ZIVILSCHUTZ
Burgenland

Internet-Sicherheit

SIZ
SICHERHEITS
INFORMATIONSZENTRUM
Burgenland

www.bzsv.at

Inhaltsverzeichnis/Impressum

Inhaltsverzeichnis/Impressum	2
Liebe Leserinnen und Leser!	3
Die Gefahren/Risiken im Überblick	4
Risiken bei der Internetnutzung	5-6
Allgemeine Regeln	7
Zehn grundlegende Tipps	8-9
Passwörter	10-11
Online Banking	12
Phishing Mails	13
Soziale Netzwerke - Das Ich im Netz	14-15
Cybermobbing	16-17
Malware	18-20
Onlineshopping	21-22
Smartphones	23-24
Datenschutz & Urheberrecht	25
Sexting	26
Digitaler Nachlass	27
Für Eltern	28
Der Vertrag im Internet	29
Wie sicher ist mein Computer?	30-31
Der Burgenländische Zivilschutzverband	32

Impressum:
Medieninhaber, Herausgeber, Eigentümer, für den Inhalt verantwortlich und Layout:
Österreichischer Zivilschutzverband – Landesverband Burgenland, 7000 Eisenstadt

Herrsteller: Rötzer Druck Gesellschaft mbH, 7000 Eisenstadt
Verlagsort: Eisenstadt Herstellungsort: Eisenstadt

Aus Gründen der besseren Lesbarkeit wird größtenteils auf die gleichzeitige Verwendung männlicher und weiblicher Sprachformen verzichtet. Sämtliche Personenbezeichnungen gelten gleichwohl für beiderlei Geschlecht.

Haftungsausschluss:
Obwohl wir uns um Aktualität, Vollständigkeit und Richtigkeit der Inhalte bemühten, können wir hierfür keine Garantie und Haftung übernehmen. Zudem schließt der BZSV die Haftung für angegebene Websites aus.

Stand: 2016 Fotos: Fotolia bzw. zur Verfügung gestellt

SIZ
SICHERHEITS INFORMATIONSZENTRUM Burgenland

Liebe Leserinnen und Leser!

Computer und Internet sind aus unserem Alltagsleben nicht mehr wegzudenken. Zahlreiche technische Möglichkeiten erleichtern uns das Leben, machen es komfortabler und helfen Zeit zu sparen, um uns mit wichtigen Dingen des Lebens zu beschäftigen. Viele Entwicklungen sind erst durch Internet, WWW, Computer oder Datenverarbeitung möglich geworden.

Doch wo Licht ist, ist auch Schatten. Immer wieder hören wir Schlagworte wie Hacking, Computerkriminalität oder Betrug mit Hilfe von Sozialen Netzwerken. Das Risiko, Opfer von Internetbetrügern zu werden, ist ohne entsprechende Sicherheitsmaßnahmen ein hohes. Online Security ist daher ein Gebot der Stunde. Eine weitere Gefahr für Kinder und Jugendliche stellt die Internetsucht dar. Das Anton Proksch-Institut schätzt, dass ca. 80.000 Jugendliche internetsüchtig sind. Aber auch Erwachsene laufen oftmals Gefahr, Opfer von Internetbetrügern zu werden.

Mit der vorliegenden Broschüre möchte der Burgenländische Zivilschutzverband auf das Problem aufmerksam machen und gute Tipps und Tricks verraten, wie man mit dem Internet oder dem World Wide Web „richtig" umgeht. Durch das Vermeiden von Fehlern und einfachen Maßnahmen wie das Erstellen von relativ „sicheren" Passwörtern soll es Kriminellen schwer gemacht werden, Betrugsopfer zu finden.

Der BZSV will dabei helfen, das Internet mit seinen vielen sinnvollen und guten Errungenschaften zu nutzen und Tipps zur sicheren Anwendung geben, um in keine „Fallen" zu tappen.

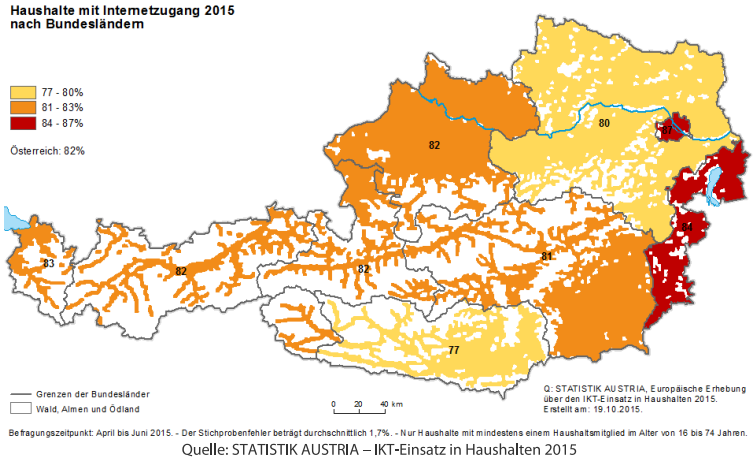
Erwin Preiner

NR Bgm. Erwin Preiner
BZSV-Präsident

Fakten zur Internetnutzung in Österreich

Das Internet hält in immer mehr österreichischen Haushalten Einzug. Laut Erhebung der Statistik Austria sind mehr als 82% aller Haushalte mit einem Internetzugang ausgestattet. 84% aller ÖsterreicherInnen im Alter von 16 bis 74 Jahren nutzen bereits das Internet, wobei die Altersgruppe von 16-34 fast zu 100% InternetuserIn ist.

Dieser Zugang ist keineswegs mehr eine langsame 56k-Leitung von früher, sondern vielmehr eine Breitbandverbindung. Über 82% aller Haushalte genießen somit schnelle Zugriffszeiten auf Websites, Video-Streaming-Dienste, Tauschbörsen oder Socialnetworks.



Befragungszeitpunkt: April bis Juni 2015. - Der Stichprobenfehler beträgt durchschnittlich 1,7%. - Nur Haushalte mit mindestens einem Haushaltsmitglied im Alter von 16 bis 74 Jahren.

