

Safer Internet Day 2009

FAQ der BSI-Hotline

Anlässlich des Safer Internet Day am 10. Februar 2009 beantwortete das Bundesamt für Sicherheit in der Informationstechnik (BSI) telefonisch alle Fragen rund um das Thema "Surfen – aber sicher!". In diesem Dokument finden Sie die häufigsten Fragen und dazugehörigen Antworten.

1. Was muss ich beim Einkaufen im Internet beachten?

Beim Online-Shopping gibt es gerade in punkto Sicherheit ein paar Dinge, die man beachten sollte:

- Informieren Sie sich über Ihren Geschäftspartner!
- Achten Sie darauf, dass Ihre Daten verschlüsselt übertragen werden!
- Sichern Sie Ihre Daten!
- Bewahren Sie Zugangscodes sicher auf!
- Verzichten Sie auf das Ausführen "Aktiver Inhalte"!
- Schützen Sie sich vor Internet-Schädlingen!
- Prüfen Sie, ob alternative Bestellmöglichkeiten existieren!
- Reagieren Sie nicht auf Phishing-Mails!

2. Wie sieht ein sicheres Passwort aus?

Es sollte mindestens acht Zeichen lang sein und neben Buchstaben auch Sonderzeichen und/oder Zahlen enthalten. Dabei sollten allzu gängige Varianten vermieden werden, also nicht 1234abcd usw. Einfache Ziffern am Ende des Passwortes anhängen oder eines der üblichen Sonderzeichen \$, !, ?, #, am Anfang oder Ende eines ansonsten simplen Passwortes ist ebenfalls nicht empfehlenswert.

3. Was sind „Aktive Inhalte“ und wieso ist das gefährlich?

Wenn Sie die Grundeinstellung Ihres Browsers unverändert lassen, erlauben diese meist die Ausführung nicht sichtbarer Funktionen, die in den besuchten Internetseiten verborgen sein können. Solche versteckten Programmteile oder Skripte werden als "Aktive Inhalte" bezeichnet. Die bekanntesten sind: Java-Applets, ActiveX-Controls, JavaScript und VBScript. Da Sie nicht an der in Ihrem Browser angezeigten Seite erkennen können, welche Funktionen sich im einzelnen dahinter verbergen, haben Sie als Benutzer keinerlei Kontrolle dar-

über, wer auf Ihren Rechner zugreift und was die Aktiven Inhalte eigentlich alles auf Ihrem PC anstellen. Über "Aktive Inhalte" können Spionageprogramme oder illegale Dialer auf ihrem Rechner installiert werden. Aber auch einmalige Aktionen können beim Besuch einer Webseite mit Aktiven Inhalten ausgeführt werden, die Ihre Daten im Zweifelsfall in Mitleidenschaft ziehen. Deshalb empfiehlt das BSI, „Aktive Inhalte“ prinzipiell auszuschalten.

4. Was muss ich beim Online-Banking beachten?

Alle Gefahren, die Ihnen auch sonst im Internet drohen, gibt es auch bei Bankgeschäften über das Internet. Ihre Daten können bei der Übertragung ausspioniert, verändert oder sogar gelöscht werden. Wenn Sie folgende Regeln beachten, können Sie Ihr Risiko auf ein Minimum reduzieren:

- Setzen Sie Verschlüsselung ein. Prüfen Sie die Echtheit der Bank-Website.
- Geben Sie die Internetadresse Ihrer Bank bei jedem Aufrufen erneut über die Tastatur ein. Bereits minimale Abweichungen weisen auf eine gefälschte Web-Seite hin.
- Wählen Sie Zugangsdaten sorgfältig aus und gehen Sie vorsichtig damit um. Schützen Sie Kennwörter und Zugangsdaten wie PIN und TAN vor dem Zugriff Dritter und speichern Sie solche Zugangsdaten keinesfalls ab – auch nicht im Passwort-Manager
- Betreiben Sie Online-Banking, soweit möglich, nur von eigenen Geräten aus.
- Setzen Sie nur Programme aus vertrauenswürdiger Quelle ein.
- Schützen Sie Ihren PC vor unerlaubten Zugriffen und setzen Sie aktuelle Virenschutzsoftware und Firewalls ein.
- Spielen Sie aktuelle Sicherheitsupdates für Ihr Betriebssystem ein.
- Überprüfen Sie regelmäßig Ihre Kontenbewegungen!
- Vereinbaren Sie mit Ihrer Bank ein Limit für tägliche Geldbewegungen beim Online-Banking.
- Reagieren Sie nicht auf Phishing-Mails!
- Sperren Sie Ihren Online-Banking-Zugang, wenn Ihnen etwas verdächtig vorkommt.

5. Was ist ein Botnetz?

Im IT-Fachjargon ist mit Bot ein Programm gemeint, das ferngesteuert auf Ihrem PC arbeitet. Von Botnetzen spricht man dann, wenn sehr viele PCs, meist mehrere Tausend, per Fernsteuerung zusammengeschlossen und zu bestimmten Aktionen missbraucht werden.

6. Woran erkennt man Phishing-E-Mails?

- Die Anrede ist unpersönlich gehalten ("Lieber Kunde der x-Bank!")
- Dringender Handlungsbedarf wird signalisiert ("Wenn Sie nicht sofort Ihre Daten aktualisieren, gehen diese verloren...")
- Drohungen kommen zum Einsatz ("Wenn Sie das nicht tun, müssen wir Ihr Konto leider sperren...")
- Vertrauliche Daten (z.B. PINs und TANs) werden abgefragt, z.B. in einem Formular innerhalb der E-Mail.
- Die Mails enthalten Links oder Formulare, die vom Empfänger verfolgt bzw. geöffnet werden sollen.
- Die Nachrichten sind manchmal (aber nicht immer!) in schlechtem Deutsch verfasst. Die Gründe dafür: Sie werden manchmal von Computerprogrammen aus anderen Sprachen automatisch übersetzt.
- Die E-Mails enthalten kyrillische Buchstaben oder falsch aufgelöste bzw. fehlende Umlaute (z.B. nur "a" statt "ä" bzw. "ae").

7. Was ist eine Firewall?

Eine Firewall ist ein Programm, das den Rechner vor Angriffen aus dem Internet schützt und auch verhindert, dass bestimmte Programme, zum Beispiel so genannte Spyware, Kontakt vom eigenen Rechner zum Internet aufnehmen. Dazu kontrolliert die Firewall alle Verbindungen in andere Netzwerke und überprüft sowohl die Anfragen ins Internet als auch die Daten, die zum Rechner kommen. Mehr Information zum Thema Firewall finden Sie hier http://www.bsi-fuer-buerger.de/infiziert/06_05.htm