Sicherheit im Online-Banking

BASISWISSEN

Schutz vor Daten-Spionen

Online-Banking ist einfach und sicher. Dennoch: Damit Sie Ihr Geld vor dem Zugriff von Internet-Betrügern schützen, muss Ihr Computer frei sein von schädlichen Spionage-Programmen. Dieses Dokument erklärt Ihnen, worauf Sie achten und was Sie tun müssen.

Inhalt

So funktionieren Phishing-Mails

Der Begriff „Phishing" ist in aller Munde. Auch Sie haben vielleicht schon Phishing-Mails in Ihrem Posteingang gehabt, genauso wie unzählige andere Spam-Mails.

Spam-Mails sind unerwünschte E-Mails mit meist werblichem Charakter. Mails, die die Empfänger auffordern, geheime Kontodaten über das Internet preiszugeben, nennen Fachleute „Phishing-Mails". Der Begriff „Phishing" ist eine Kombination aus den englischen Wörtern „Password" und „fishing".

Phishing-Mails stammen von Betrügern

Die Betrüger fischen also online nach Passwörtern, um damit den Zugang zu fremden Konten zu erhalten. Die Absender verschicken diese Mails in der Regel massenhaft und weltweit von mehreren Computern aus, die sie zu ganzen Netzwerken (Bot-Netzen) zusammenfassen. Um diese Phishing-Mails unschädlich zu machen, gibt es eine wirksame Möglichkeit: Löschen Sie diese Mails sofort! Und bedenken Sie:

Ihre Bank bittet Sie weder per E-Mail noch telefonisch, Kontodaten wie PIN und TAN preiszugeben!

Wie Sie Phishing-Mails erkennen

Phishing-Mails gibt es in vielen Varianten. Eins haben sie aber gemeinsam: Sie nutzen Vorwände und gefälschte Absender-Adressen, Web-Seiten und Eingabe-Masken, die beispielsweise einer Banking-Anwendung täuschend ähnlich sehen. Hier einige Beispiele für Vorwände, die in Phishing-Mails oft auftauchen:

- Software oder Bankdaten sollen aktualisiert werden
- Phishing-Mails warnen selbst vor Phishing-Mails
- Sie erhalten eine Mahnung zum Beispiel für Ihre Telefon- oder GEZ-Rechnung
- Ihre Kreditkarte oder VR-BankCard ist abgelaufen
- Sie sollen Ihr Passwort erneuern
- Sie sollen Daten für Umfragen oder Gewinnspiele bestätigen

Ein typischer Beispielfall: Sie erhalten per E-Mail eine gefälschte Rechnung mit einer sehr hohen Forderung. Diese Mail enthält einen Link oder einen als PDF-Datei getarnten Anhang. Beim Ausführen installiert sich ein Spionage-Programm auf dem PC.

Viele Phishing-Seiten bestehen aus einer Eingabe-Maske, in die Sie sowohl Ihre Kontonummer als auch PIN und TAN eintippen sollen. Auf echten Banking-Seiten werden PIN und TAN immer auf nacheinander folgenden Seiten abgefragt.

Viele Phishing-Mails erkennen Sie daran, dass sie verhältnismäßig viele Rechtschreib- und Grammatikfehler enthalten. Seien Sie deshalb vorsichtig, wenn Sie in einer geschäftlichen E-Mail über schlechtes Deutsch stolpern.

Grundsätzlich können Sie erwarten, dass ein Unternehmen, bei dem Sie Kunde sind, Sie persönlich mit Ihrem Namen anredet. Nicht alle, aber die meisten Phishing-Mails beginnen mit unpersönlichen Anreden wie „Sehr geehrter Kunde" oder ähnlichem.

Deswegen: Löschen Sie alle E-Mails, deren Herkunft Sie nicht genau kennen.

Unseriöse Job-Angebote

Ebenfalls in Form von E-Mails tauchen immer wieder Job-Angebote auf, in denen seriös anmutende Unternehmen den Empfängern anbieten, als Finanz-Makler tätig zu werden. Auch wenn Sie angeblich lukrative Provisionen einstreichen können, stellen Sie Ihr Konto nie für fremde Zahlungen zur Verfügung!