Quelle: STATISTIK AUSTRIA – IKT-Einsatz in Haushalten 2015

Birgt das Internet Gefahren für die Bevölkerung?

Ja, definitiv. Wir sind der Meinung, dass sich generell jede/r Internetnutzer/in einer ständigen Gefahr aussetzt, die sich jedoch durch aufgeklärte, bewusste und vorsichtige Nutzung minimieren lässt. Eine völlige Sicherheit kann aber seriöserweise nie garantiert werden.

Das breite Informations- und Möglichkeitsspektrum im Internet spiegelt leider auch die Vielfalt der Betrügereien wider. Doch nicht nur kriminelle Akte werden zum Problem – durch die unachtsame Veröffentlichung persönlicher Informationen werden Identitätsprofile erstellt, Daten für Werbezwecke verkauft oder Jobs plötzlich aufgekündigt.

1. Risiko PCs und Software

Fehlerhafte Einstellungen, veraltete Software oder unachtsames Downloaden von Dingen aus dem Internet am PC führen zu Sicherheitslücken und öffnen für Zugriffe von außen Tür und Tor.

2. Risiko Datenmissbrauch

Mit wenigen Klicks sind heutzutage Informationen, Statusmeldungen oder Fotos veröffentlicht. Leider vergessen manche sehr schnell die damit verbundenen Gefahren.

3. Risiko Online-Einkauf

Mit dem Internet gibt es kaum Grenzen beim Shoppen: Schnäppchen jagen, Bücher und DVDs aus Amerika bestellen, Medikamente, Luxushäuser uvm. Doch was ist verboten? Worauf muss ich achten? Wem vertraue ich hier meine Kreditkartendaten an?

4. Risiko Urheberrecht / Illegalität

Beim weitverbreiteten, illegalen Tausch von Musik oder Videos sind sich Internetuser der Illegalität bewusst. Doch wie sieht es mit dem Urheberrecht vom Bild aus? Darf ich von der Website XY ein Bild kopieren und auf meiner verwenden? Was ist geschützt? Was darf ich? Welche Möglichkeiten gibt es?

5. Risiko Internet-Speicherplatz-Provider (bei vertraulichen Daten)

Der neueste Trend bei der jungen Nutzergemeinde ist die eigenen Daten bei diversen Onlinespeicherdiensten wie Dropbox, Google Drive, etc. zu speichern. Auch hier gibt es unzählige Faktoren, die beachtet werden müssen.

6. Risiko Hacker / Viren / Trojaner

Die lose Gruppierung „Anon“ oder „Anonymous“ wurde in den letzten Monaten zum Synonym für Hacker. Neugierige Computerprofis finden im Internet nahezu „alles, was man so braucht“, um ungesicherte Computer auszuspähen, lahm zu legen und aus der Ferne zu steuern.

7. Risiko MitarbeiterInnen

Mangelndes Sicherheitsbewusstsein und zu geringe Kenntnisse bei den MitarbeiterInnen öffnen Sicherheitslücken.

8. Risiko Datenübertragung / Unsicheres Einkaufen

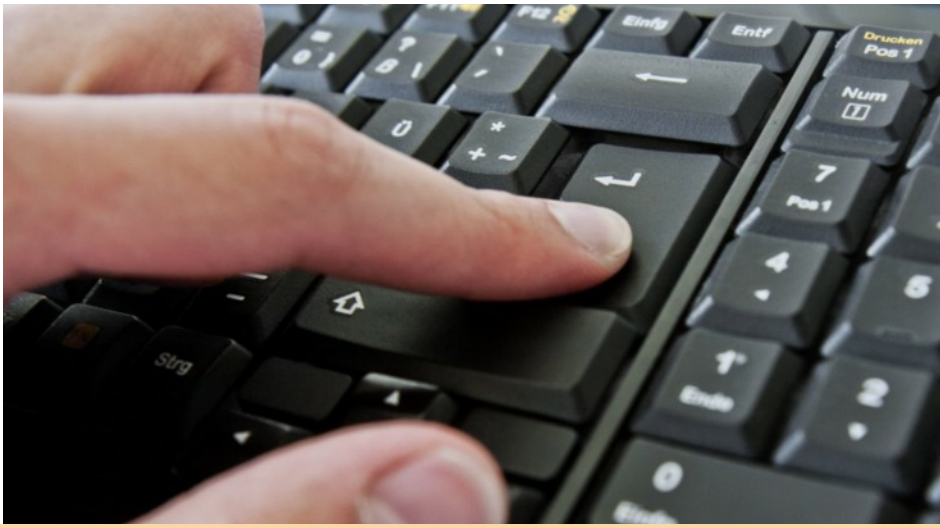
Unverschlüsselte Daten können vielfach abgefangen, manipuliert und/oder belauscht werden. Durch die technischen Gegebenheiten von Netzwerken werden Daten zwischengespeichert; meist ohne, dass es ersichtlich ist, wo, wann und in welchem Ausmaß und wer die Daten lesen kann. Dies ist vergleichbar damit, Gehaltsabrechnungen auf Postkarten zu verschicken.

9. Risiko halbherzige Sicherheitsvorkehrung

Für viele Unternehmen ist die Nutzung von EDV und Internet unerlässlich. Viele scheuen aber die damit verbundenen Kosten für Beratung und Betreuung. Bei sich zuhause wird auch nicht die Vordertür versperrt, die Hintertür aber weit offen gelassen.

10. Risiko mangelhafte oder fehlende Sicherheitsrichtlinien

Eine weitere Schwierigkeit für Unternehmen stellen die in der Praxis oft nicht vorhandenen Richtlinien oder für den Laien unverständliche Formulierungen dar. Um einen sicheren Umgang mit vertraulichen Daten zu gewährleisten, müssen die Risiken sowohl auf der technischen, als auch auf der personellen Ebene berücksichtigt und in ein Gesamtkonzept integriert werden.



