

# Sicherheit am PC und im Internet

## Wie mache ich meinen PC sicher?

### Basis-Schutz

- Virenschutzprogramm und Anti-Spyware-Programm installieren und täglich aktualisieren
- Personal Firewall installieren und regelmäßig aktualisieren
- Sicherheitsupdates für Betriebssysteme und Software auf dem aktuellen Stand halten
- unterschiedliche Benutzerkonten einrichten
- Sorgfältiger Umgang mit Zugangsdaten: Kennwörter, Benutzername, Zugangscodes sicher aufbewahren
- Wechseln der Passwörter in regelmäßigen Abständen
- Vorsicht bei E-Mail Anhängen, im Zweifel beim Absender nachfragen, ob der Anhang tatsächlich von ihm stammt
- Downloads von Webseiten prüfen, ist die Quelle vertrauenswürdig
- Vorsicht bei Weitergabe von persönlichen Informationen
- Verschlüsselung der Kommunikation bei Voice over IP (VoIP), Wireless LAN (WLAN)
- Sicherungskopien der wichtigsten Dateien auf CD-ROM/DVD oder externe Festplatte

### Passwort

- sollte mindestens acht Zeichen lang sein
- sollte Sonderzeichen (?!%+...) und Ziffern enthalten
- Passwörter regelmäßig ändern
- Passwörter nicht notieren
- Keine einheitlichen Passwörter verwenden
- Voreingestellte Passwörter ändern
- Bildschirmschoner mit Kennwort sichern

### Datenverschlüsselung

- Schutz der Vertraulichkeit: Die Nachricht darf nur für den lesbar sein, für den sie bestimmt ist.
- Schutz der Authentizität: Die Echtheit des Absenders soll gewahrt sein. Ist der Absender wirklich die Person, die als Absender angegeben wird?
- Schutz der Integrität: Die Nachricht darf auf dem Weg vom Absender zum Empfänger nicht verändert werden.

### Schadprogramme

**Viren** oder **Würmern – Programmen** sind Programme, die sich selbständig verbreiten oder über E-Mails versandt werden und Schäden auf Ihrem PC anrichten können.

**Trojanischen Pferden** sind Programme, die vom Nutzer unbemerkt sicherheitskritische Funktionen durchführen, indem sie beispielsweise Passwörter abfangen.

### Schutz vor Schadprogramme:

- Virenschutzprogramm und Anti-Spyware-Programm installieren und täglich aktualisieren  
Personal Firewall installieren und regelmäßig aktualisieren
- Sicherheitsupdates für Betriebssysteme und Software auf dem aktuellen Stand halten  
unterschiedliche Benutzerkonten einrichten

### Phishing

Phishing werden Versuche genannt, an Daten eines Internet-Benutzers zu gelangen, z. B. über gefälschte WWW-Adressen, E-Mail oder Kurznachrichten.

### Schutz vor Phishing

- E-Mail-Programm: HTML-Darstellung und Java-Script deaktivieren
- Eigene E-Mails als reinen Text versenden
- E-Mail-Filter einiger Antivirenprogramme können gefälschte Phishing-E- erkennen und eliminieren.
- Antivirenprogramm muss auf aktuellem Stand sein
- E-Mail-Programme wie z. B. Mozilla Thunderbird und Browser wie der Internet Explorer 8, Mozilla Firefox 3.6 oder Opera 9.xx warnen vor Phishingseiten.

### Spam

Als Spam, Spamming oder Junk Mail sind

- Massenversand nichtangeforderter Werbe- E-Mails
- Werbebeiträge in Newsgroups, die nichts mit dem Thema der Newsgroup zu tun haben
- Kettenbriefe

### Schutz vor Spam

- Beteiligen Sie sich nicht an Internetgewinnspielen, Gratisproben und dererlei Unfug.
- Verwenden Sie die Spam-Filter Ihres Email-Providers
- Melden Sie Spam immer an Ihren Email-Provider.
- Deaktivieren Sie das Anzeigen von Grafiken.
- Setzen Sie Emailprogramme mit effektivem, selbstlernenden Spam-Filtern ein.
- Gehen Sie sorgfältig mit Ihrer privaten Emailadresse um.
- Legen Sie sich eine Zweit- oder Drittadresse bei einem der kostenlosen Emailprovider zu.
- Verschlüsseln Sie Emailadressen auf Ihrer Homepage.

## Kommunikation über das Internet

- **Chat**
- **Internettelefonie**
- **soziale Netzwerke**

## Schutz bei Internet-Kommunikation

- geben Sie keine persönlichen Daten an
- Erstellen Sie Profile mit größter Vorsicht
- Verwenden Sie keine persönlichen Bilder
- Nutzen Sie Pseudo-Namen
- Bewegen Sie sich im Netz möglichst anonym

## Pop-up-Fenster

Pop-up-Fenster (in der Regel einfach als Pop-ups bezeichnet) sind Fenster, die automatisch und ohne Ihre Zustimmung angezeigt werden.

Möglichkeiten Pop-ups zu blocken:

- Pop-ups wahlweise erlauben/blockieren auf Nachfrage
- Pop-ups generell blockieren

Vorsicht: Einige Websites, beispielsweise Homebanking-Seiten, verwenden Pop-ups für wichtige Funktionen. Durch das Blockieren aller Pop-ups werden diese Funktionen außer Kraft gesetzt.