SCHUTZ VOR IT-KRIMINALITÄT

Sicher im Netz – 10 Tipps wie Sie sich vor Gefahren schützen können

1. Schutz des PC

An oberster Stelle steht eine gute Sicherheitsausstattung für Ihren Computer. Um den PC vor schädlichen Dateien zu schützen, sollten vor der ersten Nutzung des Internets ein Anti-Viren-Programm und eine Firewall installiert werden. Für diese Schutzprogramme, das Betriebssystem und den Internet-Browser werden regelmäßig von den Herstellern Aktualisierungen, so genannte Updates, angeboten, die auch automatisiert abgerufen werden können. Es wird empfohlen diese Updates umgehend zu installieren. Das gilt auch für auf dem PC installierte Anwendungsprogramme. Da Schadsoftware zunehmend über externe Datenträger wie CDs oder USB-Sticks verbreitet wird, sollten diese vor der Nutzung auf Viren geprüft werden.

2. E-Mails und Chat

Öffnen Sie nur E-Mails, die von vertrauenswürdigen Absendern stammen. Dubiose Mails von Unbekannten möglichst sofort löschen. Schadprogramme verbergen sich oft in Grafiken oder E-Mail-Anhängen. Verdächtige Dateien sollten Sie auf keinen Fall öffnen! Vorsicht auch vor angeblichen E-Mails von Kreditinstituten: Banken bitten Kunden nie per Mail, vertrauliche Daten im Netz einzugeben. Auch in Communitys empfangene E-Mail-Anhänge sollten mit einem Schutzprogramm überprüft werden. Riskant können auch Chat-Nachrichten von Unbekannten sein: Kriminelle versenden oft Links zu Webseiten mit Viren. Das Aufrufen dieser Seiten installiert Ihnen möglicherweise bereits eine Schadsoftware (Malware).

3. Software

Achten Sie darauf, welche Software oder Zusatzprogramme („Plug-Ins“) Sie installieren. Eine Gefahr sind Schadprogramme, die in Gratis-Downloads oder Raubkopien von dubiosen Anbietern versteckt sind. Gesundes Misstrauen hilft: Wenn Zweifel an der Seriosität bestehen, besser auf Download und Installation einer Software verzichten.

4. Tauschbörsen

Wer im Internet mit Unbekannten Dateien tauscht, riskiert eine Infektion seines PCs mit Schadprogrammen. Zudem ist der Tausch von urheberrechtlich geschützten Musik-, Film-

oder Software-Kopien strafbar und kann gegebenenfalls neben Geld- und Freiheitsstrafen zu Schadenersatzansprüchen der Rechteinhaber führen.

5. Online-Shopping

Zeichen für die Seriosität eines Online-Shops sind ein Impressum mit Nennung und Anschrift der Firma, des Geschäftsführers oder einer Umsatzsteuer-Identifikationsnummer (UID-Nummer) sowie klare Geschäftsbedingungen (AGB). Kunden sollten auch die Datenschutzerklärung lesen. Manche Shops werden von unabhängigen Experten geprüft und erhalten ein Zertifikat oder Siegel. Auch der Kunde kann Kontrolle ausüben: Auf vielen Shopping-, Preisvergleich- und Auktionsseiten werden Händler beurteilt. Gute Bewertungen können ein Hinweis auf seriöse Geschäftspraktiken sein. In jedem Fall ist jedoch eine Portion gesundes Misstrauen angebracht – vor allem auf Webseiten mit Angeboten weit unter dem tatsächlichen Wert. Weiterführende Informationen sowie „nicht zu empfehlende Webseiten“ bieten die verschiedenen nationalen und internationalen Konsumentenschutzorganisationen (www.europakonsument.at).

6. Bezahlung im Web

Beim Kauf von Waren im Internet ist allgemein Vorsicht geboten, insbesondere bei Vorauszahlung. Zur Bezahlung sollten Konto- oder Kreditkartendaten über eine verschlüsselte Verbindung übertragen werden, erkennbar an den Buchstaben „https“ in der Adresszeile der Webseite und einem Schloss- oder Schlüssel-Symbol im Internet-Browser. Sichere Webseiten sind auch an einer grün hinterlegten Adresszeile oder an einem grün hinterlegten Zertifikatszeichen erkennbar, wenn sich der Betreiber einer unabhängigen Prüfung unterzogen hat. Zahlungen können per Lastschrift, Kreditkarte oder Rechnung erfolgen. Es gibt auch seriöse Bezahl-Dienste, bei denen die Bankdaten einmalig hinterlegt werden. Vorkasse per Überweisung ist zwar weit verbreitet, gilt aber generell als sehr viel riskanter.

