www.bundespolizei-virus.de /it-sicherheit/phishing/

Was ist Phishing und wie kann ich mich schützen?

- Startseite
- IT-Sicherheit
- Phishing

7. Januar 2023 | Von: ,

Felix Bauer


Felix Bauer

Felix Bauer ist Security Consultant und beriet bereits zahlreiche Unternehmen als IT-Sicherheitsexperte. Felix Bauer schrieb zahlreiche Fachartikel für IT-Fachmagazine (u. a. für Computerwelt, IT-Administrator und für die Nachrichten-Website Heise online). Zudem findet Felix Bauer Erwähnung in diversen Büchern sowie in Fach- und News-Beiträgen (u. a. in der Wiener Zeitung, in der Computerworld und auf dem Nachrichtenportal Watson). Schauen Sie sich Felix Bauers Referenzen an.

Felix Bauer hat bereits mehr als 20 Jahre Erfahrung in der IT-Sicherheitsbranche.

Seit einigen Jahren beschäftigt sich Felix Bauer intensiv mit Virenscannern und deren verhaltensbasierter Erkennung. In seinem Blog berichtet er regelmäßig über aktuelle Themen der IT-Sicherheit.

Akademischer Grad: Felix Bauer besitzt den Abschluss Master of Science in Security and Forensic Computing.

René Hifinger

René Hifinger

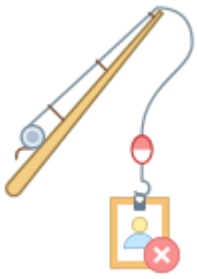
René Hifinger beschäftigt sich bereits seit einigen Jahren mit den Themen IT-Sicherheit, Datenschutz und neue Technologien. Erste Erfahrungen sammelte er in verschiedenen Sicherheitsforen und auf diversen IT-Portalen. Er hat zahlreiche Fachartikel zu unterschiedlichen IT-Sicherheitsthemen veröffentlicht - u. a. für die österreichische Fachzeitung Computerwelt, für das Magazin Informatik-Aktuell und für das Magazin DIGITALE WELT. Weitere Fachartikel und Veröffentlichungen von René Hifinger finden Sie hier.

Abseits von Security-Themen verfügt René Hifinger über fundiertes Fachwissen im Bereich Softwareentwicklung. Er beherrscht die Programmiersprachen C, C ++, HTML, JavaScript, PHP und Python.

René Hifinger berät Unternehmen weltweit in den Bereichen IT-Sicherheit und Softwareentwicklung. Er bringt über 15 Jahre Erfahrung mit und hat für verschiedene Unternehmen gearbeitet.

In unserem Alltag nutzen wir mittlerweile wie selbstverständlich E-Mails. Längst haben auch Cyberkriminelle dieses Medium als guten und darüber hinaus auch kostenlosen Weg mit hoher Reichweite entdeckt. Laut einem aktuellen Bericht der IT-Sicherheitsfirma CybSafe ist die Zahl der Phishing-Mails in den vergangenen 2 Jahren rasant angestiegen[1]. Dem Bericht zufolge wurden der IT-Sicherheitsfirma im vergangenen Jahr (2019) 877 Phishing-Fälle gemeldet – zum Vergleich: 2017 waren es „lediglich“ 16 Fälle. Meist handelte es sich um ungezielte Massenangriffe. Gezielte Angriffe (Spear-Phishing) werden jedoch immer beliebter.

Was ist Phishing?

