

Was Sie schon immer über Phishing wissen wollten und sollten!

Sicherheitshinweise und Informationen

Was ist Phishing?

Phishing setzt sich aus dem englischen Begriff für Passwort-Fischen zusammen. Es handelt sich um eine besondere Form von unverlangt zugesandter e-Mails (sog. Spam), mit denen versucht wird, von Ihnen geheime Zugangsdaten abzufragen, wie hier z.B. die zum Konto. Wie beim Fischen hoffen die Täter auch, dass ihnen dabei einige arglose Verbraucher ins Netz gehen. Phishing kann auch andere Zugangsdaten betreffen, z.B. die zum Benutzerkonto bei eBay oder anderen Diensten im Internet.

Wie funktioniert Phishing?

Ein falscher Link und eine vertrauenswürdig klingende Lüge sind in der Regel die Grundlage des Phishing – dem Griff nach Ihrem Kontozugang und Ihrem Geld!

Im wesentlichen sind zwei Hauptmerkmale festzustellen.

Mit der Mail wird Ihnen ein Link zugesendet, mit dem Sie angeblich auf die Seite Ihrer Bank gelangen, um dort mit Hilfe Ihrer Zugangsdaten zu Ihrem Konto zu gelangen. Dieser Link ist aber falsch und führt zu einer Seite, die nicht der Bank, sondern Betrügern gehört.

Wichtig: Es ist leider ohne weiteres möglich, die Adressangabe so zu verfremden, dass die Tatsache der Fälschung der echten (Bank)Adresse kaum erkannt werden kann. Wenn Ihr Browser zum Beispiel zu Beginn der Internetadresse in der Adresszeile die Adresse Ihrer Bank zeigt, ist dies allein leider KEIN verlässliches Zeichen, dass Sie sich auch auf deren Internetseite befinden. Besonders gefährlich sind Links, die im Browserfenster lange kryptische Anhänge enthalten, wie man dies aber gewohnt ist, wenn man sich bei der Bank eingewählt hat. In diesen Anhängen ist zum Teil extrem raffiniert die Adresse des betrügerischen Servers versteckt. Selbst fortgeschrittene Nutzer können sie leicht übersehen. Die neueren Phishing-Mails täuschen regelmäßig auf diese Weise über die in Wahrheit angesurft Internetadresse. Die falschen Internetseiten sehen aber oft den echten Internetseiten Ihrer Bank zum Verwechseln ähnlich.

Die Betrüger täuschen Ihnen nun ein Grund vor, warum Sie Ihre „Bankseite“ ansurfen und Ihre persönlichen Zugangsdaten eingeben sollen. Das ist eigentlich eine alte Masche von Hackern. Es kann sich auf die „platte“ Aufforderung zur Eingabe von Kontonummer und der PIN und einer TAN beschränken. Es kann aber auch eine Aufforderung sein, dass Sie aus technischen oder Sicherheitsgründen unbedingt Ihr Konto durch Eingabe von PIN und TAN „freischalten“ müssten. Folgen Sie einer solchen Aufforderung, tun Sie das dann auch, aber eben für den Betrüger. Es wurde sogar schon in solchen gefälschten Mails mit einer Information - ähnlich dieser – vor dem Phishing gewarnt, nur um Ihnen einen falschen Link zur angeblichen Kontrolle Ihres Kontos unterzujubeln. Wie Sie sehen, sind der kriminellen Kreativität keine Grenzen gesetzt.