Oft handelt es sich um Gelder, die aus den Erträgen von Phishing-Mails stammen. Unter Umständen riskieren Sie Freiheitsstrafen wegen Geldwäsche und Schadenersatz-Ansprüche der geschädigten Bankkunden. Informieren Sie Ihre Bank und die Polizei, wenn Sie eine solche Mail erhalten.

Der Stornierungs-Trick

Ein anderer Trick funktioniert nach folgendem Muster: Betrüger bestellen per E-Mail Gebrauchtwagen oder andere Waren, oder sie buchen eine Ferienwohnung. Mit dem Anbieter vereinbaren sie, den Preis vorab zu überweisen. Dazu benutzen Sie allerdings ein fremdes, mittels Phishing ausgespähtes Konto. Unter einem Vorwand stornieren die Täter dann den Kauf – ebenfalls per E-Mail. Die bereits überwiesene Geldsumme soll das Opfer ins Ausland transferieren. Dass ihm angeblich wegen der entstandenen Unannehmlichkeiten ein Teilbetrag zugesprochen wird, ist ein Trick, um ihn in Sicherheit zu wiegen. Das Geld landet beim Täter oder der Tätergruppe.

Seien Sie deshalb vorsichtig, wenn Gutschriften auf Ihrem Konto erscheinen, die kurze Zeit später zurückgefordert werden – insbesondere bei Auslandstransfers. Informieren Sie im Zweifelsfall Ihre Bank oder die Polizei.

So funktionieren Daten-Spione

Ein technisch einwandfreier Computer ist die Grundvoraussetzung dafür, dass Sie Ihre Überweisungen sicher online erledigen können. Wenn Ihr Computer nicht ausreichend geschützt ist, können schädliche Computer-Programme, zum Beispiel so genannte Trojaner, unbemerkt auf Ihre Festplatte gelangen und dort die unterschiedlichsten Schäden anrichten.

So können Trojaner auf Ihren Computer gelangen:

- Eingebettet in scheinbar harmlosen Downloads
- Über Datenträger wie Diskette oder CD-ROM
- Versteckt als Datei-Anhang in einer Phishing-Mail (zum Beispiel mit dem Namen "Rechnung.pdf.exe")
- Durch Surfen auf einer manipulierten Internet-Seite

Antiviren-Software und Firewall sind Pflicht

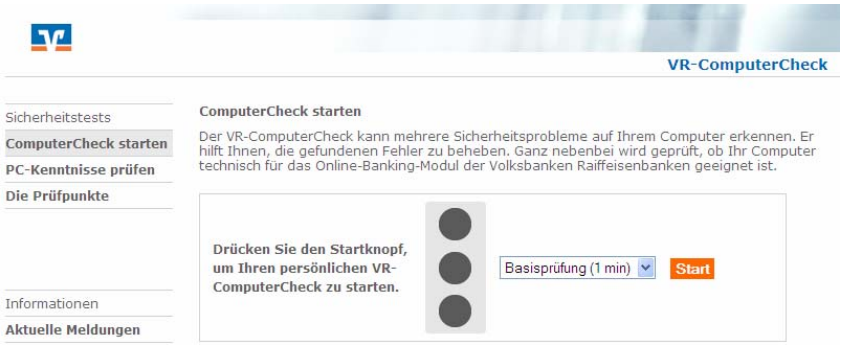
Einige Trojaner sind so programmiert, dass sie beispielsweise die PIN/TAN-Eingabe beim Online-Banking manipulieren. Andere leiten den Nutzer auf eine gefälschte Internet-Seite.

Unerlässlich ist es deshalb, dass auf Ihrem Computer ein Antiviren-Programm sowie eine Firewall installiert sind, die Sie regelmäßig aktualisieren. Diese Programme können Trojaner und andere Viren identifizieren und löschen. Auch Ihr Betriebssystem und Ihre Browser-Software sollten stets dem aktuellen Versionsstand entsprechen.

Wie Sie Trojaner erkennen

Da sich Trojaner in der Regel unbemerkt vom Nutzer auf dem Computer installieren, werden sie erst mit Hilfe eines Antiviren-Programms sichtbar, dass die schädliche Software löscht.

Im **VR-ComputerCheck** finden Sie eine Liste mit Links zu kostenlosen Downloads von Virenschutz-Programmen und Firewalls. Sie finden den VR-ComputerCheck im Internet-Auftritt Ihrer Bank unter Konto & Karten / Sicherheit.



