Präventionstipps

- Wenn Sie die Internetseite Ihrer Bank oder andere sensible Seiten aufrufen, geben Sie immer **manuell die Adresse in die Adresszeile** Ihres Browsers ein!
- Achten Sie darauf, dass die Verbindung zu Ihrer Bank in der **Adresszeile mit https:// beginnt** (sichere Verbindung)!
- Achten Sie darauf, dass bei einer zertifizierten sicheren Verbindung in der unteren **Browserleiste ein Schloss** angezeigt wird!
- Informieren Sie sich über die **verschiedenen Verfahren zum sicheren Durchführen von Online-Banking** (z. B. HBCI, MS-TAN usw.).

Was ist zu tun nach einem Phishing-Angriff ?

- Sperren Sie unverzüglich Ihr **Bankkonto** und Ihren Zugang zum Online-Banking. Am schnellsten geht das, indem Sie zum Beispiel die Anmeldemaske zum Online-Banking aufrufen und dreimal hintereinander die falsche PIN eingeben. Oder Sie rufen den **zentralen Sperr-Notruf 116 116** (aus dem Ausland +49 116 116) an und lassen Ihren Zugang telefonisch sperren!
- Wenden Sie sich danach an Ihre **Bank** und **melden** die Auffälligkeiten! Gegebenenfalls besteht die Möglichkeit, Kontobewegungen rückgängig zu machen.
- **Prüfen Sie** umgehend die **Kontoumsätze** anhand des Papierauszuges!
- Sollten Sie tatsächlich Opfer eines Phishing-Angriffs mittels eines Trojaners geworden sein, müssen Sie Ihren **PC fachgerecht von der Schadsoftware befreien** lassen!
- Erstatten Sie **Anzeige bei der Polizei** wegen Betrug gegen Unbekannt!

Grußwort

Das Internet ist aus unserem Alltag nicht mehr wegzudenken: wir buchen unseren Urlaub ebenso elektronisch wie wir einen Tisch in unserem Lieblingsrestaurant direkt online reservieren. Einen großen Stellenwert nimmt das Versenden und Empfangen von E-Mails ein. Es ist erstaunlich, wie viele Daten in einer atemberaubenden Geschwindigkeit um die Welt gehen.
Ausgerüstet mit einem qualitativ hochwertigen Virenprogramm fühlen wir uns auf der sicheren Seite - stets mit dem Gedanken im Hinterkopf, dass wir bei so viel Schutz gar kein Opfer von Internetbetrug sein können. Doch sollten wir uns nicht täuschen. Opfer von Internetbetrug kann jeder Einzelne von uns werden. Wir alle kennen solche E-Mails: Ein durchaus vertrauenswürdiger Absender fordert uns auf, eine bestimmte Webseite - etwa der eigenen Bank - im Internet zu besuchen und dort Zugangsdaten wie Benutzernamen und Passwort anzu- geben. Das Trügerische daran: Weder der Absender ist zuverlässig noch die Internetseite. Im Gegenteil: Bei diesem Vorgehen handelt es sich um kriminelle Handlungen - um das sogenannte Phishing. Die Seite ist gefälscht und die Täter interessieren sich für vertrauliche Daten wie für unsere Online-Banking- und Kreditkartendaten.
Wie können wir Abhilfe schaffen? Wie können wir dazu beitragen, dass es gar nicht erst zu einem Betrug kommt? Wie können wir uns schützen? Antworten auf diese Fragen finden Sie in dem vorliegenden Faltblatt zum Thema Phishing, die eine hilfreiche Handreichung ist.

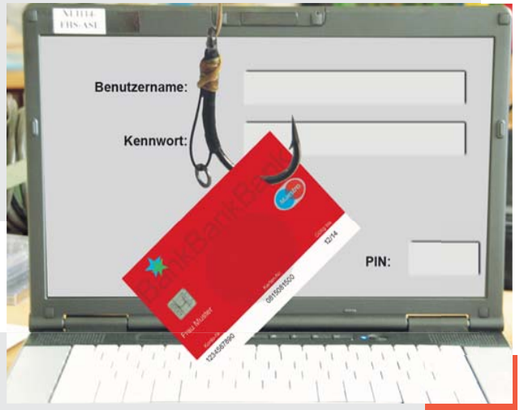
Seien wir gemeinsam vorsichtig im World Wide Web, damit wir Internet-Betrügern nicht ins Netz gehen.

