Phishing-Angriff aufs Konto

Angriff auf Ihr Konto. Wie Sie sich schützen können und was Sie tun sollten, wenn Sie hereingefallen sind. Zögern Sie nicht zu handeln. Lassen Sie den Tätern keine Chance, Erfolg zu haben!

DAS WICHTIGSTE IN KÜRZE

1. Mit Hilfe des sogenannten Phishings versuchen Betrüger an die Kontodaten von Verbrauchern zu gelangen.
2. Gefälschte Eingabemasken auf manipulierten Internetseiten sollen potenzielle Opfer dazu animieren, ihre Login-Daten preiszugeben.
3. Phishing-Mails werden immer professioneller und sind in vielen Fällen nur noch schwer als solche erkennbar.

Stand: 24.02.2017

Phishing ist ein Kunstwort, das sich aus „password“und „fishing“ zusammensetzt. Es handelt sich um eine besondere Form unverlangt zugesandter E-Mails – sogenannter Spam-Mails –, mit denen versucht wird, von Ihnen geheime Zugangsdaten abzufragen.

Beim Phishing geht es oft um Ihr Konto. Es kann aber auch andere Zugangsdaten betreffen, beispielsweise die Daten zu Ihrem Benutzerkonto bei Ebay, Paypal oder anderen Diensten im Internet. Wie beim Fischen hoffen die Täter, dass ihnen einige arglose Verbraucher ins Netz gehen.

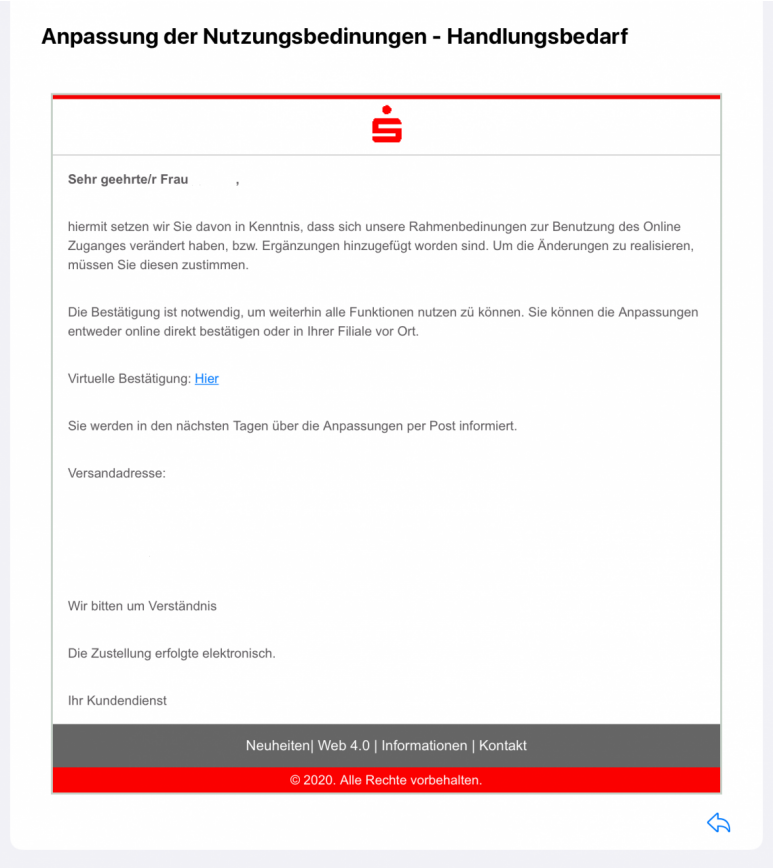
Wie funktioniert Phishing?

Per E-Mail erhalten Sie einen Link, mit dem Sie angeblich auf die Seite Ihrer Bank gelangen, um dort mit Hilfe Ihrer Zugangsdaten zu Ihrem Konto zu gelangen – um irgendetwas zu prüfen, nachzutragen oder zu korrigieren. Doch der Link ist falsch und führt zu einer Seite, die nicht der Bank, sondern Betrügern gehört.

Wichtig: Leider ist es ohne weiteres möglich, die Adressangabe so zu verfremden, dass die Tatsache der Fälschung der echten (Bank)Adresse kaum zu erkennen ist. Wenn Ihr Browser zum Beispiel zu Beginn der Internetadresse in der Adresszeile die Adresse Ihrer Bank anzeigt, ist dies allein 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 diese leicht übersehen. Die neueren Phishing-Mails täuschen regelmäßig auf diese Weise über die in Wahrheit angesurfte Internetadresse. Zudem sehen die falschen Internetseiten den echten Internetseiten Ihrer Bank oft zum Verwechseln ähnlich.

Die Betrüger täuschen Ihnen also einen 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 die Betrüger. Dass in diesen gefälschten Mails sogar oft vor dem Phishing gewarnt wird, zeigt, dass der kriminellen Kreativität keine Grenzen gesetzt sind.



Screenshot einer Phishing-Mail. Der Absender ist nicht die Sparkasse.

Wie vermeiden Sie Phishing?

- 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 Internetseite.
- Wenn Ihre Bank Sie sonst nicht per E-Mail anschreibt, ist die Wahrscheinlichkeit besonders hoch, dass die Nachricht nicht echt ist.

Wie gefährlich ist Phishing wirklich?

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 unter Umständen nicht erkennen, dass diese Buchung nicht von Ihnen stammt.

Momentan sind zahlreiche 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. Viele Nachrichten sind mittlerweile sehr glaubwürdig.

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.

Täter können 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, um 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, bezüglich 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 Online-Dienste. 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.

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 substanziell 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 Geschädigter Strafanzeige stellen, ermöglichen Sie der Polizei die Ergreifung der Täter und unter Umständen die Sicherstellung der erbeuteten Gelder.
- **Informieren Sie uns,** damit wir von solchen Vorfällen erfahren und unsere Warnhinweise aktualisieren können. Bei uns erhalten Sie auch Rat und Hilfe im Fall,

dass Sie geschädigt wurden.

UNSER RAT

Handeln Sie bei Phishing sofort – ändern Sie Ihre Zugangsdaten, informieren Sie Ihre Bank und erstatten Sie Strafanzeige!

Auch wenn die E-Mail oder die Internetseite, auf die Sie hereingefallen sind, dumm und laienhaft erscheint, zögern Sie nicht zu handeln. Betrüger nutzen Unsicherheit und Scham aus und kommen allzu oft damit durch. Lassen Sie den Tätern keine Chance, Erfolg zu haben! Wer „hereingefallen“ ist, ist nicht selbst schuld, sondern Opfer einer perfiden Straftat geworden.

https://www.vzhh.de/themen/finanzen/konto/phishing-angriff-aufs-konto