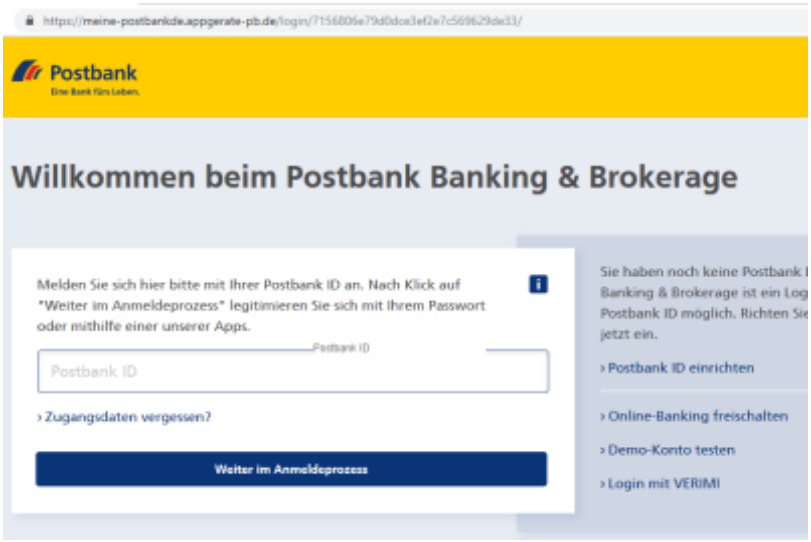


Das Ziel von „Phishing-Mails“ ist es, den Empfänger dazu zu bringen, Zugangsdaten preiszugeben oder eine schädliche Datei zu öffnen. Bankkunden beispielsweise werden beim Phishing (abgeleitet von „fishing“, engl. für „Angeln“) von Kriminellen dazu verleitet, ihre vertraulichen Bankdaten herauszugeben. Die Täuschung ist oft hoch professionell ausgeführt und nur schwer zu erkennen.

In einem typischen Phishing-Szenario erhält man eine E-Mail, die angeblich von der eigenen Bank gesendet wurde. Diese enthält meistens eine kurze Erklärung und die Aufforderung, auf einen Link zu klicken. Als Vorwand kann zum Beispiel ein technisches Problem bei der Bank dienen. Klickt man auf den Link, wird man auf eine Webseite geleitet, die Daten über eine täuschend echte Anmeldemaske abgreift.

Ein Phishing-Beispiel:

Eine angebliche E-Mail von der Postbank. Klicken Sie auf den Link, landen Sie nicht bei Ihrer Bank, sondern auf einer manipulierten Internetseite:



Schutz vor Phishing-Angriffen

Achtsamkeit ist leider keine Garantie, denn auch die Phishing-Strategien der Betrüger werden ausgefeilter und immer schwieriger zu identifizieren. Oftmals kann man optisch also nicht unterscheiden, ob gute oder böse Absichten hinter einer E-Mail stecken. Aber dennoch gibt es wiederum einige Hinweise, die einen Phishing-Angriff vermuten lassen.

Phishing-Angriffe erkennen

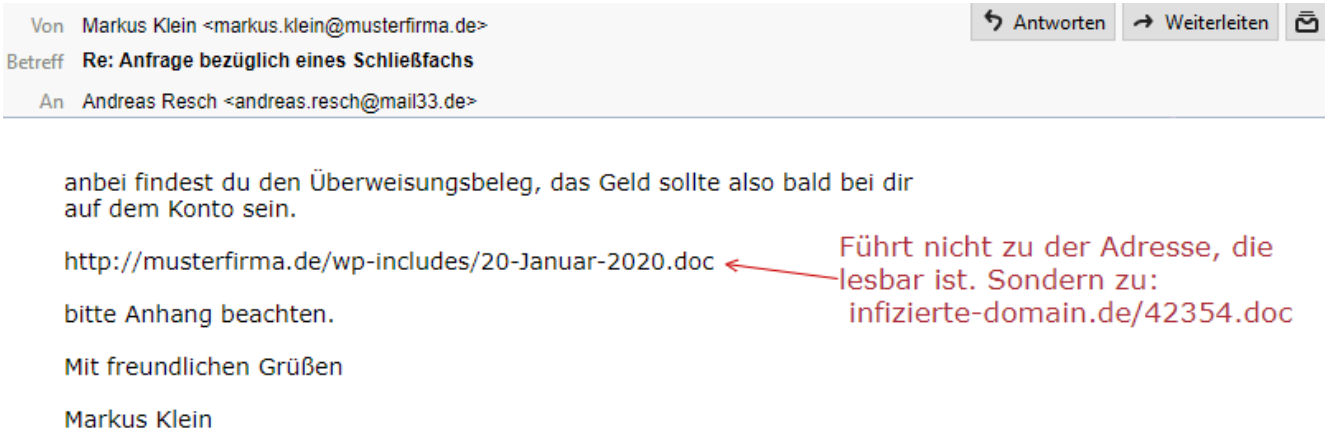
- Schauen Sie sich die Absender-Adresse der E-Mail genau an. Hier ist es wichtig, nicht nur den angezeigten Namen, sondern die dahintersteckende E-Mail-Adresse zu prüfen. Wichtig: Leider

