

Sicherheitshinweise bei der Nutzung des Internets und bei OnlineBanking

Das Medium Internet bringt neben vielen Vorteilen wie Informationsbeschaffung, OnlineBanking, E-Mail-Kommunikation, Preisvergleiche, Internet-Handel (z. B. eBay) usw. auch Gefahren mit sich. Kriminelle versuchen immer öfter das Internet dazu zu benutzen, um gut- und leichtgläubige Internet-Nutzer zu betrügen.

Mit diesem Informationsblatt möchten wir Sie auf die wichtigsten Gefahren hinweisen und Ihnen zeigen, wie Sie diese mit einfachen Mitteln ausschließen bzw. reduzieren können.

Die Gefahren betreffen die gesamte Nutzung des Internets und beziehen sich nicht ausschließlich auf den Bereich OnlineBanking.

Aufgrund der Vielzahl an Risiken und Möglichkeiten stellt diese Informationsschrift nur einen Ausschnitt dar und erhebt keinen Anspruch auf Vollständigkeit. Trotz sorgfältiger Prüfung können wir keine Gewähr für die Richtigkeit und Wirksamkeit der Aussagen übernehmen.

1.1 Was ist „Phishing“?

Phishing ist ein Kunstwort und setzt sich aus den englischen Begriffen „Password“ und „Fishing“ zusammen. Durch „Phishing“ versuchen Kriminelle, persönliche Kundendaten wie PIN- und TAN-Nummern, Kreditkartennummern, Passwörter zu Auktionshäusern usw. zu ergaunern, um diese dann missbräuchlich zu verwenden und so Schaden anzurichten.

Beim Phishing werden gefälschte E-Mails an beliebige E-Mail-Adressen gesandt. Diese E-Mails sehen aus wie offizielle Schreiben von Banken, eBay usw., das heißt, sie tragen das Firmenlogo, sind in der gleichen Schrift gestaltet und ähneln der Internet-Seite des Unternehmens.

Im Text ist oft die Rede von „Sicherheitsüberprüfungen“ oder anderen wichtig klingenden Maßnahmen. Alle Phishing-E-Mails verfolgen das Ziel, Sie durch eine eingebaute Internet-Verlinkung auf eine Formularseite weiterzuleiten, auf der Sie Ihre Geheimzahlen, TAN-Nummern und Passwörter eintragen sollen. Diese Formularseiten sind ebenfalls perfekt den offiziellen Internet-Seiten nachgebaut. Auch wenn Sie die Link-Adresse als richtig erkennen ist Vorsicht geboten – sie ist trotzdem gefälscht.

Der Absender dieser Mails weiß nicht, ob Sie wirklich mit dem angegebenen Unternehmen, z. B. „eBay“ zu tun haben. Er hofft, dass ein Teil der E-Mail-Empfänger auf den Phishing-Versuch hereinfällt und persönliche Daten weiterschickt.

1.2 Wie kann ich mich gegen „Phishing“ schützen?

- Seriöse Internet-Anbieter fragen niemals per E-Mail nach persönlichen Kundendaten wie PIN- oder TAN-Nummern.
- Antworten Sie grundsätzlich nicht auf E-Mails, bei denen - aus welchem Grund auch immer- nach Ihrer PIN oder TAN gefragt wird.
- Verwenden Sie keine Links aus E-Mails, um Ihr OnlineBanking aufzurufen. Geben Sie die Adresszeile immer von Hand ein oder benutzen Sie „Lesezeichen“ bzw. „Favoriten“ in Ihrem Internet-Browser (z. B. Internet-Explorer, T-Online-Browser, Mozilla, Firefox...), die Sie selbst angelegt haben.
- Löschen Sie derartige E-Mails, ohne sie zu öffnen.

Wir werden Sie nie auffordern, uns Ihre PIN oder TAN-Nummern, Kreditkartennummern... per E-Mail, SMS usw. mitzuteilen!

2.1 Was sind „Viren“, „Trojaner“ oder „Würmer“?

Hierunter versteht man Computerprogramme, die sich auf Ihrem PC einschleichen und Schaden anrichten. Sie sind ein grundsätzliches Risiko bei allen Computeranwendungen.

Diese Programme verbreiten sich über das Internet und können überall lauern, z. B. wenn Sie ungeschützt Daten und Anwendungen aus dem Internet auf ihren PC herunterladen. Derartige Schad-Programme können auch als Anhang von E-Mails auf Ihren PC gelangen.