Auf den folgenden Seiten finden Sie weitere ausführliche und verständliche Hinweise für die Sicherheit Ihres Computers und Ihres Online-Bankings. Lesen Sie die Hinweise aufmerksam.

Wenn Sie Fragen haben, wenden Sie sich an den Berater in Ihrer Filiale. Er gibt Ihnen gerne Auskunft.

Diese Hinweise sollten Sie beachten

PIN und TAN gehen nur Sie was an

- Speichern Sie vertrauliche Daten wie Ihre Persönliche Identifikations-Nummer (PIN), Transaktions-Nummern (TAN) oder andere Passwörter nicht auf Ihrer Festplatte.
- Ändern Sie regelmäßig Ihre PIN.
- Geben Sie nie per E-Mail persönliche Daten wie Bankkonten, PIN und TAN, Kreditkarten-Daten oder Passwörter preis.
- Lassen Sie den Online-Zugang sofort sperren, falls Sie Ihre TAN-Liste verlieren.
- Vergewissern Sie sich, ob die auf der Internet-Seite geforderten Eingaben in Zusammenhang mit der von Ihnen gewünschten Aktion sinnvoll sind.
- Aktivieren Sie Ihre Spam-Filter. Alle großen Provider haben typische Phishing-Absender in ihre Filter aufgenommen.

Sicherheit der Internet-Verbindung

- Benutzen Sie für das Online-Banking keine Rechner in Internet-Cafés; hier sind Manipulationen Tür und Tor geöffnet.
- Halten Sie Ihr Betriebssystem sowie Browser-, Antiviren- und Firewall-Software aktuell. Im **VR-ComputerCheck** (im Internet-Auftritt Ihrer Bank unter Konto & Karten / Sicherheit) finden Sie eine Liste mit Links zu kostenlosen Downloads von Virenschutz-Programmen und Firewalls.
- Wenn Sie über ein Funknetz (WLAN) ins Internet gehen: Achten Sie darauf, dass die Daten-Übertragung ausreichend verschlüsselt ist.
- Auch Eingaben in Funktastaturen sind nicht abhörsicher. Verzichten Sie deshalb in Büros und Mehrfamilienhäusern möglichst auf solche Tastaturen.
- Installieren Sie nur Programme auf Ihren PC, deren Herkunft Sie als vertrauenswürdig und seriös einschätzen.
- Löschen Sie alle E-Mails, deren Herkunft Sie nicht kennen.
- Klicken Sie keine Links oder Datei-Anhänge in E-Mails an, deren Herkunft Sie nicht kennen.
- Schließen Sie stets alle anderen Browser-Fenster, bevor Sie die Online-Banking-Anwendung starten.
- Deaktivieren Sie die Zusatzfunktion „ActiveX" in Ihrem Browser (beim Internet Explorer unter Extras/Internetoptionen/Sicherheit => „Stufe anpassen").
- Surfen Sie nicht mit Administrator-Rechten im Internet. Denn dann haben auch Angreifer aus dem Internet Administrator-Rechte auf Ihrem Computer. Legen Sie deshalb in der System-Steuerung von Windows unter „Benutzerkonten" einen neuen Benutzer mit dem Kontotyp „Eingeschränkt" an. Mit diesem surfen Sie im Internet (gilt ab Windows 2000).
- Geben Sie persönliche Daten grundsätzlich nur über SSL-verschlüsselte Internet-Seiten weiter und auch nur an Unternehmen, denen Sie vertrauen. Online-Banking ist eine solche SSL-gesicherte Anwendung. Sie erkennen eine