entsprechen die Informationen, welche im Mail-Header stehen, oft nicht der Wahrheit. Die meisten Absenderangaben gehören nicht zu einer existierenden Mailbox. Jeder SMTP-Server muss alles entgegennehmen, was ihm angeboten wird. Es ist daher kein Problem, in der Zeile „MAIL FROM:“ einen beliebigen Absender einzutragen.

- Überprüfen Sie die verlinkte Internet-Adresse genau. Oftmals wird lediglich ein Buchstabe vertauscht oder hinzugefügt, manchmal auch eine ähnlich klingende Subdomain hinzugefügt.

- Der angezeigte Link im Text, muss noch lange nicht das tatsächliche Linkziel sein. Deshalb sollten Sie sich jeden Link ganz genau anschauen, indem Sie mit der Maus darüberfahren (ohne zu klicken). In der Statusleiste (unten links) wird Ihnen dann der richtige Linkpfad angezeigt.

  Ein Beispiel:



- Es wird die Eingabe von sensiblen Kundendaten gefordert, die ausschließlich für den Kunden bestimmt sind, wie PINS, TANs oder Passwörter. Solche Daten werden nie auf einer Seite unspezifisch abgefragt, sondern nur in einem ganz bestimmten von der Bank festgelegten Kontext.
- PINs von EC-Karten, ebenso wie von Online-Konten dürfen aus Sicherheitsgründen lediglich dem Kunden und nie den Bankangestellten bekannt sein. Daher werden Sie nie von Bankangestellten oder Bank-Webseiten danach gefragt werden.
- Die Angreifer nutzen oftmals eine nicht korrekt verschlüsselte Verbindung – weder ein Schlosssymbol noch ein „https://“ sind in der Adresszeile des Webbrowsers erkennbar.

Schutzmaßnahmen vor Datenfischern

Wichtigster Grundsatz ist, sich ein "gesundes Misstrauen" bei allen Online-Aktivitäten zu bewahren. Wenn Sie dazu folgende Tipps beachten, sind Sie gut gegen „Datenfischer“ gewappnet:

- Folgen Sie keinen Aufforderungen in E-Mails, sozialen Netzwerken o. Ä., eine bestimmte Webseite aufgrund von "dringenden Umständen" (z. B. einer Sicherheitsabfrage) zu besuchen.
- Kontaktiert Sie (angeblich) ein Geschäftspartner per E-Mail, fragen Sie telefonisch nach. Suchen Sie die Servicenummer in Ihren Unterlagen oder im Telefonbuch und benutzen Sie nicht eine in der E-Mail angegebene Telefonnummer.
- Geben Sie niemals persönliche Daten am Telefon, per E-Mail, SMS etc. bekannt.
- Folgen Sie keinem Link zu Ihrer Bank, sondern geben Sie die Adresse selbstständig im Adressfeld ein (auch wenn selbst dies keine hundertprozentige Garantie ist, unbemerkt umgeleitet zu werden). Achten Sie darauf, sich nicht zu vertippen.

- Werden Sie während des Online-Bankings aufgefordert, mehrere TANs anzugeben, brechen Sie den Vorgang ab und fragen Sie bei Ihrer Bank telefonisch nach.
- Melden Sie sich nach jedem Online-Banking-Besuch ab ("Logout").
- Sie sollten Ihre Kontoauszüge regelmäßig prüfen. Wenn Sie auffällige Transaktionen sehen, die Sie nicht erkennen, wenden Sie sich umgehend an Ihre Bank. Die meisten Banken bieten Schutz vor Online-Betrug, aber das geht nur, wenn dieser auch gemeldet wird. Vereinbaren Sie gegebenenfalls mit der Bank ein Tageslimit für Überweisungen.
- Sichern Sie Ihr Computersystem ausreichend. Installieren Sie insbesondere ein wirksames Internet-Security-Programm und achten Sie darauf, dass alle installierten Programme auf dem neuesten Sicherheitsstand sind. Beachten Sie die Sicherheitstipps unter Phishing mit Schadsoftware ↓, um sich keine Viren, Trojaner oder Spyware einzufangen.
- Nutzen Sie Phishing-Filter in E-Mail-Programmen und Browser-Erweiterungen, die Sie vor verdächtigen Webseiten schützen.
- Das Bundesamt für Sicherheit in der Informationstechnik (BSI) und die Verbraucherzentrale veröffentlichen regelmäßig Informationen über aktuelle Phishing-Kampagnen. Nutzen Sie diese Informationsquellen.
- Gehen Sie nicht zu freizügig mit Ihren persönlichen Daten um. Lesen Sie auch: Woher haben Spammer meine persönlichen Daten? ↓.