So genannte "Trojanische Pferde" manipulieren – von Ihnen unbemerkt - die auf dem PC installierten Programme. Dies kann dazu führen, dass Eingaben und Bildschirmanzeigen Ihres PCs (z. B. mit PIN- und TAN-Nummern) über das Internet an fremde PCs weitergeleitet werden oder dass anstatt der von Ihnen aufgerufenen Seite eine nachgeahmte Internet-Seite erscheint, weil der Trojaner im Hintergrund die Internetadresse verändert (sog. Pharming).

So können Kriminelle an PIN und TAN-Nummern gelangen und diese dann für Überweisungen missbräuchlich verwenden.

Phishing-E-Mails (siehe Punkt 1.1) können auch mit Trojaner-Programmen im Datei-Anhang kombiniert auftreten! Es gibt auch E-Mails mit einem Trojaner als Mail-Anhang, bei denen als Absender namhafte Firmen wie „eBay“ oder „Deutsche Telekom“ angegeben ist. Diese E-Mails stammen nicht von den als Absender genannten Firmen sondern von Kriminellen!

2.2 Wie können Sie sich vor Viren, Trojanern und Würmern schützen?

- Installieren Sie entsprechende Sicherheits-Software (Viren-Scanner, Firewall usw.) auf Ihrem PC und aktualisieren Sie diese regelmäßig, am besten täglich (Updates).
- Halten Sie das Betriebssystem Ihres PC`s immer auf dem aktuellsten Stand (Updates).
- Stellen Sie Ihren Browser so ein, dass keine Software ohne Ihre ausdrückliche Zustimmung geladen werden kann.
- Setzen Sie ggf. alternative Browser ein, z. B. Opera, Mozilla usw.
- Installieren Sie nur Software, deren Hersteller Ihnen vertrauenswürdig erscheint.

Unter www.vr-computercheck.de können Sie Ihren PC einer kostenlosen Sicherheitsprüfung unterziehen. Wir empfehlen, diese Prüfung regelmäßig zu machen. Im Download-Bereich von www.vr-computercheck.de finden Sie entsprechende Sicherheits-Programme, die Sie auf Ihrem Computer installieren können.

3.1 Woran erkennen Sie, dass Ihre Internet-Verbindung zur Bank korrekt ist?

Grundlage der sicheren Internet-Verbindung beim eBanking ist die Verwendung des SSL Protokolls. Das Bestehen einer sicheren SSL-Verbindung wird Ihnen bei Verwendung von Firefox, Mozilla und Internet Explorer durch ein geschlossenes Schloß-Symbol angezeigt, bei Netscape durch die Darstellung eines ungebrochenen Schlüssel-Symbols. Ein weiteres Erkennungsmerkmal ist die Adresse (URL) selbst; beginnt sie mit https, so ist dies ein Zeichen für eine sichere Verbindung (z.B. <https://www.vr-ebanking.de>.....).

Prüfen Sie mit einem Doppelklick auf dieses Schloß- oder Schlüssel-Symbol die Echtheit des Zertifikates für diese Anwendung. Das Zertifikat für unser Internet-Banking ist ausgestellt auf „www.vr-ebanking.de“. Details zum Antragsteller: FIDUCIA IT AG (IT-Dienstleister Ihrer Raiffeisen-Volksbank). Wenn Sie den Verdacht haben, dass die vorliegende Webseite manipuliert ist, verlassen Sie diese und befolgen Sie keinesfalls die dort angegebenen Anweisungen. Informieren Sie ggf. Ihren Bankberater über die auffällige Seite.

Stellen Sie unabhängig von der Verschlüsselung innerhalb des eBanking sicher, dass Ihr PC frei von Viren, Trojanern usw. ist. Siehe hierzu Punkt 2.2.

3.2 Verlassen/Beenden des eBanking

- Verlassen Sie die eBanking-Anwendung immer ordnungsgemäß über den Navigationspunkt "Abmelden" (links oben).
- Sollten Sie einmal vergessen haben, die Anwendung zu beenden, oder längere Zeit Ihren Rechner unbeaufsichtigt lassen, keine Angst: Die eingebaute Zeitsperre bricht das Programm ab, sobald fünfzehn Minuten lang keine Eingabe erfolgte.
- Um sicherzustellen, dass kein unberechtigter Dritter Einsicht auf Ihre online abgefragten Daten erhält, empfehlen wir Ihnen beim Beenden der Anwendung eBanking den "Cache/temporäre Internetdateien" im Browser zu löschen. Im Internet-Explorer erfolgt dies z. B. über „Extras“ – „Internetoptionen“ – „temporäre Internetdateien“ – „Dateien löschen“.

