



ZIVILSCHUTZ
Österreich

www.zivilschutzverband.at

INTERNET RATGEBER

**Surfen und chatten,
auf das ist zu Achten**

Weitere Informationen, Broschüren und Produkte
finden Sie unter www.zivilschutzverband.at

INTERNET SICHERHEIT

Worauf sollte beim Surfen
und Chatten geachtet werden?

Vorher denken, dann klicken!

www.zivilschutz.steiermark.at  Ist Ihnen Ihre Sicherheit nicht einen Klick wert?



Impressum

Herausgeber, Verleger, Redaktion und Gestaltung:

Österreichischer Zivilschutzverband, Spiegelgasse 6/13, 1010 Wien

Fotos: pixabay.com, 123rf.com

INTERNETNUTZUNG IN ÖSTERREICH

Klar ist, dass das Internet nicht mehr aus unserem Leben wegzudenken ist. Es hat unsere Gesellschaft grundlegend verändert, vom Beruf bis zur Familie. Dazu kommt noch, dass immer mehr Menschen das Internet auch über das Smartphone und Tablets von überall aus nutzen.

Es ist so selbstverständlich, dass wir uns der Gefahren nicht mehr bewusst sind.

Das breite Informationsspektrum spiegelt die Vielfalt aller damit verbundenen Gefahren. Doch nicht nur kriminelle Akte werden zum Problem, auch die Unachtsamkeit der Nutzer wird häufig unterschätzt.

Daher bedenken Sie:

Nur wer sich der Gefahr bewusst ist, kann sich davor auch schützen. Gut geschützt ist man aber nur mit ausreichenden Wissen.

Durch einen bewussten Umgang mit Internet und den neuen Medien kann man sich viel Ärger und Probleme ersparen.



Die unendliche Welten des Internets

RISIKEN

Die Nutzung des World Wide Webs birgt Risiken. Durch überlegtes Handeln können diese oft schon ohne großen Aufwand minimiert werden. Denken Sie daran, im Internet gibt es nicht nur „gute“ Nutzer.

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.

RISIKO DATENMISSBRAUCH

Mit wenigen Klicks sind Informationen, Statusmeldungen, Fotos und viele andere Infos veröffentlicht. Leider vergessen manche sehr schnell die damit verbundenen Risiken und Gefahren.

Bedenken Sie immer: Das Internet vergisst nichts!

RISIKO ONLINE-EINKAUF

Mit dem Internet gibt es keine Grenzen beim Shoppen. Vertrauen Sie keinen noch so „GUTEN und GÜNSTIGEN“ Angeboten. Auch im Internet wird Ihnen nichts geschenkt. Achten Sie darauf bei wem sie was erwerben und sind Sie mit den Angaben zu Ihrer Personen bzw. Ihren Bankdaten sehr vorsichtig. Daten können vielfach abgefangen bzw. manipuliert werden.

Dies ist vergleichbar damit, Gehaltsabrechnungen auf Postkarten zu verschicken.

Achten Sie bei Online-Shops auf das österreichische E-Commerce-Gütezeichen und auf Euro-Label – Infos auf www.euro-label.com
Seien Sie besonders vorsichtig bei Einkäufen ohne Gütezeichen. Versuchen Sie alle Informationen über den Anbieter herauszufinden. Dabei kann man sich an die Kriterien des Euro-Label orientieren.

- Ist der Name des Anbieters bzw. dessen Kontaktdaten (Adresse, Telefon, Mail, ...) angegeben?
- Eine Domain die mit „at“ endet ist keine Garantie dafür, dass das Unternehmen in Österreich seinen Sitz hat.
- Sie die allgemeinen Vertragsbedingungen leicht zu finden und zu verstehen?
- Gibt es einen Hinweis auf das Rücktrittsrecht?
- Sind Vorgang der Bestellung bzw. die Angabe des Preises nachvollziehbar und transparent?
- Gibt es eine vereinbarte Lieferzeit?
- Welche Zahlungsmöglichkeiten werden angeboten?
- Gibt es Bewertungen zu Ihrem ausgewählten Anbieter? Glauben Sie aber nicht jede Jubelmeldung über das Unternehmen, diese könnte auch selbst verfasst worden sein.



Vorsicht bei Zahlungen im Internet

BEZAHLUNG

Eine sehr kritische Phase beim Onlineshopping ist der Bezahlvorgang. Hier müssen Sie darauf achten, dass die Kommunikation verschlüsselt ist.

