



Volksbank Plochingen eG

Das Internet stellt viele Möglichkeiten zur Verfügung. Es ist immer und nahezu überall verfügbar - weltweit. Da liegt es nahe, auch die persönlichen Bankgeschäfte online zu erledigen. Im weltweiten Netz tätigen Sie zum Beispiel einfach und bequem Ihre Überweisungen oder rufen zu jeder Tageszeit Ihren Kontostand ab. Aber das Internet birgt auch Gefahren. Vermehrt warnen Experten und Medien jetzt vor Risiken wie z.B. Phishing-Attacken, neuen Viren oder Würmern. Trotzdem können Sie die Vorzüge des Online-Bankings gesichert nutzen, wenn Sie diese Gefahren kennen und wissen, wie Sie die Abwehr Ihres PCs stärken.

Wir helfen Ihnen gerne und zeigen einige Möglichkeiten auf, wie Sie Ihren PC ganz einfach und wirkungsvoll vor unerwünschten Zugriffen schützen.

Machen Sie sich mit den Gefahren vertraut

Phishing

Beim Password-Fishing, kurz Phishing, versuchen Kriminelle über das Internet an Ihre persönlichen Geheimzahlen PIN und TAN zu gelangen. Sie erhalten in der Regel eine E-Mail, die angeblich von Ihrer Bank stammt. Darin werden Sie aufgefordert, durch einen Link die Internetseite Ihrer Bank zu besuchen und dort PIN und TAN einzugeben, da diese Daten abhanden gekommen seien. Es handelt sich hierbei um eine gefälschte Bankseite, die lediglich zum Ausspionieren Ihrer Daten dient. Sie können sich ganz sicher sein: Ihre Bank wird Sie nie nach Ihrer PIN und/oder Ihren TANs fragen. Geben Sie deshalb Ihre persönlichen Daten auf keinen Fall weiter.

Pharming

Beim Pharming werden Sie während des Surfens im Internet auf eine gefälschte Seite gelotst. Dabei setzen die Betrüger auf eine Manipulation der technischen Abläufe beim Aufrufen der Seite. Ziel ist es, vertrauliche Informationen zu stehlen. Es handelt sich hierbei um eine Fortentwicklung des klassischen Phishings.

Viren, Würmer und Trojaner

Immer wieder gibt es Schlagzeilen zu neuen Varianten von Viren, Würmern oder Trojanern. Diese infizieren beim Surfen im Internet z.B. über Sicherheitslücken im Internet-Explorer unbemerkt Ihren PC oder werden als E-Mail-Anhänge verbreitet. Haben Sie erstmal eine dieser Varianten auf dem PC ist es schwer, sie wieder loszuwerden. Wenn Sie aber die Funktionsweise dieser Internet-Parasiten kennen, können Sie sich entspannt im Internet bewegen. Öffnen Sie keine Anhänge von unbekanntem E-Mail-Absendern oder Anhänge, die Ihnen ein unbekannter Absender unaufgefordert schickt und schützen Sie Ihren PC mit Antivirus-Software und Firewall.

Allgemeine Verhaltensregeln für den sicheren Umgang mit Internet und OnlineBanking.

Regel Nr. 1:

Machen Sie einen persönlichen Sicherheitscheck

Nehmen Sie sich, bevor Sie Ihren neuen Internet-Anschluss aktivieren, einige Minuten Zeit und machen Sie einen persönlichen und realistischen Sicherheitscheck. Nutzen Sie die Sicherheitseigenschaften des Betriebssystems und installieren Sie keine überflüssige Server-

Software, durch die der Rechner erst von außen erreichbar wird. Vor allem: Welchen Schaden verkraften Sie, wenn trotz aller Vorsicht etwas schief geht? Hier gilt z.B.: Ein PC, der größere Mengen sensibler Daten speichert (z. B. den Geschäftsverkehr eines Rechtsanwaltes), sollte nicht als Internet-PC eingesetzt werden. Außerdem: Ein Online-Shopper wird sich vor allem um die Sicherheit bei der Übermittlung

seiner Kreditkartennummer kümmern, während diejenigen, die gerne in den Internet-Programmsammlungen stöbern, sich vorwiegend mit der Wirksamkeit von Antiviren-Programmen auseinandersetzen sollten. In jedem Fall heißt es: Bleiben Sie realistisch. Nicht überall im Internet lauern Piraten, die es nur darauf abgesehen haben, Ihre privaten E-Mails zu lesen. Nicht jeder "Chat-Partner" ist darauf aus, Sie um Ihre Ersparnisse zu erleichtern.