Auf einem Standard-PC befindet sich eine Vielzahl an Programmen die für den alltäglichen Gebrauch benötigt werden. Um sich sicher im Internet bewegen zu können, sollte man auf folgende Punkte achten:

- aktuelle Firewall

- aktuelle Antivirensoftware

- Updates von Betriebssystemen installieren

- Browser (Chrome, Internet Explorer, Firefox,...) aktualisieren

- installierte Programme auf dem aktuellsten Stand halten

Vor allem auf den letzten Punkt wird gerne vergessen. Selbst wenn Sie Ihren Browser oder das Betriebssystem aktuell halten, kann es trotzdem passieren, dass Ihnen per Mail ein infiziertes PDF zugeschickt wird. Wenn sich Ihre Software zum Betrachten von PDF nun nicht auf dem aktuellsten Stand befindet, ist Ihr PC auf diesem Weg immer noch angreifbar.

Zehn grundlegende Tipps

Generell empfehlen wir, folgende zehn Grundregeln bei der Nutzung des Internets zu beachten:

1. Computer schützen

Regelmäßige Updates, eine Firewall und eine aktuelle Antivirus-software bieten schon einen guten Schutz für den PC.

2. Privatsphäre wahren

Das Internet vergisst nichts! Daher persönliche Daten nicht leicht-fertig hergeben.

3. „Gesundes" Misstrauen

Nicht alle Informationen im Internet entsprechen der Wahrheit. Gerade wenn Angebote zu gut klingen, um wahr zu sein, sollte man misstrauisch werden.

4. Umsonst gibt's nichts

Beispiel: In den vergangen Monaten tauchten mehrmals Angebote auf, wo tausende Smartphones oder Tablets verschenkt wurden. Wir empfehlen Punkt 3 zu beachten!

5. Keine Vorauskasse bei unbekannten Onlineshops

Shoppen im Internet wird immer beliebter und Waren lassen sich leicht aus dem Ausland bestellen. Wenn es sich vermeiden lässt, zahlen Sie bei unbekannten Shops nicht mit Vorauskasse!

6. Vorsicht bei der Nutzung von fremden Inhalten

Fremde Fotos, Musik oder Videos sind häufig urheberrechtlich geschützt. Sollten Sie diese auf der eigenen Website verwenden wollen, fragen Sie vorher um Erlaubnis!

7. Nicht alles glauben

Häufig erhält man Nachrichten und E-Mails mit sensationellen Angeboten, Gewinnbenachrichtigungen, Geldversprechen, Erbschaften, und vieles mehr. Achten Sie hier auf Absender und seriöse Daten. Ansonsten Punkt 3 und 4 beachten.

8. Phishing Mails sofort löschen

Banken oder Kreditkartenunternehmen fordern Sie nie via E-Mail auf, Ihre Daten zu überprüfen! Löschen Sie solche Mails sofort. Ein weiterer Hinweis: viele Sprach- und Grammatikfehler.

9. Das Internet vergisst nichts

Achten Sie darauf, was Sie im Internet veröffentlichen! Fotos, Statusmeldungen auf Facebook oder dergleichen können nach Jahren ein Problem sein.

10. Rasch Hilfe holen

Unsicher? Fragen Sie die Profis! In dieser Broschüre findet man zahlreiche Links und Informationen zu diversen Stellen.

ZIVILSCHUTZ
Burgenland

Passwörter

Sie benötigen bei fast allen Diensten ein Passwort und einen Benutzernamen. Durch technologische Fortschritte ist es einfach, schwache Passwörter zu brechen. Deswegen sollten Sie darauf achten, dass Ihre Passwörter nach derzeitigen Richtlinien zwischen 6-8 Zeichen lang sind oder noch länger, besonders wenn Sie keine Sonderzeichen und Zahlen verwenden. Das Passwort sollte aus Groß- und Kleinbuchstaben, sowie Sonderzeichen und Zahlen bestehen. Es sollte einfach zu merken sein.

Beispiel für ein gutes Passwort:

- Mein Sohn ist am 12. Mai 1987 geboren!
  Passwort: MSia12.M1987g!

Beispiele für schlechte Passwörter:

- Ihr Geburtsdatum
- Name von Ihnen, Haustieren oder Familienmitgliedern
- alles unter einer Länge von 14 Zeichen
- Einfache Zahlenketten (1234, 12345!)

Um sich komplizierte Passwörter zu merken, gibt es im Grunde zwei sichere Möglichkeiten:

1. Schema

Hier bilden Sie einen Satz, nehmen von jedem Wort einen oder zwei Buchstaben und ersetzen anschließend diese Buchstaben durch Sonderzeichen die ähnlich aussehen.

Beispiel:

Dies ist das Beispielpasswort aus der Broschüre des Burgenländischen Zivilschutzverbandes.

D s i t d s B t a s d r B e d s B n Z s.
(Anfangs- und Endbuchstabe jedes Wortes)

D s 1 7 d s B 7 a s d r B 3 d s B n Z s.
(i durch 1, t durch 7 und e durch 3)

Ds17dsB7asdrB3dsBnZs.

Dieses Vorgehen mag zwar kompliziert wirken, aber man muss sich nur den Satz merken und es ist zusätzlich noch möglich, dass man für die verschiedenen Dienste Zusätze anhängt.

So erhält man für jeden Dienst ein anderes Passwort.

Ds17dsB7asdrB3dsZs.,MAIL

Ds17dsB7asdrB3dsZs.,ARBEIT

2. Passwortmanager

Sie können auch Programme verwenden, die Ihre Passwörter verschlüsselt speichern. Sie müssen sich dann nur noch dieses eine Passwort merken und können alle anderen dann aus diesem Programm rauskopieren.

Online Banking

Online Banking, auch Electronic Banking genannt, erfreut sich immer größerer Beliebtheit und mehr als die Hälfte der Internetuser in Österreich nutzt es regelmäßig.
Um die Sicherheit der Daten und der Nutzer zu gewährleisten, wurden viele Sicherheitsmechanismen implementiert. Durch unsachgemäßen oder leichtfertigen Umgang mit Zugangsdaten und Transaktionsnummern (TAN) kann aber trotzdem leicht großer finanzieller Schaden entstehen.