Fazit:

- Trauen Sie mitgesandten Links ABSOLUT NIEMALS!
- Geben Sie die Internetadresse zu Ihrer Bank immer selbst ein bzw. legen Sie selbst einen Link in Ihrem Browser an.
- Vertrauen Sie auch keinen Linklisten oder Angaben auf dritten Internetseiten oder Funktionen, die Ihnen einen Link im Browser anlegen.
- Schauen Sie in Ihre Kontounterlagen. Misstrauen Sie aber auch im Zweifel Postzusendungen, die Sie jetzt erhalten und eine Ihnen nicht bereits bekannte Adresse enthalten. Prüfen Sie genau, ob diese Post wirklich von Ihrer Bank stammt.
- Ihre Bank wird von Ihnen NIEMALS die Angabe von PIN und TAN zu Kontrollzwecken verlangen. Nutzen Sie beide Angaben nur für die Kontobewegungen auf der von Ihnen angesurften Webseite. Seien Sie im übrigen misstrauisch.
- Wenn Ihre Bank Sie sonst nicht per e-Mail anspricht, ist die Wahrscheinlichkeit besonders hoch, dass die Mail nicht echt ist.

Hier aber ein wirklich [sicherer Zugang zu Ihrer Bankseite](#)

Wie gefährlich ist Phishing wirklich?

Die Gefahr geht über die Gefahr eines Virus deutlich hinaus, Sie könnten Ihre Geld verlieren.

Vorsicht im Vorfeld, aber auch besonnenes Verhalten im Fall der Fälle, können den Schaden vermeiden bzw. verhindern.

Wer Ihre PIN hat, kann in der Regel Ihr Konto einsehen. Wer auch eine TAN hat, kann eine Kontoverfügung vornehmen, sich zum Beispiel das Kontoguthaben überweisen lassen. Ihr Geld kann dabei durch verschiedene Transfers ins Nichts verschwinden. Daher sind diese Spams nicht weniger gefährlich als Viren, in der Wirkung sogar wesentlich schlimmer. Die Täter sammeln diese Daten unerkannt ein und buchen möglicherweise aus bzw. über das Ausland von Ihrem Konto ab. Die Bank kann u.U. nicht erkennen, dass diese Buchung nicht von Ihnen stammt.

Momentan sind viele dieser Mails recht stümperhaft. Schreibfehler, englische Sprache und andere Dinge machen hoffentlich schnell misstrauisch. Sie sollten sich aber nicht darauf verlassen, dass Sie diese immer so leicht ausmachen werden. Einige zukünftig zu erwartenden Attacken dieser Art könnten sehr glaubwürdig wirken.

Zur Zeit hält sich der Schaden in Deutschland noch in Grenzen. Das hängt auch mit den aktuellen Warnungen über die Gefahr, dem richtigen Verhalten der betroffenen Verbraucher und der Banken zusammen. Es ist aber nicht sicher, ob dies auch so bleiben wird., In den USA ist es bereits zu beträchtlichen Schäden gekommen. Daher ist es wichtig, die Gefahr zu verstehen und vorsichtig zu bleiben.

Sind nur bestimmte Banken betroffen, wie die in den Medien jetzt viel zitierte Postbank, Deutsche Bank und Citibank?

Nein, die Täter könnten sich jede Bank, die mit dem PIN/TAN-System arbeitet, aussuchen. Denken Sie auch daran, dass Ihre Bank bei dieser Verfahrensweise zunächst nichts tun kann, diesen speziellen Angriff zu unterbinden. Erst wenn sie Kenntnis von einer gefälschten Webseite bekommt, kann sie gegen den Betrüger einschreiten und die Internetadresse, über die dieser versucht, an Kontodaten zu gelangen, abschalten lassen. Wenn Sie also die Bank, zu der Sie eine derartige

Spam zugesendet bekommen, kennen, sollten Sie diese umgehend mit einer eigenen Mail auf den Phishing-Versuch hinweisen.

Wirkungslos werden diese speziellen Attacken nur, wenn eine Online-Bank ein anderes als das PIN/TAN Verfahren anbietet und sichere Verschlüsselungssysteme einsetzt, die man nicht durch einfache Abfragen wie beim Phishing unterlaufen kann.

Kann ich den Links in einer Mail, die von meiner Bank zu kommen scheint, trauen?

