

Tipps zum Schutz vor Internet-Kriminalität

Schützen Sie Ihren PC zur Nutzung des Internets mit einem guten Virenprogramm und einer Firewall und installieren Sie regelmäßig Updates um den Schutz aktuell zu halten.

E-Mails und Chat

Öffnen Sie nur E-Mails, die von vertrauenswürdigen Ab-sendern stammen. Dubiose Mails von Unbekannten möglichst sofort löschen. Vorsicht bei E-Mails von Kreditinstituten: Banken bitten Kunden nie per Mail, vertrauliche Daten im Netz einzugeben.

Online-Shopping

Seien Sie misstrauisch, wenn die Angebote unrealistisch günstig sind. Googeln Sie den Anbieter, ob es Hinweise auf Betrugshandlungen gibt. Opfer stellen Betrüger oft ins Netz. Prüfen Sie die Seriosität des Anbieters aufgrund von Bewertungen oder durch Suchanfragen, ob es dessen Niederlassung tatsächlich in einem Branchentelefonbuch gibt. Weiterführende Informationen sowie „nicht zu empfehlende Webseiten“ bieten die verschiedenen nationalen und internationalen Konsumentenschutzorganisationen (www.europakonsument.at) an.

Online-Banking

Achten Sie immer auf die Web-Adresse, ob sie mit „https://“ beginnt und somit eine „sichere“ Seite darstellt. Geben Sie beim Einstieg in Ihr Bankkonto beim Tele-banking zuerst falsche Daten ein. Es muss sofort eine Fehlermeldung kommen. Wenn nicht, ist die Seite sehr wahrscheinlich zum Ausspionieren Ihrer Daten manipuliert. Vorsicht gilt, falls mehrere Transaktionsnummern auf einmal abgefragt werden: Dann ist Phishing im Spiel. Phishing ist eine Art von Diebstahl persönlicher Daten über das Internet.

Private Infos, Fotos und Passwörter

Gehen Sie vorsichtig mit Ihrer Privatsphäre um. Dies gilt besonders im Umgang mit privaten Fotos und persönlichen Daten, wie z.B. Telefonnummern oder Wohnadressen. Einmal veröffentlicht, können Fotos negative Auswirkung, z.B. in Form von Mobbing, Erpressung, sexueller

Missbrauch auf das weitere Leben haben. Auch im Web haben es die Nutzer in der Hand, den Zugang zu privaten Infos zu beschränken. Nur gute Bekannte sollten in entsprechenden Foren und Communitys Zugriff auf Fotos oder Kontaktdaten erhalten. Speichern Sie weiters keine Passwörter (PIN, TAN...) auf dem PC. Mitarbeiter von Banken werden Sie nie nach Zugangsdaten fragen. An-fragen per Mail kommen in der Regel ausschließlich von Betrügern.

Neffentricks (Erbschaften, Geldbedarf für Heimreisen etc.)

Wenn Sie Zuschriften erhalten, dass Sie einen großen Geldbetrag erben, ist es eine Lüge. Die Aufforderung Spesen zu bezahlen, damit die Erbschaft ausgezahlt werden

kann, ist Betrug. Teilen Sie mit, dass Sie mittellos sind und nichts bezahlen können, der Erblasser aber als Spesenersatz 50 % von der Erbschaft behalten kann. Sie werden nichts mehr von den Betrügern hören. Wenn doch: Die Zuschriften einfach löschen und ignorieren. Bekannte im Ausland in Geldnöten werden oft vorgetäuscht. Helfen Sie nur, wenn Sie mit Ihrem Bekannten persönlich reden können oder auf andere vertrauenswürdige Quellen zugreifen können.