Um im Internet sicher Ihre Bankgeschäfte zu erledigen, halten Sie ein paar Grundregeln ein!

- Lernen Sie Ihren PIN-Code auswendig! Falls Sie ihn doch notieren, bewahren Sie Ihren PIN-Code getrennt von Ihren TANs auf. Speichern Sie PIN und TANs nie auf Ihrem PC und geben Sie diese nicht weiter!
- Ändern Sie Ihren PIN-Code in regelmäßigen Abständen!
- Verwenden Sie die aktuelle Version Ihres Internet-Browsers und Ihres Antivirenprogramms!
- Deaktivieren Sie die „Auto-Vervollständigen"-Funktion Ihres Browsers!
- Führen Sie Ihre Bankgeschäfte nur auf vertrauenswürdigen Computern durch, idealerweise auf Ihrem eigenen!
- Nachdem Sie Ihre Bankgeschäfte abgeschlossen haben, melden Sie sich im Browser von der Online Banking-Website ab!
- Melden Sie den Verlust Ihrer Bankomatkarte oder Ihrer TAN-Liste sofort Ihrer Bank!
- Bei der Verwendung von Online Banking auf Ihrem Smartphone, achten Sie darauf, dass niemand unberechtigt Zugriff erhält!

Die Bank wird nie anrufen oder mailen und die Zugangsdaten des Benutzers verlangen!
Als Absicherung kann man auch mobile TANS verwenden, welche per SMS geschickt werden und nur einmalig einzugeben sind.

Eine zusätzliche Gefahr stellen betrügerische E-Mails, sogenannte Phishing-Mails dar, mithilfe derer an Zugangsdaten zu verschiedenen Angeboten im Internet, unter anderem zum Online Banking, gelangt werden soll. Oft enthalten diese E-Mails Aufforderungen, PIN-Codes oder TANs zu senden, oder beinhalten Links zu täuschend echt nachgebauten Online Banking-Websites, bei denen sich der Nutzer anmelden soll.

Um Phishing beim Online Banking zu erkennen und zu vermeiden, beachten Sie folgende Regeln:

- Geben Sie PIN-Code und TAN-Codes nie an Dritte weiter! Ihre Bank wird Sie nie danach fragen!
- Achten Sie darauf, dass Sie die richtige Internetadresse Ihrer Bank eingeben und dass sie mit https:// beginnt!
- Überprüfen Sie regelmäßig Ihre Kontoauszüge nach nicht von Ihnen getätigten Zahlungen!

„Wenn Ihnen etwas Verdächtiges auffällt, melden Sie das sofort Ihrer Bank!“

ZIVILSCHUTZ Burgenland

Mit Leuten in Kontakt bleiben, die neuesten Fotos aus dem Urlaub teilen oder einfach nur mal kurz nachsehen, was bei Freunden gerade so los ist. Soziale Netzwerke wie Facebook, MySpace oder Twitter bieten ihren Usern viele Möglichkeiten, das eigene Leben mit dem virtuellen „Ich" zu verknüpfen, jedoch bringen diese Optionen auch neue Probleme mit sich.

Statusmeldungen: Mit kurzen Nachrichten kann man schnell einmal erzählen, was heute so in Schule, Arbeit oder auf dem Fußballplatz los war. Einfach und schnell wissen es alle Freunde. Problematisch wird es dann, wenn man seinem Ärger über Freunde in der virtuellen Welt Luft macht (durch Beschimpfungen und Beleidigungen) und die Betroffenen direkt aus dem Netzwerk oder über andere User davon erfahren.

Beispiel: Man sollte es vermeiden, sich über den Kollegen nebenan oder sogar den Chef zu beschweren oder gar zu schimpfen, und das womöglich während der Arbeitszeit. Auch Nachrichten, in denen es um die Anzahl der getrunkenen Tequilas am Wochenende geht, sollte man unterlassen. Solche Nachrichten rücken einen in ein schlechtes Licht z.B. für zukünftige Bewerbungsgespräche. Deshalb sollte man stets im Hinterkopf behalten, dass nicht nur das soziale Netzwerk nicht vergisst, sondern auch der Chef, die Kollegen oder Freunde werden sich noch lange an Beschimpfungen oder schlechte Nachrede erinnern.

Unsere Tipps:

- Surfen in sozialen Netzwerken nicht während der Arbeitszeit.
- Keine beleidigende Nachrichten posten und sich dessen bewusst sein, dass diese Postings z.B. auch von „Freunden von Freunden" gelesen werden können!
- Keine Statusnachrichten posten, die einen in der Zukunft selber Probleme bereiten können (z.B. übermäßiger Alkoholkonsum, prahlen über unerlaubtes Fernbleiben).
- Keine Ankündigungen über den derzeitigen Standort (Einkaufsbummel, Urlaub, Ausflug, etc.) posten. Erst dann posten, wenn man wieder zu Hause ist.

Fotos im Netz - Ein Bild sagt mehr als tausend Worte

Nicht nur Statusmeldungen, auch Bilder können Schwierigkeiten mit sich bringen. Ob es nun die Fotos von der letzten Feier zu Hause oder dem Fortgehen im Club am Wochenende sind, auf aktuelle oder zukünftige Arbeitgeber machen Fotos von potenziellen Mitarbeitern mit der Flasche Wodka in der Hand keinen guten Eindruck.

Immer wieder werden außerdem aufreizende Bilder, bei denen viel nackte Haut gezeigt wird, ins Netz gestellt. Solche haben dort ebenfalls nichts zu suchen. Ein bisschen Haut ja, aber nur so viel wie man auch bei einem Bewerbungsgespräch zeigen würde.

Das „Creative Commons" bei eigenen Fotos ist zu empfehlen. Es gibt bereits Apps, welche Fotos mit„Creative Commons" (watermark) versehen. So dürfen Dritte das Foto nicht verwenden.

