Impressum

Herausgeber:
Initiative D21 e.V. und Bayerisches Staatsministerium der Justiz und für Verbraucherschutz

Redaktion:
Martin Falenski (Initiative D21) – V.i.S.d.P.

Gestaltung:
Ulrike Miller, www.miller-partners.com

Kontakt:
Initiative D21, Reinhardtstraße 38, 10117 Berlin
kontakt@initiatived21.de, www.initiatived21.de

Bayerisches Staatsministerium der Justiz und für Verbraucherschutz
Prielmayerstraße 7, 80335 München
poststelle@stmjv.bayern.de, www.justiz.bayern.de

Bildnachweis:
dreamstimes.com
i stockphoto.com

Aufbruch Bayern

Besondere Gefahren: Online Banking

Mal eben noch schnell eine Überweisung tätigen? Mit Online-Banking geht das bequem vom heimischen Sofa aus. Bereits 28 Millionen Bundesbürger nutzen nach Angaben des BITKOM das Internet, um Bankgeschäfte zu erledigen. Der Nutzer muss sich jedoch bewusst sein: Eine 100%ige Sicherheit gibt es beim Online-Banking nicht! Daher sind einige Sicherheitsvorkehrungen zu treffen.

Obwohl besondere Signaturverfahren grundsätzlich mehr Sicherheit bieten, ist das einfacher handhabbare PIN/TAN-Verfahren am meisten verbreitet. In der Regel kommen dabei das sogenannte iTAN-oder das mobileTAN-Verfahren zum Einsatz.

Die größten Gefahren drohen beim Online-Banking durch das sogenannte Phishing, dem Abgreifen von Kontodaten mittels einer gefälschten E-Mail („phishing" (engl.) = (ab-) fischen) oder durch das Ausspähen von Daten mittels einer Spionage-Software.

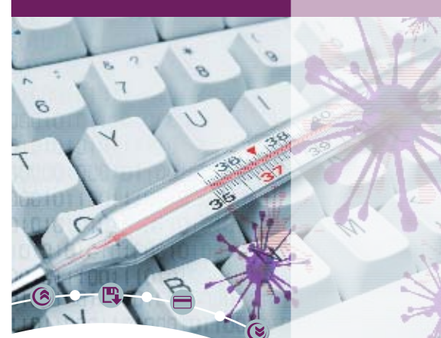
Sicherheitstipps:

- Achten Sie auf verschlüsselte Kommunikation. Die Web-Adresse der Bankseite muss mit einem „**https**" beginnen. Außerdem sieht man ein **Schlosssymbol** im Eingabefenster des Browsers.
- Nie Online-Banking von öffentlich zugänglichen Netzen (zum Beispiel Cafés mit einem Internetzugang) aus machen.
- Geben Sie die Adresse der Bank manuell in das Browserfenster ein. Das Anklicken eines Links kann Sie auf eine Phishingseite führen.
- Nutzen Sie nur sichere Passwörter (Kombination aus Groß- und Kleinbuchstaben, Ziffern und Sonderzeichen).
- Vereinbaren Sie mit Ihrer Bank ein nach oben begrenztes Wochenlimit und prüfen Sie regelmäßig Ihre Kontovorgänge.
- Prüfen Sie – wenn möglich – die Echtheit der Seite. Viele Banken bieten zum Beispiel ein Zertifikat an, das die Echtheit belegt.
- Kommt Ihnen irgendetwas anders vor als sonst? Im Zweifel lieber Finger weg und die Bank informieren!

Im Notfall sollte man das Konto telefonisch sperren lassen: Entweder direkt bei der Bank oder den zentralen Sperr-Notruf **116 116** wählen (aus dem Ausland **0049 116 116**).

Verhält sich der Rechner irgendwie anders? Haben Sie das Gefühl, er ist langsamer als sonst oder im Hintergrund laufen irgendwelche Prozesse? Trotz aller Vorsicht können PC oder SmartPhone doch einmal mit einem Schädling infiziert sein. Die Folge können manipulierte Daten, ausgespähte Informationen oder die komplette Übernahme des Systems durch einen Dritten sein. Nun heißt es: Ruhe bewahren – aber schnell handeln!

- Gehen Sie offline. Kappen Sie alle Verbindungen des Rechners ins Internet.
- Überprüfen Sie den PC oder das SmartPhone komplett mit einem Virenschutzprogramm, das auf dem aktuellsten Stand ist.
- Sichern Sie vorsorglich Ihre Daten auf einem externen Speichermedium.
- Schalten Sie den Rechner aus und holen Sie sich gegebenenfalls professionelle Hilfe. Man kann unter Umständen mit der Änderung der Boot-Reihenfolge und einer System-CD den Rechner relativ einfach vom Schädling befreien.
- Versuchen Sie festzustellen, woher der Schädling kam und vermeiden Sie künftig die Quelle.
- Wenn Sie wieder online sind, kann die Überprüfung des Systems durch einen zusätzlichen Online-Scan sinnvoll sein. Eine Auswahl findet man zum Beispiel unter https://www.botfrei.de/scanner.html.
- Auf den Seiten des Antibotnetz-Beratungszentrums findet man auch Tipps und Tricks, wie man besonders hartnäckige Schädlinge etwa mit Hilfe einer kostenfreien Rettungssystem-CD bekämpfen kann (www.botfrei.de).



Gut zu wissen!