Woher haben Spammer meine persönlichen Daten?

Beim Erhalt so mancher Phishing-Mail werden Sie sich wahrscheinlich fragen, woher der Absender Ihre persönlichen Daten wie E-Mail-Adresse, Name, Anschrift oder Telefonnummer hat. Die Details stammen aus zahlreichen Quellen: Von Adresshändlern, von Hackern oder von ganz normalen Internetseiten, die von Spammern automatisch nach Adressen abgesucht werden. Gelangen die Daten in den Besitz von Spammern, so werden Sie bald mit Werbemails zugemüllt, und nach kurzer Zeit sind weniger als 5% der eingehenden Nachrichten für Sie wirklich von Interesse.

Persönliche Daten im Internet schützen

Sparsamkeit und Vermeidung bei der Angabe von Daten im Internet sind der beste Schutz:

- Schützen Sie sich und Ihre Privatsphäre, indem Sie nicht sorglos und unbedacht persönliche Informationen ins Internet stellen.
- Lesen Sie Nutzungs- und Datenschutzbestimmungen. Teilweise räumen diese Bestimmungen dem Anbieter weite Rechte ein und enthalten eine Einwilligungserklärung für die Nutzung und Weitergabe Ihrer Daten.
- Überlegen Sie vor einer Anmeldung, ob Ihnen die Mitgliedschaft irgendeinen Nutzen bringt.
- Verwende Sie bei der Nutzung von kostenlosen Webdiensten ein Pseudonym.
- Richten Sie eine extra ("Schmutz-") E-Mail-Adresse ein, die Sie angeben, wenn Sie einen Online-Dienst in Anspruch nehmen (z. B. Anmeldung zu einem Newsletter). Benutzen Sie dafür einen Fantasienamen, der nicht auf Ihre Identität schließen lässt.
- Wenn Sie ein Bestellformular ausfüllen, geben Sie nur die Daten bekannt, die der Anbieter für die Leistungserbringung unbedingt benötigt (Namen, Lieferadresse). Weitergehende Informationen zu Hobbys, Einkommen, Kaufverhalten u. Ä. dienen allein der Erstellung von Kundenprofilen.

- Kontrollieren Sie regelmäßig Ihre Web-Identität, indem Sie Ihren Namen in einer allgemeinen Suchmaschine oder einer speziellen Personensuchmaschine eingeben.
- Benachrichtigen Sie den Webseitenbetreiber, wenn Sie Einträge finden, mit denen Sie nicht einverstanden sind.
- Wenn Sie eine private Internetseite betreiben, auf der Ihrer E-Mail-Adresse in lesbarer Form hinterlegt ist, verschleiern Sie die E-Mail-Adresse, indem Sie die Sonderzeichen ersetzen. Beispiel: „Schreiben Sie uns eine E-Mail an kontakt AT meinedomain PUNKT de“.
- Internetseiten wie „Have I Been Pwned" informieren über große Datenlecks. Hinterlegt man dort seine Mailadresse, wird man automatisch benachrichtigt, wenn die Adresse gehackt wurde. Infos zu über zwei Milliarden gestohlene Zugangsdaten finden sich in der Datenbank des Anbieters. Eine Registrierung ist nicht nötig.

Phishing mit Schadsoftware

Immer öfter versehen Cyberkriminelle Mails mit schädlichen Dateien. Aktuell verbreitet sich zum Beispiel das Schadprogramm Emotet per Phishing-Mails. Infiziert das Schadprogramm einen Computer, versendet es sich selbst an alle gespeicherten Kontakte des infizierten Computers. Einmal voreilig geklickt und der Computer ist kompromittiert.