Unsere Tipps:

- Peinliche Fotos nicht online stellen (z.B. angetrunken auf einer Party)!
- Auf Fotos nicht zu viel nackte Haut zeigen - wirkt unseriös!
- Personen, die fotografiert wurden, fragen, ob das Foto ins Netz gestellt werden darf! Bei Bedarf Gesicht unkenntlich machen!

Cybermobbing ist Mobbing, es passiert jedoch rund um die Uhr und überall. Nicht nur an der Schule, Arbeitsstelle oder in der Freizeit, sondern auch über sämtliche digitale Medien (SMS, MMS, Telefonanrufe, Internetplattformen, E-Mails, etc.).

Betroffene können nicht mehr abschalten und sind sehr schnell in der Rolle des Opfers, in der sie sich selbst als Schuldigen für diese Situation sehen.

Cybermobbing kann bis hin zum Selbstmord führen (Fall: Amanda Todd).

Unsere Tipps:

- Wenn man von Cybermobbing erfährt, sollte dies rasch gemeldet werden! Am besten wendet man sich an Lehrer, Vertrauenspersonen oder (psychosoziale) Beratungsstellen in der Nähe!

- Wenn möglich, sollte die betroffene Person kontaktiert werden! Es ist wichtig, Opfern zu zeigen, dass sie nicht alleine sind und man sich wehren kann.

Beratungsstelle Mobbing:
www.mobip.at *www.mobbingberatung.org*

Tipps für Opfer:

- Am besten zeigt man keine Reaktion auf Angriffsversuche auf sich selbst!
- Sagen Sie, dass Sie gemobbt werden!
- Suchen Sie sich eine Vertrauensperson, die Ihnen hilft, sich gegen Cybermobbing zur Wehr zu setzen!
- Melden Sie Mobbingseiten/Mobbingprofile dem Betreiber der Seite, um diese löschen zu lassen!
- Geben Sie Fotos nur an Personen weiter, die Sie kennen und denen Sie vertrauen!

Kriminalprävention: Mit **059-133** erreicht man immer die nächstgelegene Polizeidienststelle in Österreich. Auch bei Mobbing sollte man nicht davor zurückschrecken, die Polizei zu Rate zu ziehen!

Telefonseelsorge: Mit **142** erreicht man die in ganz Österreich kostenlose Telefonseelsorge.

Was ist Malware?

Im Allgemeinen ist Malware eine Software, die das Ziel verfolgt, auf einem Computersystem unerwünschte Aktionen auszuführen. Allerdings werden fehlerhafte Programme nicht als Malware bezeichnet.

Je nachdem, wie diese Schadsoftware auf das Computersystem gelangt und wie sich diese darauf verhält oder auch verbreitet, wird sie in verschiedene Kategorien unterteilt. Einige davon sind Viren, Würmer, Trojaner, Rootkits und andere.

Ziele von Malware können sein:

- Spionage
- Verbreitung von illegalen Daten (Kinderpornographie)
- Anonymisierung von illegalen Tätigkeiten
- Diebstahl von Daten (Kreditkarteninformationen)

Mittlerweile gibt es fast kein Computersystem, welches generell als „Malware-sicher" gilt. Je populärer eine Technologie wird, umso mehr zahlt sich das Produzieren von Malware für dieses Computersystem aus.

Infektion

Malware kann über verschiedene Wege in ein Computersystem eindringen. Diese Möglichkeiten reichen vom einfachen Ausführen von fremden Dateien über bösartige Websites bis hin zu Programmfehlern in bereits installierter Software.

Oft wird Malware auch in kostenpflichtigen Programmen eingebaut und dann als Gratisversion veröffentlicht. Benutzer des Smartphone-Betriebssystems Android sind davon besonders betroffen.

Malware kann schon in einer einfachen PDF-Datei enthalten sein. Der eingebettete Programmcode wird dann beim Öffnen oder Speichern der Datei ausgeführt.

Schutz und Bereinigung

Antiviren-Hersteller stellen eigene Programme zur Verfügung, welche Malware erkennen und vom System entfernen bzw. deren Funktionen blockieren können. Die Erkennung findet im Normalfall durch Datenbanken statt, die bereits aufgedeckte Malware beinhalten. Dadurch ist es enorm wichtig, diese Datenbank immer am aktuellsten Stand zu halten, da nur so auch neu erschienene Bedrohungen erkannt werden können.

Ist nun ein System bereits infiziert, bieten Antivirenprogramme oft auch die Möglichkeit, ein ganzes System zu bereinigen.

In manchen Fällen werden von diesen Programmen präventiv regelmäßig alle Dateien eines Systems auf Schadsoftware gefiltert.

Bei professioneller Malware werden allerdings auch moderne Virenscanner oft versagen, da Malware auch die Eigenschaft besitzt, sich in einem befallenen Computersystem zu verstecken.

In diesen Fällen kommt man um fachmännische Hilfe oder um das Einspielen eines sauberen Backups (Daten sichern) kaum herum.

Wenn man sich bei fremden Dateien nicht sicher ist, kann man diese bei **www.virustotal.com** von vielen Virenscannern checken lassen.

Checkliste

- Verwendung von modernen und aktuellen Antiviren-programmen
- Regelmäßige Aktualisierungen der Datenbanken
- Regelmäßige Updates der verwendeten Programme und des Betriebssystems
- Regelmäßige Erstellung eines Backups
- Vorsicht mit unbekannten Dateien und Websites
- Verwendung von vorhandenen Sicherheitseinrichtungen (Firewalls)

Im Internet sind viele kostenlose Antiviren-Programme verfügbar. Auf neuen Computersystemen sind oftmals auch schon Testversionen vorinstalliert.

Onlineshopping gewinnt Jahr für Jahr mehr an Bedeutung. Auch in Österreich erfreut sich diese Form des Einkaufens immer größerer Beliebtheit. Dabei vergisst man schnell darauf, dass auch Gefahren und Betrüger dahinter lauern können.