4. Allgemeine Sicherheitshinweise

- Gehen Sie vorsichtig mit Ihren eigenen, vertraulichen Daten um!
- Seien Sie kritisch im Umgang mit E-Mail und beim Surfen im Internet!
- Achten Sie auf Veröffentlichungen Ihres Internet-Anbieters auf dessen Web-Sites!
- Fragen Sie sich, ob die auf der Webseite geforderten Eingaben in Zusammenhang mit der von Ihnen gewünschten Aktion Sinn machen.
- Öffnen Sie sicherheitsrelevante Seiten immer in einer neuen Browser-Sitzung, nachdem Sie vorher alle Browser-Fenster geschlossen haben.
- Sollten Sie versehentlich eine zweifelhafte Internetseite besucht und Ihre Daten (eBanking PIN, eBanking TANs, Kreditkartennummern und PIN, EC-Kartenummer und PIN...) preisgegeben haben, so lassen Sie am sichersten die betroffene Karten und Konten sperren. Ändern Sie mindestens die PIN und sperren Sie betroffene TAN-Bögen. Dies erfolgt einfach durch dreimalige Eingabe einer falschen PIN oder TAN. Wenden Sie sich in jedem Fall an Ihren Bank-Berater!
- Beachten Sie, dass E-Mails im Regelfall unverschlüsselt sind und mitgelesen werden können (vergleichbar einer elektronischen Postkarte). Vermeiden Sie es grundsätzlich persönliche Informationen oder vertrauliche Daten per E-Mail unverschlüsselt zu versenden.
- Speichern Sie vertrauliche Daten wie PIN und TAN oder Passwörter nicht auf Ihrer Festplatte.
- Ändern Sie - wenn möglich - regelmäßig Ihre PIN und Passwörter.
- Benutzen Sie für Onlinebanking möglichst keine Rechner in Internetcafés; hier sind Manipulationen Tür und Tor geöffnet.
- Bei der freien Wahl Ihres selbst gewählten Kennwortes sollten Sie leicht zu erratende Kennwörter wie gleiche Zeichen und regelmäßige Zeichenfolgen (12345) ebenso vermeiden wie Geburtstage, Postleitzahlen, Telefonnummern oder bekannte Zeichenfolgen (wie 4711 und 0815).
- Überprüfen Sie regelmäßig Ihre Konto-Bewegungen; teilen Sie Unstimmigkeiten umgehend Ihrem Bankberater mit.

5. Hotline zum Thema „Sicherheit im Internet“

Benötigen Sie Hilfestellung speziell zum Thema Sicherheit oder möchten Sie einen Phishing-Verdachtsfall melden? Dann wählen Sie die zentrale Rufnummer 0180 50 53 111 (12 Cent pro Minute aus dem Festnetz der Deutschen Telekom). Ihr Anruf wird täglich in der Zeit von 8:00 bis 24 Uhr entgegen genommen. Bei technischen Fragen zu eBanking wenden Sie sich bitte direkt an Ihren Bankberater oder die Electronic Banking-Hotline 08671/505-1234.

6. Betragslimit für Online-Überweisungen:

Vereinbaren Sie mit uns ein Tageslimit für Online-Überweisungen. So kann möglicher Schaden begrenzt werden.

7. Alternative OnlineBanking-Verfahren:

Neben dem reinen InternetBanking „eBanking“ über unsere Homepage bieten wir Ihnen die Möglichkeit, OnlineBanking mit PC-Software (VR-NetWorld-Software oder ProfiCash) über den HBCI-Standard zu nutzen.

HBCI ist mit PIN/TAN- Absicherung, mit Absicherung durch Schlüsseldatei oder mit HBCI-Chipkarte möglich.

Grundvoraussetzung für die Datensicherheit beim OnlineBanking ist bei allen drei HBCI-Verfahren, dass auf Ihrem PC keine Viren, Trojaner usw. installiert/versteckt sind.

8. Im Falle eines Falles:

Sind Sie Opfer eines Phishing-E-Mails geworden oder wurden von Ihrem Konto Überweisungen getätigt, die Sie nicht selbst veranlasst haben, informieren Sie bitte unverzüglich Ihren Berater und erstatten Sie Anzeige bei der Kriminalpolizei. Speichern Sie die gefälschte E-Mail zur Beweissicherung. Falls noch möglich, machen Sie Ihre PIN für den Betrüger unbrauchbar, indem Sie sie durch eine neue ersetzen oder sperren.