Ihr

Holger Stahlknecht

Minister für Inneres und Sport
des Landes Sachsen-Anhalt

Phishing



Betrug im Internet

SACHSEN-ANHALT
Ministerium für Inneres und Sport

Präventionstipps

Schutz vor Phishing:

- Setzen Sie eine **Firewall und Virenschutzsoftware** ein und bringen Sie diese regelmäßig auf den aktuellen Stand! Installieren Sie die vom Hersteller des Betriebssystems bereitgestellten Sicherheitsupdates zeitnah oder nutzen Sie automatische Update-Dienste!
- **Öffnen Sie niemals ungeprüft Dateianhänge** von E-Mails! Wenn Sie unsicher sind, fragen Sie beim Absender sicherheitshalber nach!
- Oft verraten sich **virenbehaftete E-Mails** durch einen Betreff, der den Adressaten **neugierig machen soll** (z. B. Begriffe aus dem Erotikbereich oder zu aktuellen Promi-Skandalen), öffnen Sie keine E-Mails mit derartigen Anhängen!
- Seien Sie **misstrauisch**, wenn Sie E-Mails von angeblichen Bekannten ohne oder mit **fremdsprachigem Betreff** erhalten, diese sollten Sie sofort löschen!
- Seien Sie **besonders kritisch** bei ausführbaren Programm-Dateien mit den Endungen .exe, aber auch .bat, .com oder .vbs und insbesondere bei doppelten **Dateiendungen** wie .dod.exe!
- Stellen Sie die Sicherheitseinstellungen Ihres E-Mail-Programms so ein, dass **keine Handlung automatisch ausgeführt** werden kann!
- Kreditinstitute fordern grundsätzlich **keine vertraulichen Daten per E-Mail oder per Telefon** von Ihnen ab. Kontrollieren Sie regelmäßig Ihren Kontostand!
- Verwenden Sie für **jede Anwendung ein anderes Passwort**!
- **Phishing-E-Mails** kann man manchmal an **mangelhafter deutscher Sprache** (kyrillische Zeichen, „a“ statt „ä“ oder „ae“) oder namenloser Anrede (Sehr geehrte/r Kunde/in) erkennen.
- **Gefälschte E-Mails** enthalten oft **Drohungen oder** signalisieren einen dringenden **Handlungsbedarf** („Verifizieren Sie Ihre Daten innerhalb der nächsten zwei Tage.“).

Phishing

Phishing ist ein Kunstwort aus der Hackerszene und setzt sich aus den englischen Worten **P**assword **H**arvesting f**ishing** (Passwort ernten/fischen) zusammen.

Es ist eine Methode des Betrugs, bei der mit Hilfe gefälschter E-Mails, gefälschter Webseiten und anderer Techniken vertrauliche Daten von Internetnutzern erlangt werden.

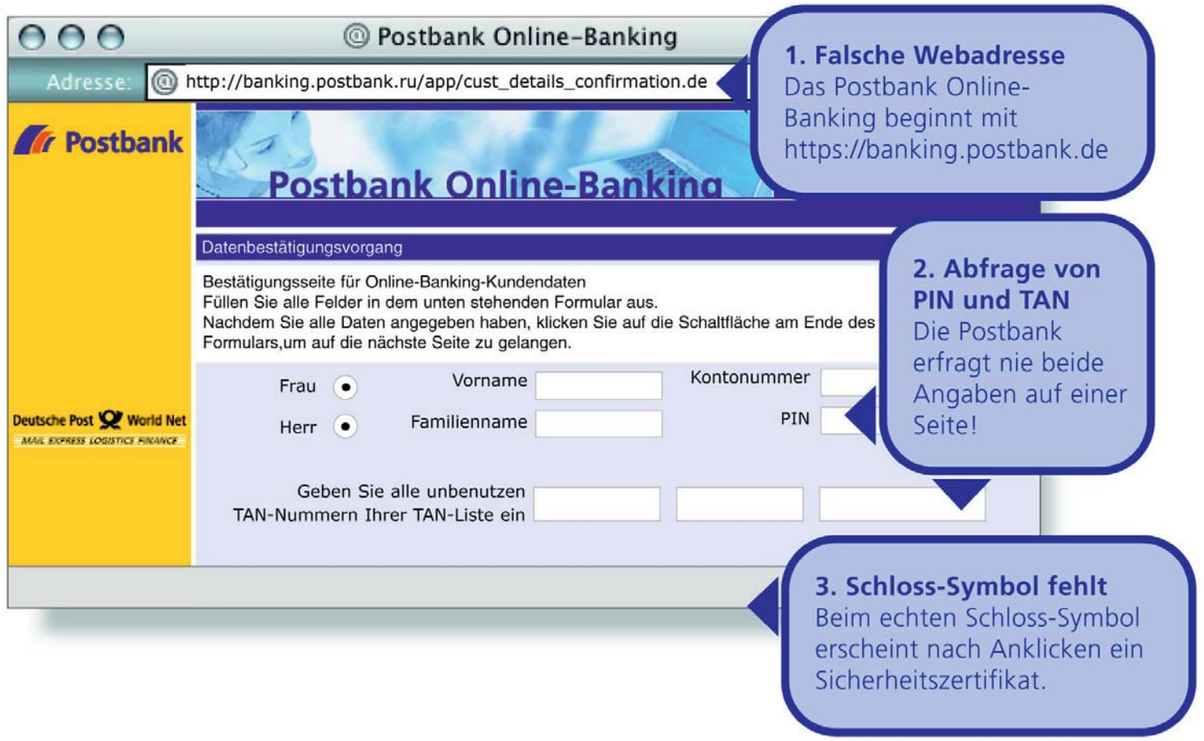
Dabei handelt es sich hauptsächlich um Zugangsdaten, Passwörter, PIN/TAN und sonstige persönliche Daten für das Online-Banking und den elektronischen Versandhandel. Die Täter nutzen dabei ein durch die Täuschung über die tatsächliche Identität erlangtes Vertrauensverhältnis aus. Das Ziel der Täter besteht darin, mit den erlangten Daten unter der Identität des Inhabers im Onlineverkehr Handlungen vorzunehmen.