Meine Daten im Internet

Wie bei den meisten Angelegenheiten im Internet ist es auch hier erforderlich, dass man bei der Registrierung persönliche Daten wie Name, Adresse, Geburtsdatum, aber auch Kontodaten angibt. Hier kann bereits die erste Falle „Datendiebstahl" auf unachtsame Benutzer warten! Noch vor der Ausfüllung des Registrierungsformulars sollte man sich ein Bild über den Onlineshop machen.

Dafür hat man zahlreiche Möglichkeiten sowohl offline als auch online. Man kann zum Beispiel im Freundeskreis nachfragen, ob jemand schon Erfahrungen mit dem jeweiligen Anbieter/Shop gemacht hat.

Oder man stürzt sich in die Welt der Suchmaschinen und macht ein, zwei Suchanfragen nach „Shopname Betrug", „Shopname seriös" oder „Shopname Abzocke". Ergibt die Suche keinen Treffer, so ist man schon auf gutem Weg, dennoch lohnt sich meistens ein Blick auf die Website des Anbieters. Unseriöse Seiten erkennt man oft an einer schlechten Ausdrucksweise und/oder Grammatik.

Wenn der Firmensitz in fernen Ländern wie Zypern, Kaiman-Insel, etc. eingetragen ist, sollte man besonders vorsichtig sein.

Bezahlung

Die kritischste Phase beim Onlineshopping ist der Bezahlvorgang. Hier sollten Sie vor allem darauf achten, dass die Kommunikation verschlüsselt ist (erkennbar an dem Schloss-Symbol). Dies ist bereits ein gutes Zeichen, heißt aber nicht, dass der Bezahlvorgang zu 100% sicher ist. Die gespeicherten Kontodaten oder Kreditkartennummern werden üblicherweise vom Betreiber gespeichert, damit Sie bei wiederholtem Einkauf diese nicht erneut eingeben müssen. Hier besteht noch die Gefahr, dass sie von Dritten gestohlen werden können. Deswegen sollten Sie aufgrund dieses Restrisikos nur bei vertrauenswürdigen Anbietern bestellen.

Checkliste

- Sich über den Onlineshop informieren (AGB, Impressum, Gütesiegel)
- Shop via Suchmaschinen-Recherche überprüfen
- Im Betrugsfall Polizei oder Konsumentenschutz kontaktieren

Nützliche Links

- Österreichs Internet Ombudsmann
  Hier findet man neben Informationen zum Onlineshopping auch Tipps, wie man Betrug im Internet allgemein erkennt. *www.ombudsmann.at*
- Online Sicherheitportal vom Bundesministerium für Finanzen, Bundeskanzleramt und A-SIT. Die Seite bietet umfassende Informationen darüber, wie man sich und das eigene System schützt. *www.onlinesicherheit.gv.at*
- Onlineinitiative vom Österreichischen Institut für angewandte Telekommunikation (ÖIAT) in Zusammenarbeit mit dem Verband der Internet Service Providers Austria (ISPA)

Nützliche Tipps für die Internetnutzung gibt es auf
www.saferinternet.at

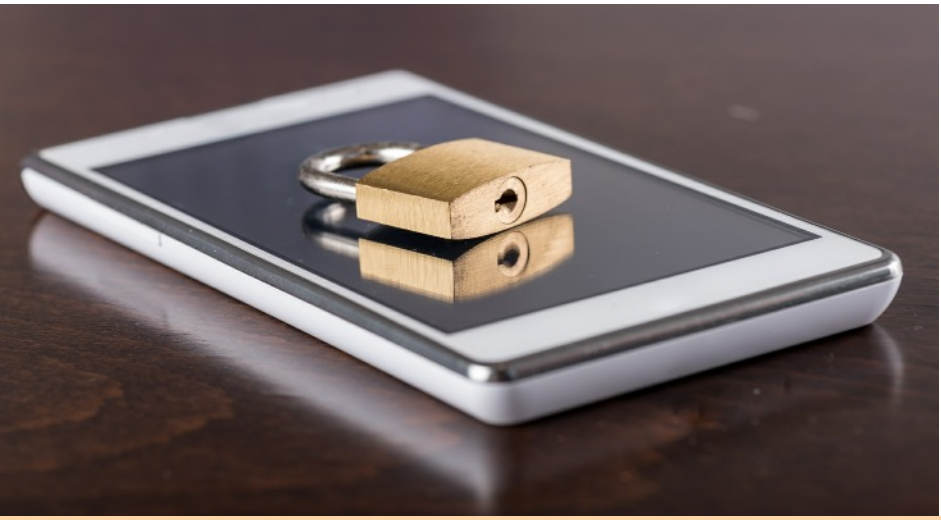
Zu der Handhabung von Smartphones sei gesagt, dass auch diese wie ein PC funtionieren, dass heißt, ich muss auch mein Smartphone mit Antivirus und Firewall ausstatten; die Updates sollten immer auf der Betreiberseite und nicht über Seiten von Drittanbietern durchgeführt werden. Wenn man Antivirus installiert hat, wird man sofort bei einer auffälligen App vor dem Download auf allfällige Sicherheitsrisiken aufmerksam gemacht. Es kommt nicht nur bei Android vor, sondern auch beim appstore von apple. In diesem Zusammenhang sei die Internetseite *www.watchlist.at* erwähnt, da man dort alle Apps, Anwenderprogramme und verseuchten Seiten, aber auch alle Arten von Viren, Trojanern und Schadsoftware im Netz in Listen angeführt hat. Die Seite watchlist.at ist eine Partnerseite zu Saferinternet. Dort kann man sich immer wieder Tipps holen und nachsehen, was gerade aktuell ist.

Telefon Bildschirmsperre

Alle Smartphone-Betriebssysteme bieten die Möglichkeit, durch Pins, Pattern oder die Eingabe eines Passwortes vor unbefugten Zugriffen auf Daten zu schützen.

Ab Android 4.0 wird vom System eine Gesichtserkennung angeboten, wodurch ein einfaches und schnelles Entsperren nur für den rechtmäßigen Besitzer ermöglicht wird.