GUT ZU WISSEN – Verbraucherschutz in Bayern

Gefahren aus dem Netz

Viren, Würmer & Co.

INITIATIVE D21

Bayerisches Staatsministerium der Justiz und für Verbraucherschutz

Einführung

Liebe Leserin, lieber Leser,
über 76% der deutschen Bevölkerung sind online, Tendenz steigend. Die Zugangsmöglichkeiten werden immer vielfältiger, die Infrastrukturen immer komplexer. Wer hätte vor fünf Jahren gedacht, dass man ganz einfach über das TV-Gerät ins Internet kommt oder dass man im Auto Online-Anwendungen nutzt? Das hat aber seinen Preis: Die wachsende Vernetzung bringt Gefahren mit sich, da die Netze angreifbarer werden. Niemand möchte erleben, dass die Daten auf dem heimischen PC durch einen Virus oder einen anderen Schädling aus dem Internet vernichtet werden, weil das Smartphone infiziert wurde. Treffen Sie Vorkehrungen, um Ihre Systeme und Daten zu schützen! Dieser Flyer soll Ihnen dabei eine kleine Hilfestellung sein.

Ihre Dr. Beate Merk, MdL

Bayerische Staatsministerin der Justiz und für Verbraucherschutz

Überblick: Gefahren aus dem Netz

Computer, Smartphone und Co. bringen immensen Nutzen, bergen aber auch eine Vielzahl von Gefahren. Derzeit werden wieder eine Vielzahl von Phishingmails registriert. Auch Postkunden sind aktuell im Visier der Versender von Schadmails; in der Anlage findet sich ein Trojaner, der die Daten der arglosen Nutzer ausspäht.

Wenn man nicht auf einige Sicherheitsvorkehrungen achtet, können Bilder, Songs und sonstige Daten ganz schnell unwiderruflich verloren sein.

Auch finanzielle Schäden können drohen.
Die größten Gefahrenquellen sind:

- **Viren:** Sind Programme, die sich selbst verbreiten. Einmal infiziert, kann die Hard- und die Software des Opfers manipuliert werden und Schaden nehmen. Das Virus wird in der Regel automatisch mit einem anderen (dem infizierten) Programm gestartet.
- **Würmer**: Im Gegensatz zu einem Virus versuchen Computerwürmer aktiv und eigenständig Prozesse zu manipulieren. Traurige Berühmtheit erlangte etwa der Computerwurm „I love you", der unter anderem alle Bilder auf den infizierten Rechnern löschte.
- **Trojanische Pferde:** Schadsoftware, die an einem (scheinbar) nützlichen Programm angedockt ist, das der arglose Nutzer heruntergeladen hat. Hierunter fallen etwa viele Spionage-Programme („Spyware"), die es dem Täter erlauben, Vorgänge auf dem Rechner des Opfers mitzuverfolgen.

Oftmals treten auch Mischformen dieser sogenannten „Malware" (Schachtelwort aus „malus" = lat. für „schlecht" und „ware" von „Software") in Erscheinung.

Sicherheitsvorkehrungen – Checkliste:

- Immer ein aktuelles Virenschutzprogramm verwenden. Achtung: Kostenfreie Lösungen schützen oftmals nicht vollumfänglich. Wichtig ist zum Beispiel auch der Schutz beim Surfen im Netz, da manipulierte Seiten auch durch das bloße Aufrufen einen Rechner infizieren können. Prüfen Sie regelmäßig, ob Updates vorhanden sind oder nutzen Sie die automatische Updatefunktion.
- AntiSpy-Programme schützen vor unerwünschten Beobachtern oder davor, dass Daten (zum Beispiel bei der Passworteingabe) unbemerkt übermittelt werden.
- Nutzen Sie eine Firewall, die den Datenverkehr überwacht und zusätzlichen Schutz vor Eindringlingen bietet.
- Installieren Sie regelmäßig die Updates des Betriebssystems oder sonstiger Software (zum Beispiel Java).
- Erhöhen Sie die Sicherheitseinstellungen Ihres Browsers. Tipps dazu finden Sie in der Regel beim Anbieter selbst (z.B. www.internet-explorer.de, www.google.com/chrome).

Links/weiterführende Informationen:

- **www.vis.bayern.de:** Verbraucherportal der Bayerischen Staatsregierung zu allen wichtigen Verbraucherthemen wie zum Beispiel Rechte der Verbraucher. Die Sicherheit im Netz bildet im Bereich Daten und Medien einen eigenen Schwerpunkt.
- **www.bsi-fuer-buerger.de:** Informationsseite des Bundesamtes für Informationssicherheit über die Gefahren des Internets und wie man ihnen am besten begegnet.
- **www.verbraucher-sicher-online.de:** Ein vom Bundesverbraucherschutzministerium gefördertes Projekt der TU Berlin. Ziel ist es u.a., Verbraucher über die sichere Internetnutzung sowie den Zugang zu digitalen Inhalten und Informationen verständlich zu informieren.
- **www.polizei-beratung.de:** Informationsseite der Polizeilichen Kriminalprävention der Länder und des Bundes mit ausführlichen Hinweisen zu den Gefahren im Internet.
- **www.heise.de/security**: Portal zum Thema IT-Sicherheit des Heise-Verlages mit aktuellen Tests und Hinweisen.
- **www.sicher-im-netz.de:** Seiten des Vereins „Deutschland sicher im Netz" mit Hinweisen für Verbraucher für mehr IT-Sicherheit.