Was passiert bei Phishing ?

- Die Täter versenden E-Mails, die dem Erscheinungsbild und dem Inhalt nach von dem vermeintlichen Geldinstitut des Opfers oder von vertrauenswürdigen Geschäftspartnern zu stammen scheinen.
- Die Opfer werden aufgefordert, ihre PIN/TAN einzugeben und gelangen dann über einen Link zu einer echt aussehenden, aber gefälschten Bankseite mit Banklogo. Dort erfolgt angeblich eine Überprüfung der Kontodaten.
- Haben die Täter vertrauliche Daten erhalten, sind sie in der Lage, mit der Identität des Dateninhabers im Internet zu agieren, z. B. auf das Konto des Dateninhabers zuzugreifen und Überweisungen zu tätigen.

Merkmale einer gefälschten Webseite

Gefälschte Postbank Webseite



Verschiedene Varianten des Phishing

- Phishing Mails können in großer Anzahl versendet werden, z. B. als Spam-Mails (meistens nicht bestellte Werbe-Mails, deren Absender oft nicht erkennbar ist).
- Sie können aber auch an einen sehr speziellen Personenkreis adressiert sein, z. B. in einer Firma, wodurch ein verstärktes Vertrauensverhältnis entsteht (Spear – Phishing).
- Phishing-Mails können auch als HTML-Mails (sind im Grunde Webseiten, die per Mail verschickt werden) gestaltet werden. Darin ist ein Formularfeld enthalten, in das vertrauliche Daten direkt eingegeben werden sollen, um so ohne eine Umleitung auf eine Webseite zum Absender zu gelangen.
- Täter schalten sich mit Hilfe von Malware (z. B. Trojaner, Würmer, Viren) in den Kommunikationsweg zwischen Bankkunde und Bank um Daten abzugreifen. Der Umweg, den Bankkunden über das Versenden einer E-Mail zur Preisgabe seiner Zugangsdaten zu verleiten, ist damit nicht mehr notwendig.

Nützliche Links mit Informationen zum Thema Phishing

www.polizei-beratung.de/presse
www.bsi-fuer-buerger.de
https://www.bsi.bund.de/ContentBSI/Publikationen/Lageberichte/bsi-lageberichte.html
https://www.a-i3.org
www.bankenverband.de/onlinebanking
www.infos-finanzen.de
www.kartensicherheit.de

Impressum

Herausgeber: Ministerium für Inneres und Sport des Landes Sachsen-Anhalt, Pressestelle
Halberstädter Straße 2/am „Platz des 17. Juni“
39112 Magdeburg
www.mi.sachsen-anhalt.de E-Mail: pressestelle@mi.sachsen-anhalt.de

Landeskriminalamt Sachsen-Anhalt
Lübecker Straße 53-63
39124 Magdeburg
www.polizei.sachsen-anhalt.de E-Mail: praevention.lka@polizei.sachsen-anhalt.de

Gestaltung/Herstellung: Medienzentrum der Polizei des Landes Sachsen-Anhalt
Fachhochschule Polizei Sachsen-Anhalt
Schmidtmannstraße 86
06449 Aschersleben

Fotos: Bundeskriminalamt und Landeskriminalämter