Schützen Sie sich gegen Angriffe aus dem Internet!

Diese Punkte sollte jeder beherzigen, im Privaten wie im Geschäftlichen.

1. Installieren Sie regelmäßig **Sicherheitsupdates** für Ihr Betriebssystem und Ihre Anwender- und Schutz-Programme.
2. Nutzen Sie auf jedem Rechner ein **Virenschutzprogramm** mit einer **Personal Firewall** und lassen Sie **hereinkommende E-Mails** damit automatisch prüfen.
3. Benutzen Sie ein **Benutzerkonto**, das **mit einem Passwort** geschützt ist, um auf Ihrem Rechner zu arbeiten. Nutzen Sie keinesfalls dafür das Administrator-Konto.
4. **Persönliche Verhaltensweisen** sind entscheidend, damit Schadsoftware draußen bleibt:
   - Seien Sie misstrauisch.
   - Klicken Sie nicht automatisch auf jeden Link im Internet, bloß weil er Ihre Neugierde weckt.
   - Möchten Sie Software herunterladen, so tun Sie das ausschließlich von der Webseite des Herstellers.
   - Machen Sie einen **3 Sekunden Check** vor dem Öffnen einer jeden E-Mail:
     - Ist der Absender bekannt?
     - Ist der Betreff sinnvoll?
     - Wird ein Anhang von diesem Absender erwartet?

       Ansonsten löschen Sie die E-Mail gnadenlos ungelesen.
5. Verwenden Sie **Internet-Browser mit Sicherheitsmechanismen** wie etwa einer Sandbox und schalten Sie den vorhandenen **Filtermechanismus** ein, der Sie vor schädlichen Webseiten warnt, bevor Sie diese aufrufen.
6. **Nutzen Sie Passwörter!** Nutzen Sie für jeden Online-Dienst wie E-Mail, Online Shops, Online Banking, Foren, Soziale Netzwerke ein anderes, sicheres Passwort.
7. Die **Übertragung persönlicher Daten** beim Online Banking, Online Shopping sollte ausschließlich über eine verschlüsselte Verbindung geschehen. Sie erkennen dies an der von Ihnen aufgerufenen Internetadresse, dass sie stets mit "**https://**" beginnt und ein kleines **Schloss-Symbol** in Ihrem Browserfenster zeigt.
8. Versenden und empfangen Sie **E-Mails** über eine **gesicherte Verbindung (SSL/TLS)**.
9. Erstellen Sie **regelmäßig Sicherheitskopien - "Backups" -** Ihrer Daten, um vor Verlust geschützt zu sein – speichern Sie die Daten bspw. auf eine externe Festplatte.
10. Nutzen Sie ein **WLAN** (Wireless LAN, also drahtloses Netzwerk)? Dann sollte dieses stets mittels des Verschlüsselungsstandards **WPA2** verschlüsselt sein.
11. Bedenken Sie, dass **Schadsoftware** auf Ihren Rechner übertragen werden kann, wenn Sie Ihr **Mobilgerät, einen USB-Stick** o.ä. anschließen und Dateien herunterladen.
12. Beachten Sie, dass über **Hot Spots** andere Geräte und Nutzer des offenen WLAN-Netzes ggf. Zugriff auf Ihr Gerät haben!

Weitere Informationen: https://www.bsi-fuer-buerger.de