Regel Nr. 2:

Überlegen Sie genau, wer Ihr Vertrauen verdient

Denn nicht jeder ist im Internet das, was er zu sein vorgibt. Für Experten ist es vergleichsweise einfach, z. B. eine E-Mail-Adresse zu fälschen oder eine ganze Web Site vorzugaukeln - sogar die Ihrer Hausbank, der Sie Ihre Kundendaten mitteilen, um sich auszuweisen. Vorsicht ist ebenso angebracht bei manchem günstigen Angebot im Web. Die Seriosität des Anbieters kann schwer zu überprüfen sein. Vergleichen Sie also regelmäßig die Adressen, die Sie in der sog. URL-Leiste angeben (oder des Links, den Sie anklicken), mit den Angaben, die Sie in der Taskleiste sehen. Diese Angaben sind schwieriger zu fälschen. Und darüber hinaus: geben Sie Informationen nur preis, wenn Sie verlässlich wissen, wer diese Daten erhält und was mit diesen geschehen soll. "Social Engineering", d. h. Erschleichung von Auskünften bei potentiellen Opfern, ist bei Hackern beliebt, um an benötigte Informationen zu kommen ("Entschuldigen Sie, ich heiße Meyer, bin Sicherheitschef bei X-Online und brauche Ihr Passwort, um Sicherheitstests durchführen zu können.").

Regel Nr. 3:

Speichern Sie sensible Daten (Passwörter, Kreditkartennummern usw.) nicht auf Ihrer Festplatte ab

Denn der Zugriff auf die Festplatte steht nicht nur dem PC-Eigentümer offen; solange Sie online sind, können sich grundsätzlich auch Außenstehende ein Bild von Ihrem Datenspeicher machen. Dies erfordert zwar überdurchschnittliches Expertenwissen, doch Ihr Computer hat im Netz eine eigene Adresse und ist damit zugänglich auch für "Kontaktangebote" der unerwünschten Art. Ein wichtiger Tipp für Windows 9x-Nutzer: Speichern Sie vor allem Ihr Passwort für den Anwahlvorgang nicht ab; so erschweren Sie den Aufbau unerwünschter Internet-Verbindungen. Am besten trennen Sie die Leitung nach Abschluss Ihrer Online Sitzung auch "physikalisch", d. h. lösen das Modem-

bzw. ISDN-Kabel zwischen PC und Telefonanschluss.

Regel Nr. 4:

Wechseln Sie regelmäßig Ihre Passwörter/PIN

Wählen Sie dabei ein sicheres Passwort bzw. eine sichere PIN. Verwenden Sie hierzu keine Informationen, die unmittelbar mit Ihnen oder Ihrem Umfeld in Verbindung gebracht werden können, wie zum Beispiel Namen oder Geburtsdatum.

Regel Nr. 5:

Betrachten Sie Programme aus dem Internet zunächst grundsätzlich als unzuverlässig

Denn Sie können kaum sicher beurteilen, ob die Quelle seriös ist. Mit Programmen, die aus dem Internet auf die heimische Festplatte geladen werden, können Viren oder Trojanische Pferde übertragen werden. Dies kann auch durch das Öffnen eines Anhangs einer elektronischen Mail geschehen. Deshalb öffnen Sie solche Anhänge nicht, während Sie gerade online sind. Speichern Sie den Inhalt zuerst ab, prüfen Sie ihn mit entsprechenden Programmen oder durch Kontrolle des Quellcodes (z. B. bei einem JavaScript-Programm) und öffnen Sie erst dann die fragliche Datei. Testen Sie unbekannte Programme, falls möglich, auf einem Zweitrechner. Und beobachten Sie aufmerksam, ob es dabei zu "Überraschungen" kommt, wie z. B. Warnmeldungen Ihres PCs oder nicht von Ihnen veranlasste Einwahlversuche.