verschlüsselte Verbindung daran, dass die URL mit "https://" beginnt.
- Prüfen Sie, ob die in der Adresszeile des Browsers angegebene Internet-Adresse mit der zertifizierten Adresse Ihrer Bank übereinstimmt. Die zertifizierte Adresse erhalten Sie per Doppelklick auf das Schloss-Symbol unten rechts im Browser (beim Internet-Explorer bis Version 6).
- Klicken Sie nicht auf Links in E-Mails, Internet-Seiten oder sonstigen Nachrichten, um auf Ihre Bankseite zu kommen!
- Geben Sie die Adresse Ihrer Bank von Hand in die Adresszeile Ihres Browsers.
- Überprüfen Sie stets die Adresszeile Ihrer Online-Banking-Anwendung. Selbst durch kleine Änderungen könnten die Daten, die Sie eingeben, auf eine gefälschte Internet-Seite gelangen.
- Schließen Sie die Banking-Anwendung immer über die Logout- oder Abmelde-Funktion.
- Löschen Sie den Zwischenspeicher (Cache) nach jedem Besuch der Banking-Anwendung.
- Wenn Sie den Verdacht haben, dass die vorliegende Seite manipuliert ist, verlassen Sie diese und befolgen Sie keinesfalls die dort angegebenen Anweisungen. Informieren Sie Ihren Bankberater über die auffällige Seite.

Im Verdachtsfall

- Löschen Sie Phishing-Mails sofort, auch aus dem Papierkorb Ihres Computers oder Mail-Programms.
- Ignorieren Sie Links, die in Phishing-Mails hinterlegt sind. Hier könnte sich ein schädliches Computer-Programm verbergen.
- Sichern Sie regelmäßig Ihre selbst erstellten Dateien auf externen Speichermedien (zum Beispiel auf CD-ROM oder DVD). Falls ein Virus Ihr System beschädigt, können Sie auf diese Kopien zurückgreifen.
- Überprüfen Sie regelmäßig alle Buchungen auf Ihrem Konto; teilen Sie Unstimmigkeiten sofort Ihrem Bankberater mit.
- Informieren Sie sofort Ihre Bank, wenn Sie Daten in gefälschte Internet-Seiten eingegeben haben oder wenn Sie einen anderen Verdachtsfall haben. Zum Beispiel wenn die Verbindung während der Online-Banking-Anwendung abbricht. Sie können Ihr Konto sperren, indem Sie drei ungültige TAN eingeben.
- Lassen Sie im Schadensfall sofort die Überweisung zurückrufen, und erstatten Sie Anzeige.

So wählen Sie eine sichere Geheimzahl

Die Persönliche Identifikations-Nummer (PIN) ist – wie der Name schon sagt – eng mit Ihrer Person verbunden. Gerade beim Online-Banking ist es wichtig, dass die PIN außer Ihnen niemandem in die Hände fällt. Auch nicht mit Hilfe elektronischer Wörterbücher oder Suchmaschinen.

Was Sie vermeiden sollten

- Vermeiden Sie leicht zu erratende Kennwörter wie gleiche Zeichen und bekannte Zeichenfolgen (12345, 4711 oder 0815) oder Geburtstage, Postleitzahlen, Telefon-Nummern.
- Verwenden Sie auch keine Wohnorte oder Namen von Haustieren oder Familien-Angehörigen als PIN, auch keine Kombinationen wie „Tim32" oder „1Moni9".
- Computer-Hacker können einfache Tastenfolgen wie „qwertz", „12345" leicht knacken, auch wenn Sie Buchstaben und Ziffern kombinieren: „abcd09".
- Vermeiden Sie gebräuchliche Abkürzungen wie „ISDN", „GmbH" oder „NRW", um mit deren Hilfe eine PIN zu bilden.
- Speichern Sie PIN und TAN weder auf Ihrer Festplatte noch auf Zettel oder Schreibtisch-Unterlagen in der Nähe Ihres Computers.

Merkmale einer sicheren PIN

- Stellen Sie Ihre PIN aus Buchstaben und Zahlen zusammen.
- Verwenden Sie generell für unterschiedliche Zugänge (E-Mail, Online-Banking, Arbeitsplatz) möglichst unterschiedliche Passwörter.
- Eine sichere PIN erhalten Sie, wenn Sie zum Beispiel einen Satz als Eselsbrücke verwenden, den Sie sich gut merken können. Zusätzlich können Sie „i" durch „1" austauschen oder umgekehrt. So wird aus „Klaus ist ein versierter Heimwerker" die PIN „k1evh".
- Ändern Sie Ihre PIN regelmäßig.

Weitere Informationen im Internet

Wissenswertes zum Thema Internet-Sicherheit finden Sie – einfach und verständlich erklärt – auf den Seiten des Bundesamtes für Sicherheit in der Informationstechnik (BSI):

>> www.bsi-fuer-buerger.de