SICHERHEIT IM INTERNET

Schutz vor Gefahren (Tipps des Bundeskriminalamtes)

Schützen Sie Ihren eigenen Computer durch ein Anti-Viren-Programm und eine Firewall und führen Sie regelmäßige Updates aus. *(Anmerkung von SiNR: Das Betriebssystem Windows hat dies integriert)*.

Verwenden Sie sichere Passwörter. *(Anmerkung von SiNR: Sie sollten mindestens 8 Zeichen lang sein, aus Groß- und Kleinbuchstaben sowie Zahlen/Sonderzeichen bestehen und in keinem Wörterbuch zu finden sein oder mit Ihnen in Verbindung stehen)*.

Öffnen Sie nur E-Mails und Dateien, die von vertrauenswürdigen Absendern stammen. Vorsicht bei verdächtigen E-Mails, die angeblich von Kreditinstituten, Behörden, Notaren u.a. kommen und vertrauliche Daten anfordern.

Installieren Sie Programme (Apps) nur über offizielle App-Shops. Achten Sie darauf, ob und welche Software oder Zusatzprogramme („Plug-Ins“) Sie zusätzlich ungewollt installieren sollen *(Anmerkung von SiNR: Häkchensetzung genau prüfen*) oder ohne Ihr Wissen Bestellungen oder Abo-Verträge abschließen *(Anmerkung von SiNR: Besondere Aufmerksamkeit und Vorsicht ist geboten, wenn Sie nachpersönlichen Daten, Zahlungsarten und Bankverbindungen gefragt werden!).*

Wenn Sie im Internet mit Unbekannten Daten tauschen, riskieren Sie einen Virenbefall Ihres PC, die Installation von Schadprogrammen und machen sich u.U. zudem strafbar!

Achten Sie bei Online-Shops darauf, dass ein Impressum mit Nennung und Anschrift der Firma oder des Geschäftsführers, ein Zertifikat oder Siegel, sowie klare Geschäfts-bedingungen vorhanden sind *(Anmerkung von SiNR: Diese sollten auf der Internetseite möglichst durch 1 Klick erreichbar sein)*. Informationen dazu bieten Konsumenten-schutzorganisationen, wie z.B. www.europakonsument.at.

Die Bezahlung mit Konto- oder Kreditkartendaten im Web sollte immer über eine verschlüsselte Verbindung übertragen werden. Diese erkennen Sie an den Buchstaben „https“ in der Adresszeile der Webseite und einem Schloss- oder Schlüssel-Symbol im Internet-Browser.

Geben Sie beim Online-Banking die offizielle Adresse der Bank direkt ein. Die Verbindung sollte ebenfalls als verschlüsselt erkennbar sein. Vorsicht gilt, wenn bei Überweisungen mehrere TANs (Transaktionsnummern) abgefragt werden: Dann ist Phishing, eine Art Datendiebstahl, im Spiel. Im Zweifelsfall sollten Sie sofort Ihr Bankinstitut kontaktieren.