Phishing

1. Begriff
2. Erscheinungsformen
3. Tipps und Verhaltenshinweise
4. Praktisches Beispiel
5. Gegenmaßnahmen

Schützen Sie sich vor der dreisten Tour der Daten-Klauer!

Online-Banking boomt. Mittlerweile nutzt fast jeder dritte Deutsche die Möglichkeit zum virtuellen Bankbesuch.

Die bequeme Art, Bankgeschäfte abzuwickeln, überzeugt viele Kunden. Rund um die Uhr – von Zuhause oder unterwegs. Die Vorteile liegen auf der Hand: Neben der Flexiblität ist es vor allem der Kostenaspekt. Oftmals sind Finanztransaktionen, die online erfolgen, nämlich preiswerter als bei herkömmlicher Abwicklung am Bankschalter.

Vor dem Hintergrund einer stetig steigenden Service-Nachfrage treffen die Kreditinstitute umfangreiche Sicherungsmaßnahmen, um Ihre Internet-Kunden zu schützen. So finden beispielsweise die Transaktionen vertraulicher Daten nur über geschützte Verbindungen statt.

Diesen Schutz versuchen Kriminelle jedoch auszuhebeln. Ihre Masche: Sie versenden fingierte E-Mails, so genannte Phishing-Mails. Diese sollen den Empfänger dazu veranlassen, persönliche Daten wie Zugangsdaten, Passwörter, Transaktionsnummer usw. preiszugeben. Dabei werden die Methoden immer raffinierter. Kamen früher Mails im Umlauf, die - einfach gestrickt und schlecht formuliert - die Absicht des Absenders auf Anhieb verrieten, so ködern die Täter ihre Opfer heute mit professionell gestalteten Internet-Seiten, die selbst von Profis nur schwer als "Fake" zu identifzieren sind.

Begriff:

passwort + fishing = phishing

Bei dem Wort "Phishing" handelt es sich um ein Kunstwort, zusammengesetzt aus "password" und "fishing". Wörtlich übersetzt bedeutet es so viel wie "das Abfischen von Passwörtern".

Doch nicht nur Passwörter werden durch die Betrüger trickreich in Erfahrung gebracht. Auch an weiteren persönlichen Daten wie Name, Geburtstag, Anschrift oder aber Bankverbindungen bzw. Online-Banking-Zugangsdaten sind die Datenklauer interessiert.

Mit diesen persönlichen Daten können Betrüger Missbrauch betreiben ("Identity Theft" = Übernahme einer fremden Identität) und mit der vorgegaukelten Identität online im Namen des Geschädigten nahezu alle Geschäfte abwickeln (Geld

überweisen, Dispokredit ausschöpfen, Online-Einkäufe tätigen etc.). So entsteht Jahr für Jahr ein beträchtlicher wirtschaftlicher Schaden.

Erscheinungsformen:

Die Tricks der Abzocker

Das so genannte „Phishing“ ist eine neue Spielart der Computerkriminalität, die in jüngster Zeit besonders häufig im Bereich Online-Banking in Erscheinung getreten ist.

Der Trick: In betrügerischer Absicht werden Bankkunden mit täuschend echt aufgemachten E-Mails dazu veranlasst, über einen Link vermeintliche Internet-Seiten von Banken aufzurufen. Dort sollen dann persönliche Daten wie Zugangsdaten, Passwörter oder ähnliches eingeben werden – angeblich aus Sicherheitsgründen, zur Bestätigung oder um, wie es oft heißt, Datenabgleiche auszführen. Tatsächlich landen die Kunden aber keinesfalls auf echten Bank-, sondern vielmehr auf gefälschten Internet-Seiten. Manchmal wird – als Variante dieser betrügerischen Tour – vor der eigentlichen Internet-Seite der Bank ein Pop-Up geöffnet, das zur Eingabe der Daten auffordert. Auch in diesen Fällen haben die Täter nur ein Ziel: Sensible Daten sollen abgefangen und für Betrügereien missbraucht werden.