Es sollte jedoch nicht nur das Gerät an sich geschützt werden, sondern auch die darauf gespeicherten Daten. Der simpelste Tipp liegt dabei auf der Hand: Speichern Sie keine sensiblen Daten auf Ihrem Smartphone. Sollte sich das nicht vermeiden lassen, ist das Benutzen von speziellen Verschlüsselungs-Apps eine gute Möglichkeit.



Programme - „Apps“

Weniger ist manchmal mehr. Umso überschaubarer die Anzahl der Apps am eigenen Smartphone ist, desto sicherer sind die persönlichen Daten.

Market/App Stores

Die riesige Auswahl an zahlreichen, unterschiedlichen Apps verdeutlicht bereits die Schwierigkeit der Übersicht und Überprüfbarkeit der App Stores.

Daher trägt der einzelne Nutzer eine umso größere Eigenverantwortung bei der sicheren Verwendung von Apps.

Eine einfache Möglichkeit vor dem Herunterladen und Installieren bietet dabei das Lesen der Kommentare nach Hinweisen auf negative Eigenschaften der Anwendung.

Auch Foreneinträge und das Überprüfen des Herstellers können wichtige Rückschlüsse auf die Vertrauenswürdigkeit geben.

Apps und deren Rechte

Die meisten Betriebssysteme bieten eine Funktion, um die von der App benötigten Rechte anzuzeigen. Damit kann der Zugriff auf persönliche Daten kontrolliert werden.

Neben den notwendigen Funktionen können unbemerkt sensible Daten gesammelt werden.

Problematisch sind vor allem Apps, die Vollzugriff auf das Telefonbuch oder andere wichtige persönliche Daten wie E-Mail Adressen oder Geburtsdaten benötigen.

Oftmals ist es möglich, im Menü bestimmte Datenverarbeitungen, wie zum Beispiel den Export von Standortdaten, zu unterbinden.

Falls diese Möglichkeit vom Betriebssystem nicht unterstützt wird, sollte man sich überlegen, ob die jeweilige App unbedingt benötigt wird und man sich auf die Weitergabe der eigenen Daten einlässt, oder lieber auf die Installation der Software verzichtet.

Das Urheberrecht hängt nicht mit dem körperlichen Eigentum an einer Sache zusammen. Wenn man etwa eine Musik-CD kauft, erwirbt man (körperliches) Eigentum an der CD. Man kann daher mit der (körperlichen Sache) CD tun, was man will, sie auch weiterverkaufen, verschenken oder zerstören. Man darf den Inhalt aber nicht öffentlich aufführen, im Internet zur Verfügung stellen oder unbeschränkt kopieren.

Wollen Sie Texte, Fotos, Videos oder Musik hochladen oder in irgendeiner Form online verwenden, informieren Sie sich vorab darüber, ob es sich um urheberrechtlich geschützte Werke handelt.

Unwissenheit ist kein Schutz vor Strafe und bei Verletzung des Urheberrechtes drohen bis zu mehreren tausend Euro Strafe.

Möchten Sie Werke für eine Veröffentlichung nützen und sich rechtlich absichern, so informieren Sie sich vorab über CC-lizenzierte Inhalte. „CC" steht für „Creative Commons" also „schöpferisches Gemeingut" und ist eine gemeinnützige Organisation, die Standard-Lizenzverträge veröffentlicht, bei denen ein Autor auf einfache Weise der Öffentlichkeit das Nutzungsrecht einräumt. *www.creativecommons.org*

Erklärung „Sextorsion“: eine meist weibliche attraktive Frau schickt über Internetplattform eine Freundschaftsanfrage (meist an junge Männer im Alter von 15-27 Jahren).

Wenn die Freundschaftsanfrage angenommen wird, wird ein wenig gechattet, bis es zu einer Verabredung über Skype kommt, wo die Dame darum bittet, sich selbst zu befriedigen. Wenn der Akt vollzogen ist, folgt unverzüglich eine Mail mit dem Inhalt an ein bestimmtes Konto einen bestimmten Betrag zu bezahlen, damit das Video welches nebenbei von der Dame über Skype angefertigt wurde, nicht ins Netz gestellt wird.

Egal, ob man bezahlt oder nicht, das Video landet auf Youporn oder Youtube. Es kann auch vorkommen, dass das Video auf der eigenen Seite im Internet geteilt wird.

Hier wäre es wichtig, sich mit dem Internet-Ombudsmann in Verbindung zu setzen und sofort eine Anzeige bei der Polizei zu machen.

Erklärung „Sexting“: SMS und MMS mit pornographischem Inhalt (Sätzen oder Bildern) welche zur Anbahnung von Kontakten versendet werden.

Dabei handelt es sich um ein Schriftstück, welches aufgesetzt wird (mit oder ohne Notar) in dem steht, wer nach dem Tod die Eintragungen bzw. Registrierungen löschen darf bzw. löschen wird. Meist ist es so, dass eine Person sich bei Internetforen bzw. Katalogen mit Benutzernamen und Passwort registriert. Wenn die Person verstirbt, wissen die Angehörigen meist nicht, wie sie die Seiten löschen bzw. die Registrierungen löschen können. Dies kann ohne einen Digitalen Nachlass sehr mühsam sein, da die meisten Internetbetreiber die Sterbeurkunde, die Geburtsurkunde, sowie das Verwandtschaftsverhältnis haben wollen, damit der Account gelöscht wird.

Das heißt, wenn ich mir aufschreibe, wo ich mit welchem Benutzer und Passwort registriert bin, können meine Angehörigen im Falle meines Todes die Accounts entfernen bzw. löschen oder einfrieren, ohne große Behördengänge zu vollziehen

Wie kann man als Eltern den Internetkonsum seines Kindes ein Stück weit kontrollieren?

Vor allem ist es für Eltern wichtig, an dem, was Ihr Kind tut, selbst Interesse zu zeigen! Fragen Sie nach, sprechen Sie aber keine allgemeinen und absoluten Verbote aus. Diese führen dazu, dass ein Kind z.B. heimlich im Internet surft und sich dann auch nicht an Sie als Elternteil wendet, wenn es zu Schwierigkeiten kommt.