Die Frage ist, ob Sie Sie mit Sicherheit feststellen können, ob eine bestimmte Mail von Ihrer Bank kommt. Wir wissen, dass einige Banken in der Vergangenheit den Zugang zu ihrer Webseite als Service-Link in einer Mail beigefügt haben. Nicht selten machen das auch Anbieter anderer Onlinedienste. Solange aber sichere Identifikations- und Authentifikationsverfahren wie zum Beispiel die elektronische Signatur nicht flächendeckend zum Einsatz kommen und nicht jeder weiß, wie er damit die Echtheit einer Mail überprüfen kann, kann jede Absenderadresse einer e-Mail gefälscht sein und Ihnen auf diesem Wege ein geschickt gefälschter Link zugehen. Falls Sie auch schon mal eine Spam-Mail erhalten haben, deren Absender angeblich sogar Sie selber waren, wissen Sie, dass Sie der Herkunftsangabe einer e-Mail nicht ohne weiteres vertrauen können.

Natürlich werden die Links, die Ihnen wirklich Ihre Bank schickt, in Ordnung sein. Da aber nicht ohne weiteres auszuschließen ist, dass eine unsignierte Mail auch falsch oder verfälscht sein kann, sollten sie die Links sicherheitshalber nicht nutzen, um im Anschluss auf der Seite Ihre Bankzugangsdaten einzusetzen.

Ist Online-Banking sicher?

Absolut sicher? Nein. Online-Banking ist ohne Frage für viele Verbraucher praktisch und flexibel und muss auch nicht per se ein Sicherheitsrisiko darstellen, aber es muss jedem klar sein, dass es eine absolute Sicherheit nie geben wird.

- Wenn Sie die Möglichkeiten des Online-Banking nicht missen möchten, besteht auf Grund der gegenwärtigen Vorkommnisse noch keine zwingende Veranlassung, das Online-Banking aufzugeben. Sie sollten nur stets die Sicherheitshinweise Ihrer Bank beachten und vorsichtig bleiben.
- Wenn Sie sehr unsicher beim Umgang mit dem Internet oder sehr sicherheitsorientiert sind und auf das Online-Banking verzichten können, sollten Sie auf die herkömmliche Weise Ihre Überweisungen tätigen. Prüfen Sie aber vorher, ob Ihnen hierdurch höhere Gebühren entstehen und schauen Sie sich gegebenenfalls nach einem Institut um, das Ihnen günstigere Konditionen bietet.

Für Banken ist das Online-Banking eine besonders kostengünstige Absatzform, im Vergleich z.B. zur Filiale. An der Sicherheit des Online-Banking darf aber nicht gespart werden. Es gibt bereits Systeme, wie etwa das HBCI (Home Banking Computer Interface, in Deutsch sinngemäß: Schnittstelle für das (sicher) Home-Banking per Computer). Dabei wird jeder Überweisungsauftrag so verschlüsselt, dass die versehentliche Preisgabe eines Passwortes auf einer Betrüger-Webseite diese nicht in die Lage versetzt, Buchungen in Ihrem Namen zu tätigen. Allerdings sind auch solche viel sichereren Systeme nicht absolut uneinnehmbar. Außerdem braucht man für derartige Systeme zumeist Zusatzhardware, wie zum Beispiel ein

Kartenlesegerät. Die Zusatzkosten hierfür sind wohl der mit ein Grund, warum sich derartige Systeme noch nicht im gewünschten Maße am Markt durchgesetzt haben.

Falsch wäre es auch, die Verantwortung nun nur auf die Verbraucher abzuwälzen. Es sind die Banken, die mit dem Online-Banking und der Art der Gestaltung

Auch die Banken sind in der Pflicht, für mehr Sicherheit zu sorgen.

Informieren Sie sich als Nutzer über die angebotenen Sicherheitsmaßnahmen und versuchen Sie diese und die Gefahren vom Prinzip her zu verstehen.

