Sicherheit und Datenschutz im Umgang mit dem PC

Beim Surfen

- Aktuelle Software, verwenden Sie ausschliesslich aktuelle Browserversionen.
- Zu viele Infos vermeiden
  In Formularen, verzichten Sie soweit möglich auf das Angeben von detaillierten persönlichen Daten. Erfassen Sie nur die absolut notwendigen Angaben für eine Transaktion.
- AGBs beachten
  Wenn dies nicht möglich ist, achten Sie auf die AGBs des Anbieters. Verpflichtet er sich keine Informationen an Dritte weiterzuleiten?
- Vor allem auf einem fremden Computer
  Verzichten Sie auf die persönliche Speicherung von Passwörtern in Ihrem Browser. Löschen Sie ggf. die temporären Cache-Dateien und die History-Liste in Ihrer Browser.
- Verschlüsselte Übertragung
  Bei Bezahlung per Kreditkarten kaufen Sie nur bei Anbietern, die eine sichere, verschlüsselte Übertragung wie. z. B. das SET- oder SSL-Verfahren anbieten.
- Gästebücher und Foren
  Beim Schreiben von Kommentaren in Gästebüchern oder Diskussionsforen müssen Sie grosse Vorsicht walten lassen. Bei Angabe Ihrer E-Mailadresse lassen sich oft noch nach Jahren Ihre privaten Interessen nachlesen. Verwenden Sie für solche Zwecke eine anonyme Zweitadresse.
- Chat und Newsgroups
  Seien Sie auch vorsichtig beim Chatten und bei der Teilnahme in Newsgroups.
- Bankgeschäfte
  Während Ihrer Tätigkeit bei Online-Bankgeschäften öffnen Sie keine weiteren Fenster mit anderen Inhalten. Beenden Sie Ihre Online-Bankgeschäfte immer mit der dafür vorgesehenen Beenden-Programmfunktion.
- Vorsicht bei Downloads
  Laden Sie Programme nur von vertrauenswürdigen Websites herunter. Also von offiziellen Hersteller-Websites und nicht irgendwelche Kopien von privaten oder dubiosen Websites.
- Zip und Co.
  Komprimierte Dateien sollten erst entpackt und auf Viren überprüft werden. Installierte Entpackungsprogramme sollten so konfiguriert sein, dass zu entpackende Dateien nicht automatisch gestartet werden.

Beim E-Mailen

- Virenscanner mit aktuellen Virensignaturen
  Setzen Sie einen Virenscanner ein und aktualisieren Sie das Programm regelmässig mit den neuen Signaturen. Aktualisieren Sie die Signaturen mindestens wöchentlich, besser täglich.
- Attachments
  Prüfen Sie auch, ob Ihr Virenscanner E-Mails und die darin enthaltenen Anhänge automatisch auf Viren überprüft.
- Firewall
  Setzen Sie unbedingt einen Firewall ein, der den Datenverkehr Ihres Rechners überprüft. (Es gibt auch kostenlose Firewalls für Privatpersonen)
- Vorsicht bei Datei-Anhängseln
  Öffnen Sie keine E-Mails aus unbekannter Herkunft oder mit nicht erwarteten Anhängen. Öffnen Sie keine Witz-Dateien, Videos und EXE-Dateien unbekannter Herkunft.
- Privat und Geschäft trennen
  Verwenden Sie für Ihre privaten E-Mails niemals Ihre Geschäftsadresse. Besorgen Sie sich bei einem E-Mailanbieter eine private E-Mailadresse.
- Zweitadresse verwenden
  Nehmen Sie öfters an Gewinnspielen teil? Inserieren Sie in Kleinanzeigen? Beteiligen Sie sich am Usenet? Abonnieren Sie Mailinglisten? Die eingereichten E-Mailadressen werden des öfteren für Spam zweckentfremdet. Besorgen Sie sich für solche Fälle eine kostenlose E-Mailadresse bei einem der zahllosen Anbieter.

- Carbon Copy vermeiden, Blind Carbon Copy verwenden
  Beim Versenden von der gleichen E-Mail an mehrere Personen verwenden Sie nicht den Befehl "CC", sondern den Befehl BCC.
- Kill den Spam
  Löschen Sie Spam (Werbemüll) sofort ohne zu öffnen.
- Ausnahmsweise nicht antworten
  Senden Sie Spam nicht mit dem Vermerk "Remove" retour. Die Spammer wissen damit nur, dass Sie die E-Mails auch wirklich lesen.
- PC verseucht?
  Überprüfen Sie regelmässig, ob E-Mails im Ausgangs-Postkorb stehen, die nicht vom Ihnen selbst verfasst wurden.
- E-Mails und Adressen schützen
  Schützen Sie Ihr E-Mailprogramm mit einem Passwort.
- Verschlüsselungssoftware verwenden
  Setzen Sie gegebenenfalls für Ihre E-Mails Verschlüsselungsverfahren wie z. B. PGP ein oder verschlüsseln Sie die Daten mit Steganografie-Software.

Allgemein

Falls Ihr PC auch für andere Personen zugänglich ist:

- Papierkorb leeren
  Leeren Sie öfters den Papierkorb (ja, den elektronischen)
- Browsercache leeren
  Löschen Sie regelmässig den Cache Ihres Browsers.
- History entfernen
  Löschen Sie regelmässig den Verlauf Ihrer Surftouren im Browser.
- Bildschirmschoner auch mit Passwort versehen
  Hinterlegen Sie den Bildschirmschoner mit einem Passwort.
- Passworte überall
  Sichern Sie wichtige, persönliche Dateien mit einem Passwort.
- Komplizierte Passwörter nutzen
  Verwenden Sie keine einfach verifizierbaren Passwörter. Verwenden Sie lange, völlig willkürliche Passwörter und schreiben Sie diese auf. Hüten Sie diese Passwortliste wie Bargeld.
- Bekannte Verstecke meiden
  Hinterlegen Sie die Passwörter nicht unter der Tastatur oder am Bildschirm.
- Austausch der Passworte
  Wechseln Sie Ihre Passwörter regelmässig.
- Datensicherung nicht vergessen
  Sichern Sie regelmässig Ihre Daten auf einem zweiten Datenträger. Lagern Sie einen zweiten Satz des Datenträgers ausserhalb Ihrer Liegenschaft.
- Gefahr Laptops
  Lassen Sie Ihren Laptop nie aus den Augen. Speichern Sie im Laptop keine Passwörter. Vermeiden Sie soweit möglich vertrauliche Daten. Verwenden Sie diverse Passwörter.
- Dateiendungen beachten
  Stellen Sie den Windows Explorer so ein, dass alle Dateitypen sichtbar sind.
- Vertrauen ist gut, Kontrolle ist besser
  Scannen Sie jede Diskette, CD-ROM, ZIP-Laufwerke etc. vor der ersten Nutzung auf Viren.
- Warnmeldungen nicht ignorieren
  Aktivieren Sie den Makro-Virenschutz von Anwendungsprogrammen und beachten Sie die allfälligen Warnmeldungen, auch wenn diese oftmals sehr lästig erscheinen.
- Passwörter ändern
  Ändern Sie nach der Installation von Hardware-Komponenten wie z. B. Routern und Netzwerk-Servern und Hubs deren Passwörter, um den Einstellungsdialog zu schützen.
- Schlupflöcher vermeiden
  Löschen Sie alle unnötigen Standardfreigaben, und installieren Sie keine Internet- oder Netzwerkdienste, die Sie nicht unbedingt brauchen.