8 Sicherheitstipps

- Fragen Sie sich bei jedem Mail-Anhang, warum Sie diesen öffnen sollten! Im Zweifelsfall sollten Sie beim Versender nachfragen (per Telefon), was es mit diesem Anhang auf sich hat.
- Erstellen Sie regelmäßig Datensicherungen.
- Installieren Sie Sicherheitsupdates sofort. Dies gilt sowohl für das Betriebssystem als auch für sonstige Programme.
- Deaktivieren Sie Makros und OLE-Objekte in Microsoft Office.
- Wenn Sie mit Windows arbeiten, dann sind Sie als Nutzer mit einem Benutzernamen angemeldet. Zur Sicherheit sollten Sie ein sicheres Benutzerkennwort setzen (Lesen Sie auch: Sichere Passwörter erstellen - So geht's). Das Benutzerkennwort ist buchstäblich der Zugangsschlüssel zu Ihrem Konto. Das Kennwort des Administratorkontos ermöglicht den uneingeschränkten Zugang zu Ihrem gesamten Rechner. Aktuelle Schadprogramme versuchen administrative Konten per Brute-Force-Methode zu knacken. Ein schwaches Benutzerkennwort bietet kaum Schutz dagegen.
- Richten Sie ein „eingeschränktes Benutzerkonto“ ein, für die tägliche Verwendung des Windows-Computers.
- Lassen Sie Dateiendungen unter Windows standardmäßig anzeigen. Öffnen Sie dazu irgendeinen Ordner und klicken oben auf den Reiter „Ansicht“. Unter „Ein-/ausblenden“ setzen Sie einen Haken unter „Dateinamenerweiterungen“.
- Installieren Sie einen Virenscanner. Ein Virenscanner ist immer noch Pflicht. Virenscanner stellen sicher, dass ein Computer selbst dann nicht infiziert wird, wenn man eine Virenverseuchte Spam-Nachricht öffnet. Die Kombination aus Echtzeit-Virenscanner und heuristischer Verhaltensanalyse bieten heute einen recht wirksamen Schutz vor Malware. Wo früher Antiviren-Updates einmal im Quartal oder (kostenpflichtig) einmal im Monat üblich waren, sind stündliche Updates heute ganz normal. Eine schnelle Antwort ist wichtig – zu schnell verbreiten sich Viren, Würmer, Trojaner und Co. Kostenlose Virenscanner bieten inzwischen einen guten Virenschutz.

Weitere Virenschutz-Tipps haben wir hier für Sie zusammengestellt.

Schlusswort

Je mehr vor Phishing gewarnt wird, umso mehr Betrugsversuche können frühzeitig erkannt werden. Besonders Unternehmen raten wir zur Vorsicht: Das eigene Personal muss unbedingt aufgeklärt werden und entsprechende Verhaltensweisen beherzigen.

An wirkungsvollen Filtermaßnahmen kommt man als Unternehmen nicht vorbei. An der Spam-Quelle kann man sich kaum zur Wehr setzen, bleibt also nur noch eine Bekämpfung am Ziel, indem man den laufenden Datenfluss überwacht.

Vor allem kleine Unternehmen sind ein sehr attraktives Ziel für Hacker[2]. Der Grund ist der, dass so gut wie alle kleinen Unternehmen mit dem Internet verbunden sind. Sie verfügen jedoch sehr oft nicht über die Mittel oder das Wissen, um diese Technologie wirklich sicher zu nutzen. Ein weiterer Grund, warum Hacker häufig kleinere Unternehmen angreifen, ist, dass sie an einem größeren Fisch interessiert sind. Kleine Unternehmen haben möglicherweise Zugang zu großen, besser geschützten Unternehmen. Kleine Unternehmen können als Einfallstor dienen, um Zugriff auf die Netzwerke und Daten der großen Unternehmen zu erhalten.

Einzelnachweise

Letzte Änderung am 07.01.2023: *Wir haben unter dem Punkt "Schutzmaßnahmen vor Datenfischern" weitere Schutzmaßnahmen hinzugefügt.*

↑ Nach oben