Das gibt Ihnen die Sicherheit, den Gefahren zu begegnen.

dieses Angebotes auch die Optionen für mögliche Betrüge-
reien setzen. Dennoch sollte Sie als Verbraucher im Eigen-
interesse Vorsicht walten lassen. Wird eine betrügerische
Überweisung tatsächlich ausgeführt, wird zwar stets zu
prüfen sein, ob der Schaden wirklich nur bei Ihnen bleibt.
Das kann aber durchaus der Fall sein. Deshalb muss man
diese Betrugsmethode wirklich sehr ernst nehmen.

In einzelnen Fällen haben Banken Dienste auf Server von
dritten Anbietern ausgelagert. Das kann es Ihnen zusätzlich
erschweren zu entscheiden, ob ein Betrugsversuch vorliegt
oder ob das in Ordnung ist. Trauen Sie solchen Seiten im
Zweifel nicht. Tätigen Sie Buchungen nur auf Seiten mit der

Internetadresse, die mit dem Namen und der Endung (z.B. name-der-bank.de)
endet, wie sie Ihnen Ihre Bank mitgeteilt hat. Banken sollten aufgrund der jüngsten
Erfahrungen auf die Verwendung von Servern Dritter in Zukunft dringend ver-
zichten.

Banküberweisungen sollten nur über besonders gesicherte Internetverbindungen
abgewickelt werden. Die Technologie dahinter heißt in der Regel SSL, was aus-
geschrieben etwa soviel wie geschützte Protokollebene heißt und im Wesentli-
chen auf einer sicheren Verschlüsselung der Kommunikation beruht. Sie erken-
nen eine so geschützte Verbindung an der Zeichenfolge <https://name-der-bank.de>
in der Adresse (also dem Zusatz **s** bei [http](http://name-der-bank.de)) bzw. an einem Symbol mit einem
Schloss o.ä. (variiert je nach dem Browserprogramm) in der Statusleiste. In der
Regel können Sie sich über dieses Symbol ein Zertifikat anzeigen lassen. Mit Hil-
fe dieses Zertifikats können Sie überprüfen, ob der Schlüssel, mit der die Bank die
Online-Daten auf der Webseite verschlüsselt, wirklich für Ihre Bank ausgestellt
wurde. Jedes Zertifikat ist wiederum mit einem Zertifikat abgesichert. Das Zertifi-
kat am Ende ist in der Regel mit dem Browser oder Betriebssystem mitgeliefert
und stammt von einer vertrauenswürdigen Zertifizierungsstelle. Durch diese mehr-
fache Absicherung soll sichergestellt werden, dass ein Betrüger sich nicht selbst
ein Zertifikat ausstellen kann. Der Name der Internetseite, für die das Zertifikat
ausgestellt ist, darf nicht nur ähnlich klingen, sondern muss absolut identisch mit
der Seite sein, die sie anwählen wollten. Denn ein Betrüger könnte sich zwar bei
einer anerkannten Zertifizierungsstelle ein Zertifikat auf einen ähnlich klingenden
Namen ausstellen lassen, aber eben nicht für die Originalseite der Bank, auf die
er nicht registriert sein kann.

Bei einer dermaßen abgesicherten Internetverbindung werden alle übermittelten
Daten so verschlüsselt, dass nur der richtige Empfänger sie entschlüsseln und
nutzen kann. Da die Daten im Internet über eine unplanbare Vielzahl von Rech-
nern weitergegeben wird, ist so gewährleistet, dass ein Betrüger nicht über seinen
eigenen Rechner die Daten heraussucht, abfängt und für seine Zwecke miss-
braucht.

Was tue ich, wenn ich versehentlich doch auf einer Betrügerseite meine Daten eingegeben habe?