Bislang nur wenig verbreitet ist das Phishing per Telefon: ein vorgeblicher Mitarbeiter eines eines Kreditinstituts oder eines CallCenters bittet die angerufene Person unter Vortäuschung von Sachverhalten um die Preisgabe vertraulicher Daten.

Bei den Tätern handelt es sich sehr wahrscheinlich nicht um Hacker im klassischen Sinn, die aus sportlichem beziehungsweise technischem Ehrgeiz heraus handeln. Vielmehr verbirgt sich hinter Phishing-Betrug die organisierte Kriminalität.

Tipps und Verhaltenshinweise:

Vertrauen ist gut, Kontrolle ist besser

Bewahren Sie sich gegenüber elektronischer Post ein gesundes Misstrauen – auch dann, wenn die Botschaften mit bekannten Logos und in vertrauter Gestaltung aufwarten. Darüber hinaus sollten Sie folgendes beachten:

- Vergewissern Sie sich, mit wem Sie es zu tun haben. Überprüfen Sie die Adressleiste in Ihrem Browser. Bei geringsten Abweichungen sollten Sie stutzig werden. Tragen Sie ständig benötigte Internet-Adressen in die Favoritenliste Ihres Browsers ein und folgen Sie nicht den in E-Mails angegeben Links.
- Klicken Sie nicht auf den angegeben Link in der übersandten E-Mail. Versuchen Sie stattdessen, die in der eMail angegebenen Seiten tatsächlich auch über die Startseite Ihrer Bank zu erreichen (ohne diese in die Adresszeile einzutippen).
- Kreditinstitute fordern grundsätzlich keine vertraulichen Daten per E-Mail oder per Telefon von Ihnen an. Wenn Sie sich unsicher sind, halten Sie Rücksprache mit Ihrer Bank.

- Übermitteln Sie auch keine persönlichen oder vertraulichen Daten (bspw. Passwörter oder Transaktionsnummern) per E-Mail.
- Folgen Sie Aufforderungen in E-Mails, Programme herunter zu laden, nur dann, wenn Sie die entsprechende Datei auch auf der Internet-Seite des Unternehmens finden (Starten Sie keinen Download über den direkten Link). Öffnen Sie insbesondere keine angehängten Dateien. Informationen zu Anti-Virenprogrammen und Firewalls finden Sie hier (LINK innerhalb unseres Angebots).
- Geben Sie persönliche Daten nur bei gewohntem Ablauf innerhalb der Online-Banking-Anwendung Ihres Kreditinstituts an. Sollte Ihnen etwas merkwürdig vorkommen, beenden Sie die Verbindung und versuchen Sie es erneut. Veränderungen sollten Sie misstrauisch machen.
- Beenden Sie die Online-Sitzung bei Ihrer Bank, indem Sie sich abmelden. Schließen Sie nicht lediglich das Browserfenster und wechseln Sie vor Ihrer Abmeldung nicht auf eine andere Internet-Seite.
- Kontrollieren Sie regelmäßig Ihren Kontostand sowie Ihre Kontobewegungen. So können Sie schnell reagieren, falls ungewollte Aktionen stattgefunden haben.
- PIN und TANs sollten Sie nur dann eingeben, wenn eine gesicherte Verbindung mit Ihrem Browser hergestellt ist. Diese erkennen Sie an folgenden Merkmalen:

Die Adresszeile beginnt mit https://

Im Browserfenster erscheint ein kleines Icon, z. B. in Form eines Vorhängeschlosses, das den jeweiligen Sicherheitsstatus symbolisiert („geschlossen“ bzw. „geöffnet“).

