sich nur wenige Phisher die Mühe machen, an dieser Stelle zu manipulieren. Sie begnügen sich stattdessen damit, den Eintrag in der Zeile *„From"* zu manipulieren, wo etwa info@paypal.de angegeben ist. Starten Sie dazu das Programm **eToolz** (*www.gaijin.at/dlet.php*), und wählen Sie oben *„Header Analyzer"*. Fügen Sie den eben kopierten Text in das Feld *„Kopfzeilen"*, und klicken Sie auf *„Start"*. Das Tool listet nun unter *„Received-Übersicht"* die Einträge aller beteiligter Mailserver auf. Es beginnt aber mit dem zeitlich ersten und damit genau umgekehrt wie im Original-Header.

Hinter *„Gesendet von"* steht die IP-Adresse des ersten absendenden Servers. Kopieren Sie diese, und fügen Sie sie ins Eingabefeld auf der Website *http://network-tools.com* ein und klicken dort auf *„Go"*. Die Website versucht, möglichst viele Infos über die IP zu erhalten.

Kontrollieren Sie im Programm eToolz weiterhin die Original-Received-Zeile (unter *„Received-Details"*). Dort finden sich meist Hinweise auf den ersten Mailserver.

Mail-Header am Smartphone analysieren

Gängige Mail-Apps für Android gewähren Ihnen keinen Zugriff auf den Mail-Header einer Nachricht. Damit Sie dennoch an diese Infos kommen, installieren Sie sich die insgesamt empfehlenswerte App **K-@ Mail – E-Mail App** (*https://play.google.com/store/apps/details?id=com.onegravity.k10.free&hl=de*). Das Einrichten eines Mailkontos läuft wie gewohnt über einen Assistenten und bedarf in der Regel nur Mailadresse und Passwort. In den Einstellungen können Sie später festlegen, dass Mails nur manuell abgerufen werden. Das ist sinnvoll, wenn Sie eine andere Mail-App als Standard-App fürs Mailen behalten möchten.

Mail-Header kopieren: Öffnen Sie in K-@ Mail – E-Mail-App eine verdächtige Mail und tippen Sie auf *„Menü-Symbol / Kompletten Header anzeigen"*. Den dann angezeigten Header kopieren Sie wie Text aus einem Editor: Doppeltippen Sie auf den Text und wählen Sie *„Alles markieren"* und dann *„Kopieren"*.