7. Online-Banking

Beim Online-Banking sollte man die offizielle Adresse der Bank immer direkt eingeben oder über eigene Lesezeichen, so genannte Favoriten, aufrufen. Maßgeblich ist die Adresse, die die Bank in ihren offiziellen Unterlagen angibt. Die Verbindung zum Bankcomputer muss wie bei Bezahlvorgängen verschlüsselt sein (erkennbar an den Buchstaben „https“ in der Adresse der Webseite). Für Überweisungen und andere Kundenaufträge sind

Transaktionsnummern (TANs) nötig. In den Anfängen des Online-Bankings konnten die Nutzer einen solchen Code aus einer Liste frei wählen. Sicherer ist das iTAN-Verfahren, bei dem die Codes nummeriert sind. Ein Zufallsgenerator der Bank bestimmt, welche TAN eingegeben werden muss. Noch weniger Chancen haben Kriminelle beim mTAN-Verfahren: Die TAN wird dem Kunden aufs Handy geschickt und ist nur kurzzeitig gültig. Weitere Schutzverfahren sind eTAN und HBCI, bei denen der Kunde als Zusatzgeräte einen TAN-Generator oder ein Kartenlesegerät nutzt. PC-Nutzer sollten Ihre Bank fragen und das modernste verfügbare Verfahren wählen.
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. Über E-Mails oder betrügerische Webseiten wird versucht, persönliche Daten oder Informationen wie Kreditkartennummern, Kennwörter, Kontodaten usw. abzufragen.
In diesem Fall informieren Sie bitte sofort Ihr Bankinstitut.

8. Private Infos und Passwörter

Die meisten Menschen würden im Alltag kaum Unbekannten ihr Privatleben offenbaren. 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. Je weniger von der eigenen Privatsphäre frei zugänglich ist, desto weniger Angriffsfläche wird potenziellen Tätern und anderen unbefugten Nutzern geboten. Seien Sie bei der Weitergabe Ihrer E-Mailadresse oder bei der Eintragung Ihrer Daten in Internetformulare vorsichtig. Gehen Sie immer davon aus, dass Ihre Daten weitergegeben und missbraucht werden können.
Bei vielen Online-Services müssen sich die Nutzer registrieren. Meist werden Benutzername und Passwort festgelegt. Soweit möglich, verwenden Sie nicht das gleiche Passwort für mehrere Dienste – etwa E-Mail-Konto, Online-Shops und Communitys. Je länger ein Passwort, desto schwerer ist es zu knacken. Es sollte mindestens acht Zeichen lang sein und aus einer zufälligen Reihenfolge von Groß- und Kleinbuchstaben, Zahlen und Sonderzeichen bestehen. Ein solches könnte leicht erstellt werden, indem sich der Benutzer einen Satz überlegt und von jedem Wort den ersten Buchstaben sowie alle Zahlen und Sonderzeichen verwendet. (zum Beispiel der Satz: „Ich bin am 1. Jänner 1970 geboren.“ ergäbe das Passwort: Iba1.J1970g.)
Wer sich die zahlreichen Codes schwer merken kann, dem helfen so genannte Passwort-Safes. Das sind PC-Programme, mit denen sich Geheimzahlen sicher speichern lassen. Der Anwender braucht sich dann nur noch ein Haupt-Passwort zu merken.

Speichern Sie weiters keine Passwörter (PIN, TAN…) auf dem PC. Mitarbeiter von Banken werden Sie nie nach Zugangsdaten fragen. Anfragen per Mail kommen in der Regel ausschließlich von Betrügern.

9. Angebote als Waren- oder Finanzagenten

Angebote im Internet oder per E-Mail als Waren- oder Geldvermittler zu arbeiten, sind konsequent abzulehnen. Der Vermittler dient den Tätern zur Verschleierung ihrer Identität. Web-Nutzer, die sich auf dubiose Angebote einlassen und Waren oder Gelder weiterleiten, betreiben Beihilfe zum Betrug oder der Geldwäsche und müssen mit strafrechtlichen Folgen und Schadenersatzansprüchen rechnen.

10. Apps und Abofallen

Seien Sie sich bewusst, dass Apps Kosten verursachen sowie sensible Nutzerdaten übertragen können. Dies kann oftmals passieren ohne dass diese für die Funktion der Apps notwendig sind. Installieren Sie daher nur Apps über die offiziellen App-Shops, da diese überprüft bzw. bei Problemen mittels Fernlöschung von Ihrem Handy entfernt werden. Seien Sie besonders bei kostenlosen Apps vorsichtig.
Achtung geboten ist zudem bei Online-Diensten bei denen eine Registrierung erforderlich ist. Neben der breiten Masse der seriösen Werbeangebote gibt es auch Fallen, bei denen versteckt Bestellungen oder Abo-Verträge abgeschlossen werden. Die Nutzer werden dabei nicht ausreichend über die Vertragsbedingungen und Preise informiert. Oft wird dies erst im Nachhinein bemerkt, wenn Rechnungen bzw. Inkassoschreiben eingehen.
Hilfestellung hierbei bietet einerseits die Watchlist des Internetombudsmannes, andererseits fungiert dieser auch als außergerichtliche Schlichtungsstelle in Streitfragen. Im Internet zu finden unter www.ombudsmann.at

Bitte beachten Sie: Der verantwortungsvolle Umgang bei der Benutzung des Internets liegt bei Ihnen!

Verdächtige Sachverhalte im Internet melden Sie bitte an die Internetmeldestelle im Bundeskriminalamt

against-cybercrime@bmi.gv.at