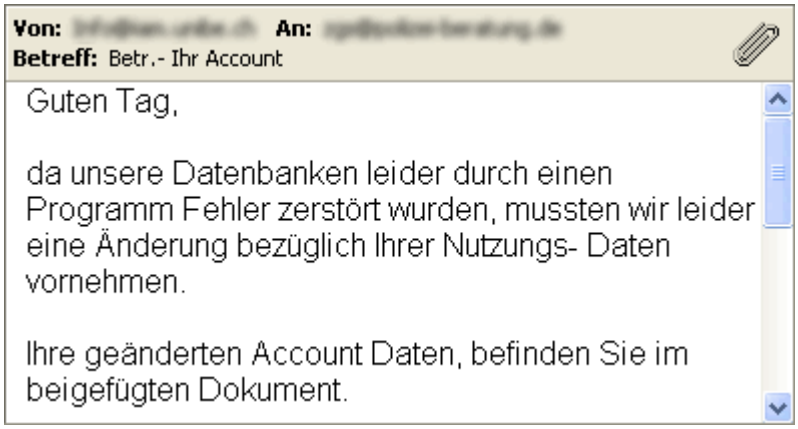
- Falls Sie externe Zugangssoftware nutzen, so stellen Sie sicher, dass es sich dabei um die offzielle Version Ihrer Bank handelt.
- Nutzen Sie Funktastaturen nur dann für das Online-Banking, wenn diese über eine eingebaute Verschlüsselung verfügen. Dies gilt auch für die Nutzung von Wireless-LAN (WLAN).
- Benutzen Sie als Passwort eine Kombination aus Zahlen und Buchstaben, am besten noch mit Groß- und Kleinschreibung. Bestehende Begriffe können mit entsprechenden Programmen erraten werden. Ändern Sie Ihre Passwörter regelmäßig.
- Benutzen Sie Passwörter nicht mehrmals für unterschiedliche Zugänge. Insbesondere unseriöse Anbieter, bei denen eine Registrierung notwendig ist, könnten so an vertrauliche Daten gelangen.
- Vernichten Sie nicht mehr benötigte Dokumente, beispielsweise die Zugangsdaten Ihrer Bank oder bewahren Sie diese an einem sicheren, nicht zugänglichen Ort auf (Safe oder ähnliches).
- Ein hohes Maß an Sicherheit bieten alle Homebanking-Programme, die eine Offline-Eingabe ermöglichen.
- Noch besser: Sie entscheiden sich für HBCI-Banking mit Chipkarte und Kartenlesegerät.
- Speichern Sie vertrauliche Daten nicht ungeschützt auf der Festplatte Ihres Computers. Sollten Sie ein Homebanking-Programm benutzen, werden die Kontodaten zumeist verschlüsselt abgelegt. Informieren Sie sich hier bei dem jeweiligen Hersteller der Software.

- Halten Sie Ihren Rechner auf dem neuesten Stand. Nutzen Sie die Update-Funktion des Herstellers Ihres Betriebssystems. Microsoft bietet die Möglichkeit, den Rechner auf aktuelle Schwächen zu prüfen und entsprechend zu aktualisieren.
- Passen Sie die Sicherheitseinstellungen in Ihrem Browser Ihren Bedürfnissen an. Bedenken Sie allerdings, dass sich strikte Einstellungen auf Ihre „Bewegungsfreiheit“ im Netz auswirken können. Verhindern Sie beispielsweise das Anlegen von Cookies, können Sie unter Umständen Bestellvorgänge bei einem Online-Shop nicht vornehmen.
- Verwenden Sie Virenscanner und zusätzliche Sicherheitssoftware wie z.B. Firewalls. Nähere Informationen erhalten Sie hier.
- Weitere Informationen zu den Sicherheitseinstellungen von Browsern finden Sie auf den Seiten von Heise Security.
- Außerdem sollten Sie Bankgeschäfte nur an Rechnern von Personen durchführen, denen Sie vertrauen. Es gibt Programme oder technische Einrichtungen, die Ihre Eingaben mitloggen können, ohne dass Sie es merken. Verzichten Sie deshalb darauf, Ihre Bankgeschäfte beispielsweise in Internet-Cafes zu erledigen.

