



BÜRGERCERT
Ins Internet - mit Sicherheit

Wer braucht welchen Schutz?

Weitere Texte finden Sie unter www.buerger-cert.de.

Wer braucht welchen Schutz?

Wieviel Aufwand Sie zum Schutz Ihres PCs - und somit natürlich auch zum Schutz Ihrer Privatsphäre - betreiben müssen, hängt in erster Linie von Ihren persönlichen Anforderungen ab. Es gibt jedoch Schutzmaßnahmen, die Sie in jedem Fall treffen sollten.

Die nachfolgende Auflistung zeigt Ihnen, welche Vorkehrungen Sie immer treffen sollten, egal welche Dienste Sie nutzen:

Fünf „Goldenen Regeln“ die Sie stets beachten sollten...

1. Installieren Sie ein **Virenschutzprogramm** und halten Sie dieses immer auf dem aktuellen Stand.
2. Setzen Sie eine **Personal Firewall** ein und aktualisieren Sie diese regelmäßig.
3. Achten Sie darauf, ob es **Sicherheitsupdates** für Ihr Betriebssystem und sonstige von Ihnen installierte Software gibt und führen Sie diese durch.
4. Arbeiten Sie nach Möglichkeit nicht als Administrator an Ihrem PC, denn so können Schadprogramme noch mehr Unheil anrichten. Richten Sie für alle Nutzer eines PCs **unterschiedliche Benutzerkonten** ein. Vergeben Sie für diese Konten nur die Berechtigungen, die der jeweilige Nutzer für seine Arbeit auch braucht. So werden auch private Dateien vor dem Zugriff Anderer geschützt.
5. Gehen Sie sorgfältig mit Ihren **Zugangsdaten** um: Halten Sie Kennwörter und Benutzernamen sowie Zugangscodes für Dienste (z.B. beim Online-Banking) unter Verschluss.

Zusätzlich zu den fünf „Goldenen Regeln“ sollten Sie bei der Nutzung bestimmter Dienste folgende Schutzmaßnahmen beachten:

PC-Nutzung	Empfohlene Schutzmaßnahme	Weitere Information unter
Text- und Datenverarbeitung	Führen Sie eine regelmäßige Datensicherung durch	http://www.bsi-fuer-buerger.de/daten/index.htm
E-Mail	<ul style="list-style-type: none"> - Benutzen Sie einen Spamschutz - Versenden, empfangen oder lesen Sie keine E-Mails im HTML-Format - Deaktivieren Sie die Autovorschau Ihres E-mail-Programms - Seien Sie vorsichtig beim Öffnen von E-Mails unbekannter Absender und klicken Sie niemals auf Links in diesen E-Mails 	http://www.bsi-fuer-buerger.de/schuetzen/index.htm
Surfen	<ul style="list-style-type: none"> - Verzichten Sie wenn möglich auf alle Aktiven Inhalte - Leeren Sie nach jeder Sitzung den Browser-Cache - Löschen Sie nach jeder Sitzung die gespeicherten Cookies 	http://www.bsi-fuer-buerger.de/browser/index.htm
Online-Banking	<ul style="list-style-type: none"> - Achten Sie auf eine verschlüsselte Kommunikation mit dem Bankenserver (SSL-Verbindung / HTTPS) - Gehen Sie sorgfältig mit Ihrer PIN und den TANs um 	http://www.bsi-fuer-buerger.de/geld/index.htm

E-Commerce/ E-Government	<ul style="list-style-type: none"> - Achten Sie auf eine verschlüsselte Kommunikation bei der Übermittlung sensibler Daten (SSL-Verbindung / HTTPS) - Gehen Sie sorgfältig mit den sensiblen Daten um (z.B. Kreditkartendaten) 	http://www.bsi-fuer-buerger.de/staat/index.htm http://www.bsi-fuer-buerger.de/einkaufen/index.htm
Online-Spiele	<p>Nach Möglichkeit sollte zum Spielen kein PC benutzt werden, auf dem sensible Daten gespeichert sind</p>	http://www.bsi-fuer-buerger.de/computerspiele/index.htm
WLAN	<p>Ändern Sie die Standardeinstellungen Ihrer WLAN-Komponenten:</p> <ul style="list-style-type: none"> - Aktivieren Sie die WLAN-Verschlüsselungsmechanismen (mindestens WPA / WPA2, nicht WEP) - Aktivieren Sie Ihre WLAN-Komponenten nur, wenn Sie sie wirklich brauchen. Ist Ihr PC ausgeschaltet, dann kann auch der Access Point ausgeschaltet werden - Aktivieren Sie wenn möglich einen MAC-Adress-Filter 	http://www.bsi-fuer-buerger.de/wlan/index.htm
VoIP	<ul style="list-style-type: none"> - Verschlüsseln Sie die Kommunikation, damit ein Abhören des Gesprächs erschwert wird 	http://www.bsi-fuer-buerger.de/intern_telefon/index.htm
Nutzung durch Kinder	<ul style="list-style-type: none"> - Vergeben Sie nur die notwendigen Rechte - Setzen Sie eine Kinderschutz-Software ein 	http://www.bsi-fuer-buerger.de/kinder/index.htm