- **Setzen Sie sich möglichst sofort mit Ihrer Bank in Verbindung! Ändern Sie sofort Ihre PIN!** Probieren Sie das mit der übermittelten TAN, sie wäre dann auch sofort verbraucht und wertlos. Achtung, hat der Täter mehr als eine TAN bekommen, nutzt ein weiterer Sperrtrick, die bewusste dreimalige Falscheingabe, nicht. Der Täter könnte den Zugang mit einer TAN wieder freischalten. Kommen die Täter bei einer PIN-Änderung zu spät, bleiben sie ausgesperrt. Gehen Sie aber davon aus, dass die Täter schnell handeln werden. In diesem besonderen Fall dürfen Sie der Bank – die Sie aber selber ansprechen bzw. anrufen sollten – die TAN nennen, die Sie auf der unsicheren Webseite eingesetzt haben. Nennen Sie aber auch dabei niemals Ihre PIN! Mit dieser TAN ist es der Bank möglich, die Überweisung, die diese Daten nutzt, vielleicht noch rechtzeitig abzufangen und nicht auszuführen. So konnten bisher Schäden abgewendet werden.
- **Stellen Sie Ihrer Bank und der Polizei die Mail, die Sie zur Eingabe der Daten veranlasst hat, zur Verfügung!** Löschen Sie diese Mail nicht. Sie gibt Aufschluss, wo sich der schädliche Server, der die Daten einsammelt, befindet, erlaubt es, diesen sperren zu lassen und kann Hinweise auf die Täter geben.
- **Erstatten Sie Strafanzeige!**

Phishing und der Einsatz ergaunerter Zugangsdaten ist ein Computerbetrug nach § 263a Strafgesetzbuch, also ein Strafdelikt. Bereits die Vorbereitungen dazu sind eine Straftat, bei der bis zu drei Jahre Haft drohen. Wird jemand substantiell geschädigt oder geht der Täter im großen Stil gewerbsmäßig vor, drohen sogar bis zu zehn Jahren Haft.

Der Angriff aus dem Ausland bleibt – hinsichtlich der Verfolgungsmöglichkeiten - ein besonderes Problem. Aber: Die Strafnorm basiert auf einer Vereinbarung der EU. Computerbetrug ist also zumindest in der europäischen Union ein über die Grenzen hinweg verfolgbares Delikt. In der Regel können die Behörden demnach, mit ausländischen Ermittlungsbehörden zusammenarbeitend, die Täter über die Grenzen hinweg verfolgen. Indem Sie als Geschädigte/r Strafanzeige stellen, ermöglichen Sie der Polizei die Ergreifung der Täter und unter Umständen die Sicherstellung der erbeuteten Gelder.
- **Informieren Sie auch Ihre Verbraucherzentrale**, damit wir von solchen Vorfällen erfahren und unsere Warnhinweise aktualisieren können. Hier erhalten Sie auch Rat und Hilfe im Fall, dass Sie geschädigt wurden.
- Auch wenn die Mail oder Seite, auf die Sie hereingefallen sind, Ihnen auf den zweiten Blick dumm und laienhaft erscheint, zögern Sie nicht zu handeln. Betrüger nutzen Unsicherheit und Scham aus. Experten wissen, dass man auf sehr vieles hereinfliegen kann. **Lassen Sie den Tätern keine Chance, damit Erfolg zu haben!** Wer hier „hereingefallen“ ist, ist in erster Linie nicht selbst schuld, sondern Opfer einer perfiden Straftat geworden.

Das haben Sie jetzt hoffentlich nur aus Neugier getan, oder?

Auch wir sind keine sichere Instanz, wenn es um den Zugang zu Ihrer Bank geht. Auch jemand anderes könnte sich für uns ausgeben oder diesen Text in einer Attacke missbrauchen.

Wenn wir Sie jetzt überrascht haben, hat das etwas Gutes. Dieser Link war absolut ungefährlich. Ein anderer könnte es nicht sein. Es gab bereits Ansätze die informierten und dann einen falschen Link angaben. Bitte geben Sie acht und geben Sie die Adresse Ihrer Onlinebank immer selbst ein. Dadurch können Sie das Risiko bereits erheblich reduzieren.

[Zurück zur Information](#)

(Anmerkung dieser Teil mit Link nur für die Information als Online-Text.)