Regel Nr. 6:

Nutzen Sie nur die aktuelle Version Ihrer bevorzugten Internet- Zugangssoftware

Denn nur die jeweils aktuellen Versionen der gängigen Internet-Software können gewährleisten, dass die bis dahin bekannt gewordenen Sicherheitslücken in diesen Programmen geschlossen sind. Fast täglich werden neue Sicherheitsprobleme entdeckt, zu schnell um jeweils mit neuen Versionen des ganzen Programms darauf zu antworten. Nicht zuletzt deshalb arbeiten die Programmierer der großen Hersteller stets mit Hochdruck daran, sog. "Bug-Fixes" zu entwickeln, d. h. kleine Programme, mit denen sich diese konkreten Probleme beheben lassen. Informieren Sie sich deshalb regelmäßig über die neueste Entwicklung: Die meisten Hersteller unterhalten entsprechende Informationsdienste. Überlegen Sie sich genau, ob Sie Zusatzprogramme, z. B. zum Darstellen von 3D-Welten oder zum Audio-Empfang in Ihren Web-Browser einbinden wollen. Denn auch solche Zusatzprogramme, sog. Plug-Ins,

können zusätzliche, unkontrollierbare Sicherheitslücken eröffnen.

Regel Nr. 7:

Aktivieren Sie die Sicherheitsoptionen Ihres Internet-Browsers

Denn Ihre Sicherheit im Internet lässt sich beträchtlich steigern, wenn Sie die Sicherheitsoptionen Ihres Internet-Browser intelligent einsetzen. Wichtig ist hier vor allem, dass Sie die Zulassung von ActiveX-Controls ausschließen und die Ausführung von Java-Applets nur nach Rückfragen gestatten. Bei diesen sog. "aktiven Inhalten" handelt es sich um kleine eigenständige Programme, die auf Ihrem PC ausgeführt werden und dort u. U. ein unkontrollierbares Eigenleben entwickeln können (z. B. Ihre Passwortdatei per E-Mail versenden). Ob Sie die sog. "Cookies" ausschließen wollen, müssen Sie ganz individuell entscheiden. Im Zweifel entscheiden Sie sich gegen solche "Kekse", die eine fremde Web Site auf Ihrer Festplatte ablegt, denn diese Daten können auch dazu genutzt werden, um Benutzerprofile anzulegen.

Regel Nr. 8:

Setzen Sie zusätzliche Sicherheitssoftware ein

Denn manche Sicherheitsprobleme lassen sich nicht alleine "mit Bordmitteln" lösen. Wichtigstes Zusatzwerkzeug: Ein leistungsfähiger Virensch scanner, der in der Lage ist, auch neue Viren zu erkennen. Fast täglich werden neue Viren entdeckt und es ist durchaus möglich, dass Sie sich bei einem Ausflug in die Online-Welt "infizieren". Bei weiterer Sicherheitssoftware sollten Sie ernsthaft prüfen, vor welchen konkreten Gefahren Sie sich dadurch schützen wollen und vor allem, ob das Kosten/Nutzen-Verhältnis stimmt. Denn hierbei gilt ebenfalls: Absolute Sicherheit kann es auch im Internet nicht geben - selbst wenn manche Hersteller das versprechen.

Regel Nr. 9:

Übermitteln Sie sensible Daten über offene Leitungen niemals unverschlüsselt

Denn jede Datenübertragung im Internet kann von potentiellen Angreifern grundsätzlich abgefangen und ausgespäht werden. Schützen Sie daher Ihre private und geschäftliche Korrespondenz durch den Einsatz sicherer Verschlüsselungsverfahren. Die Qualität hängt dabei nicht nur von der Schlüssellänge und dem verwendeten Algorithmus ab. Auch Verfahren mit 40 Bit Schlüssellänge, wie sie heute teilweise im Einsatz sind, bieten einen gewissen Schutz. Die Verwendung von längeren Schlüsseln ist aber in jedem Fall empfehlenswert. Ein

Angreifer mit einer "normalen" Ausstattung, müsste dann erhebliche Mühe aufwenden, um aus dem Kryptogramm den Klartext zu gewinnen - meist mehr Mühe, als es die verschlüsselten Daten wert sind.