Sprechen Sie mit ihrem Kind darüber, was Ihnen Sorge bereitet und versuchen Sie sich Zeit zu nehmen, das Internet auch einmal gemeinsam zu entdecken.

Lassen Sie sich von Ihrem Kind die Dinge zeigen und erklären, die es gerne im Internet macht, Kinder haben oft eine rasche Auffassungsgabe und sind Profis in eigener Sache. Damit fühlt sich Ihr Kind ernstgenommen, Sie verschaffen sich jedoch auch selbst einen besseren Überblick über die Tätigkeiten Ihres Kindes im Netz und am Computer!

Ein Großteil der KonsumentInnen nutzt das Internet im täglichen Leben für Geschäfte aller Art. Aus diesem Grunde werden die Rechte der KonsumentInnen laufend verbessert und gestärkt.

Das mit 13.06.2014 in Kraft getretene Fern- und Auswärtsgeschäftegesetz (FAGG) brachte wesentliche Änderungen für KonsumentenInnen im Bereich von Internetgeschäften:

- Umfangreiche vorvertragliche Informationspflichten der Unternehmen
- Zurverfügungstellung dieser Informationen u.a. auf dauerhaftem Datenträger
- „Button-Lösung" – ausdrücklicher Hinweis auf Zahlungsverpflichtung
- Rücktrittsbelehrung samt Zurverfügungstellung eines Musterformulars
- Rücktrittsrecht und Rücktrittsfrist
- Ausübung des Rücktrittsrechts und Rechtsfolgen
- Ausnahmen vom Rücktrittsrecht

Wichtige Adressen zur Information:

www.ombudsmann.at
kostenlose Schlichtungsstelle für Online-KonsumentInnen

www.watchlist-internet.at
aktuelle Warnungen zu Onlinebetrug oder – fallen

www.verbraucherschlichtung.at
kostenlose Schlichtungsstelle für KonsumentInnen

www.europakonsument.at
Hilfe bei grenzüberschreitenden Verbrauchergeschäften

www.konsument.at
Verein für Konsumenteninformation

www.konsumentenfragen.at
Konsumentenportal vom BMASK

Wie sicher ist mein Computer?

Wenn Sie sich diese Frage stellen, sollten Sie die nachstehende Checkliste Punkt für Punkt abarbeiten. Mit dieser können Sie überprüfen, ob Ihr PC sicher gegenüber „Angreifern“ wie Viren, Würmern, Hackern und ähnlichen unangenehmen Attacken aus dem Internet ist.

Ist Ihr PC einmal von einem Virus befallen, bringt das nicht nur Ärger und Zeitverlust, sondern meist auch Kosten mit sich. Oft können wertvolle Daten für immer verloren gehen. Aber eigentlich braucht es nicht viel, um sich vor Attacken aus dem Netz zu schützen. Man muss es halt tun.

Wenn Sie alle folgenden Punkte abhaken können, dann ist Ihr PC gegenüber Attacken aus dem Netz relativ sicher. Eine 100% Sicherheit gibt es aber nicht.
Alle nicht abgehakten Punkte weisen Sicherheitslücken auf. Diese sollten Sie möglichst umgehend beheben.

Um Angreifern auf Ihren Computer die Sache so schwer wie möglich zu machen, hier der Sicherheits-Check:

☐Eine Firewall und ein Antivirenprogramm ist installiert und aktiviert.

☐Mein PC wird in regelmäßigen Abständen einer vollständigen Virenüberprüfung unterzogen (in der Regel automatisch durch das Antivirenprogramm), das Antivirenprogramm wird laufend aktualisiert.

☐Vom Antivirenprogramm werden die E-Mail-Anhänge beim Ein- und Ausgang automatisch geprüft.

☐E-Mail-Anhänger von unbekannten Absendern und Spam-Mails werden ungeöffnet gelöscht.

☐Bei einem Kabel- oder ISDN-Anschluss: Ein Dialer-Schutzprogramm ist installiert, bzw. kostenpflichtige Rufnummern (0900, 0910 etc.) wurden gesperrt.

☐Passwörter und Zugangsdaten für Web-Banking, Online-Einkauf werden nicht automatisch gespeichert. Anfragen per Mail zur Passwort-Bestätigung, Kontonummern etc. werden ignoriert.

☐Wichtige Daten und solche, in denen „viel Arbeit steckt", werden in regelmäßigen Abständen gesichert.

☐Im E-Mail-Programm (z.B. Outlook) sind die Spam- und Sicherheitseinstellungen eingerichtet.

☐Sicherheits-Updates für Browser, E-Mail-Programm und Betriebssystem werden regelmäßig installiert.

☐Sensible Unternehmensdaten werden auf einem eigenen PC ohne Internetanschluss gespeichert.

☐Über Filesharing angebotene Dateien (z.B. Musikdateien) sind zu einem großen Teil „verseucht". Deshalb werden Filesharing-Programme nicht genutzt.

☐Der Zugang zum PC ist mit einem Passwort geschützt (nicht nur Angriffe aus dem Netz bilden eine Bedrohung. Auch Personen, die unmittelbaren Zugang zu Ihrem Computer haben, können großen Schaden anrichten).

Die Aufgabe des Burgenländischen Zivilschutzverbandes ist es, die Bevölkerung zu informieren, wie man Gefahren richtig erkennt, dabei richtig reagiert und entsprechende Maßnahmen setzt.

Kontakt:

Österreichischer Zivilschutzverband
7000 Eisenstadt, Hartsteig 2
Tel: 02682/63620 Mail: office@bzsv.at Web: www.bzsv.at

Wichtige Notrufnummern:

112	**Euronotruf (gültig in den meisten europäischen Staaten)**
122	Feuerwehr
133	Polizei
144	Rettung
128	Gasnotruf
130	Landeswarnzentrale
140	Bergrettung
141	Ärztenotdienst
01/4064343	Vergiftungsinformationszentrale