Praktische Beispiele:

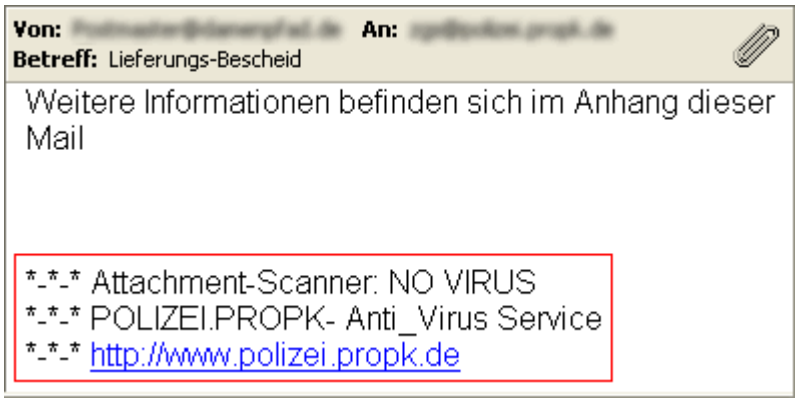
So könnten Sie auf's Glatteis geführt werden

Beispiele von Phishing-Mails:

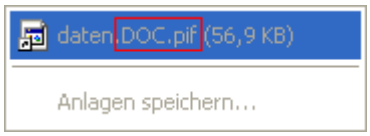


Dateianhang:

Normalerweise werden bedenkliche Anhäge gesperrt. Sie sollten diese auf keinen Fall öffnen.



Dateianhang:



Lassen Sie sich nicht durch scheinbare Virenchecks beeinflussen und achten Sie genau darauf, welche Dateianhänge sich tatsächlich in der Anlage befinden. Oftmals wird durch die Angabe einer bekannten Extension versucht, den Benutzer zum Aufrufen der scheinbar harmlosen Datei zu veranlassen.

Gegenmaßnahmen:

Was ist gegen Phishing-Attacken zu tun?

"Phishing" ist prinzipiell nichts anderes als der landläufig bekannte Haustür-Betrug, der das Vertrauen und die Arglosigkeit von Menschen ausnutzt.

Unser Tipp: Informieren Sie sich besser einmal mehr als einmal zu wenig über den Absender der E-Mail. Sind Ihre persönlichen Daten erst einmal in der Hand der Täter, kann Ihnen hoher finanzieller Schaden entstehen.

Haben Sie den Verdacht, Opfer einer Phishing-Attacke geworden zu sein, heißt es schnell zu handeln.

- Sperren Sie sofort den Onlinezugang für das betroffene Konto bei Ihrem Kreditinstitut.
- Prüfen Sie, ob auf dem Konto Verfügungen vorgenommen wurden, die nicht von Ihnen stammen.
- Sichern Sie betrügerische Mails, die Sie erhalten haben
- Erstatten Sie im Schadensfall Anzeige bei der Polizei

Ärger haben auch die Unternehmen, in deren Namen die Betrüger auftreten. Denn sie erleiden oft einen Image-Schaden. Prominentes Beispiel hierfür ist eBay. In der

zur leichteren Bedienung des Portals verfügbaren Toolbar, einer Menüleiste unterhalb der Browser-Adressleiste, ist seit Februar 2004 eine spezielle Sicherheitsfunktion integriert: Wenn man sich tatsächlich bei eBay befindet, leuchtet der Button "Sicherheits-Check" grün,. Andere Firmen arbeiten an ähnlichen Lösungen, um ihre Kunden zu schützen.

Auch die Banken greifen zu Gegenmaßnahmen. So setzen sie auf virtuelle Abfangnetze, die Phishing-Mails schnell aufspürt. Damit ist es ermöglich, betrügerische Webseiten frühzeitig zu sperren, bevor viele irregeführte Bankkunden Gelegenheit hatten, durch sie hinters Licht geführt zu werden.

In den USA haben sich Firmen bereits zur Anti-Phishing Working Group zusammengeschlossen. Auf ihrer Internetseite (www.antiphishing.org) kann man Phishing-Mails melden und nachlesen, welche Phishing-Botschaften schon aufgetreten sind.