Regel Nr. 10:

Machen Sie regelmäßige Sicherheitskopien (Backups) von Ihren Datenbeständen

Dies ist eine der wichtigsten Regeln überhaupt, denn es ist meist zu spät (und wenn, dann sehr teuer), die gespeicherten Informationen zu retten, falls das "Kind erst einmal in den Brunnen gefallen ist". Zum bequemen Datensichern können Sie z. B. eine Wechselfestplatte, einen CD-Brenner, oder ein Streamer-Laufwerk einsetzen. Wichtig ist jedoch, dass Sie regelmäßig (ca. alle zwei Wochen) eine Sicherung der geänderten sowie der neu dazugekommenen Daten vornehmen. Und bewahren Sie Ihre Backups sicher, d. h. getrennt vom PC, auf.

Regel Nr. 11:

Konfigurieren Sie sich einen eigenen Internet-PC (für Power-Surfer)

Ganz Sicherheitsbewusste sollten mit einem separaten PC in das Internet starten. Ausstattung: Betriebssystem und Internetzugangsoftware, ggf. ein Virenschutzprogramm. Dann sind Sie in der Tat sicher vor den meisten Bedrohungen, die derzeit vom weltweiten Datennetz bekannt sind. Und internettaugliche PC's sind heute bereits kostengünstig zu haben (Mindestausstattung: 133 MHz, 32 MB RAM, 500 MB Festplatte). Halten Sie sich dennoch zusätzlich an unsere Sicherheitstipps. So kann kaum noch etwas schief gehen bei Ihren Ausflügen in die Online-Welt.

Regel Nr. 12:

Löschen Sie Werbung und Werbe-E-Mails von unbekanntem Absendern

Aber löschen Sie die Werbung bitte noch vor dem Anschauen/Öffnen! Es könnten Viren enthalten sein oder es könnte für Sie kostspielig werden. Wir empfehlen Ihnen zur Sicherheit ein Virenschutzprogramm.

Regel Nr. 13:

Achten Sie auf die SSL-Verschlüsselung

Die E-Banking-Anwendung wird immer verschlüsselt gestartet. Achten Sie darauf, dass beim Aufruf der E-Banking-Anwendung eine verschlüsselte Verbindung aufgerufen wird. Eine sichere und verschlüsselte Verbindung erkennen Sie in Ihrem Browser an dem geschlossenen Schloss-Symbol.

Regel Nr. 14:

Überprüfen Sie das Zertifikat zur SSL-Verschlüsselung

Durch einen Doppelklick auf das Schloss-Symbol können Sie über die Detailinformationen des Zertifikats feststellen, wer der Antragsteller ist. Eine sichere Verbindung zum EBanking ist nur vorhanden, wenn als Antragsteller "FIDUCIA" bzw. "Rechenzentrale Bayerischer Genossenschaften" angegeben wird. Zusätzlich sollten Sie die Gültigkeit des Zertifikats prüfen. Abgelaufenen Zertifikaten sollten Sie nicht vertrauen.

Regel Nr. 15:

Überprüfen Sie regelmäßig Ihre Kontobewegungen

Informieren Sie umgehend Ihre Bank, wenn Sie eine Buchung nicht nachvollziehen können.

Regel Nr. 16:

Lassen Sie bei Missbrauchsverdacht sofort Ihren E-Banking-Zugang sperren

Informieren Sie umgehend ihre Bank bzw. sperren Sie Ihren E-Banking-Zugang selbst, wenn sie einen Missbrauchsverdacht haben.

Ein zusätzliches Sicherheitsplus stellt die Nutzung einer OnlineBanking-Software dar. Damit haben Sie die Möglichkeit, Ihre Zahlungsverkehrsaufträge offline und in aller Ruhe zu erfassen. Eine Internet-Verbindung muss nur für den Versand der Aufträge hergestellt werden. Für weitere Informationen wenden Sie sich bitte an unsere Berater für den Elektronischen Zahlungsverkehr unter der Rufnummer 07153/706-277 oder senden Sie uns eine eMail an:
ezv@volksbank-plochingen.de