Allgemeine Sicherheits-Tipps für den Umgang mit dem Internet

- **Installieren Sie ein gutes Antiviren-Programm und achten Sie auf eine regelmäßige Aktualisierung dieses Programms**
- **Achten Sie auf eine stets aktualisierte „Firewall“ (= „Brandschutzmauer“, ein Programm, welches den Zugriff von außen auf Ihren PC verhindern kann)**
- **Verwenden Sie Passwörter mit mindestens 6-8 Zeichen, bestenfalls mit Klein-und Großbuchstaben, kombiniert mit Zahlen und Sonderzeichen (z.B.: ? oder ! oder §). Geben Sie niemals Ihre Passwörter an Dritte weiter und speichern Sie NIE Ihre Passwörter auf dem PC.**
- **Machen Sie regelmäßig Datensicherungen von den für Sie wichtigen und auf Ihrem PC gespeicherten Daten (z.B. Briefe, Fotos, Videos, Rechnungen usw.) – auf externe Speichermedien wie CD/DVD, externe Festplatten, USB-Sticks, SD-Speicherkarten usw.**
- **Niemals PINs und TANs (Online-Banking) auf dem Computer speichern.**
- **Überprüfen Sie regelmäßig, ob Updates (Neuerungen/Fehlerbehebungen) für Ihr Betriebssystem (z.B. Windows 7, Windows 8 usw.) vorliegen. Wenn ja: installieren Sie diese Updates auch regelmäßig.**
- **Versenden Sie niemals Persönliches wie Kontonummern usw. an fremde Personen per Email.**
- **Zahlen Sie keine Rechnungen, die Sie per Email bekommen haben und von denen Sie wissen, dass Sie die Ware nie bestellt oder Dienstleistungen nie in Anspruch genommen haben. Dies gilt auch für Rechnungen von „Rechtsanwälten“, „Steuerbüros“, Online-Versandhäuser usw.**
- **Öffnen Sie niemals Email-Anhänge von Absendern, die Sie nicht kennen. Löschen Sie die Email am besten sofort.**
- **Besuchen Sie keine „dubiosen“ Seiten! Gute Antiviren-Programme warnen vor dem Besuch einer solchen Seite, wenn diese als potentiell gefährlich eingestuft wird.**

- **Seien Sie misstrauisch, wenn Sie „Strafe“ zahlen sollen, weil Sie angeblich etwas „Verbotenes“ getan haben. Hier sind Betrüger am Werke, die Ihnen vorgaukeln, sie wären eine offizielle Behörde (z.B. GEZ, Bundeskriminalamt usw.) und würden vorübergehend Ihren PC sperren. Bezahlen Sie auf keinen Fall, denn Ihr PC ist jetzt bereits mit einem Trojaner infiziert und wird garantiert auch nicht mehr „freigegeben“. Hier kann nur ein PC-Fachmann helfen, den Trojaner wieder zu entfernen. Schlimmstenfalls muss das Betriebssystem neu aufgesetzt werden – gut, wenn Sie nun Ihre Daten regelmäßig gesichert haben.**
- **Ihre Hausbank (Sparkasse, sonstiges Kreditinstitut) wird Sie nie per Email bitten, Ihre Bankdaten zu bestätigen, indem Sie auf einen LINK klicken und dann Ihre Kontodaten erneut eingeben. Ignorieren Sie diese Email und rufen Sie im Zweifelsfalle Ihre Bank an!**
- **Bitte bedenken Sie auch: Neben den Hacker- und Virenangriffen gibt es noch viel, viel mehr Straftaten im Internet: Kinderpornographie z.B., oder gefälschte Tickets für eine Veranstaltung, „Punktekauf“ der Verkehrssünderkartei in Flensburg -um nur ein paar solcher Straftaten zu nennen. Seien Sie wachsam und aufmerksam. Melden Sie umgehend der nächsten Polizeidienststelle, wenn Sie auf eine verdächtige Internetseite gestoßen sind oder wenn Ihnen sonst etwas Verdächtiges auffällt.**

Das Internet ist eine feine Sache – kaum jemand ist heute mehr „ohne“. Lassen Sie sich keinesfalls die Freude am „Surfen“ und „Emailen“ oder „Skypen“ nehmen – aber bleiben Sie aufmerksam.

Trotz all dieser o.g. Sicherheitsvorkehrungen gilt: Einen 100 %-igen Schutz vor Viren, Trojanern oder anderen Bosheiten gibt es leider nicht – es kann JEDEN treffen.