Keine Vorkasse bei unbekannten Onlineshops

Shoppen im Internet ist sehr beliebt und wird immer mehr. Bezahlen Sie bei unbekannten Shops nicht mit Vorkasse. Sollte dies nicht anders möglich sein, dann denken Sie darüber nach, ob Sie dieses Produkt nicht auch in Ihrer Umgebung kaufen können.

RISIKO WLAN

Vermeiden Sie Sicherheitsrisiken im öffentlichen WLAN. WLAN-Benutzer sind Risiken durch Hacker ausgesetzt! Man erhält heute nahezu überall den Zugang zu GRATIS-WLAN! Diese Freiheit hat aber natürlich auch ihren Preis und ist auch gefährlich. Daher ist es besonders ratsam, dass man sich dieser Gefahr bewusst ist.

Öffentliches WLAN ist für Hacker besonders attraktiv. Es ist keine Authentifizierung nötig, um eine Verbindung zu einem Netzwerk herzustellen, dadurch haben Hacker nahezu uneingeschränkten Zugriff auf ungesicherte Geräte im selben Netzwerk. Cyberkriminelle nutzen diese unsicheren Verbindungen vor allem für die Verbreitung von Malware.

DAS SICHERE WLAN

EINIGE TIPPS:

- **Nutzen Sie keine Standardpasswörter**

Für Hacker ist ein Leichtes, das Standardpasswort des Router-Herstellers herauszufinden, und dieses Passwort dann zu verwenden, um auf Ihr Netzwerk zuzugreifen. Deshalb sollten Sie das Administratorpasswort Ihres WLAN-Routers ändern.

- **Sorgen Sie dafür, dass Ihr WLAN-Router nicht zu ermitteln ist**

Deaktivieren Sie das SSID-Broadcasting (Service Set Identifier), um zu verhindern, dass Ihr WLAN-Router seine Existenz öffentlich preisgibt.

- **Verschlüsseln Sie Ihre Daten**

Vergewissern Sie sich, dass in den Verbindungseinstellungen die Verschlüsselung aktiviert ist. Wenn Ihr Gerät die WPA-Verschlüsselung unterstützt, wählen Sie diese Option – aktivieren Sie andernfalls die WEP-Verschlüsselung.

- **Schützen Sie sich vor Malware und Online-Angriffen**

Installieren Sie ein zuverlässiges Anti-Malware-Produkt auf Ihren Computern und anderen Geräten. Damit der Malware-Schutz immer auf dem neuesten Stand ist.

Bedenken Sie:

In einem offenen WLAN-Netzwerk liegen die gesendeten Daten praktisch auf dem Präsentierteller. Jeder, der im selben Netzwerk surft, kann mitlesen, welche Datenpakete ein Laptop, Smartphone oder Tablet sendet und empfängt.



PASSWÖRTER

Sie benötigen bei fast allen Diensten ein Passwort und einen Benutzernamen. Durch technologische Fortschritte wird es immer einfacher Passwörter zu knacken. Daher kommt der Passwort-Sicherheit ein immer höherer Stellenwert zu.

Leider werden noch immer sehr schlechte Passwörter verwendet wie: 1;2,3;4; oder hallo bzw. Passwort usw. ...

Bedenken Sie: Ein Passwort muss möglichst lang und zeichenreich sein, wenn es Sicherheit bieten soll. Verwenden Sie bei jeder Registrierung ein neues Passwort.

BEISPIELE:

Dies ist das Passwort aus der Broschüre des Österreichischen Zivilschutzverbandes mit Sonderzeichen.

DsitsdPtasdrBedsÖnZs.1010\$%&Wien
(Anfangs- und Endbuchstaben jedes Wortes)

Buchstaben durch Zahlen ersetzen

7sit7sPtas7rBe7sÖ3Zs.1010\$%&W3
(d wird durch 7 und n durch 3 ersetzt)

Meine Tochter ist am 16. Mai 1987 geboren!

Passwort: MTia16.M1987g!

ACHTUNG! Kleben Sie Ihr Passwort nicht auf einem Zettel auf den Schreibtisch oder Monitor. Notieren Sie sich keine Passwörter. Die Gefahr, dass Sie diese Zettel verlieren ist groß. Speichern Sie keine Passwörter bzw. versenden Sie diese nicht online. Informieren Sie sich über Passwortmanager.



GRUNDLEGENDE TIPPS

SCHUTZ DES COMPUTERS

Schützen Sie Ihren Computer und alle anderen Geräte, mit denen Sie online sind. Regelmäßige Updates, eine Firewall und aktuelle Antivirussoftware sind eine Basis für Ihren Computer und bieten schon einen ganz guten Schutz.

WAHREN SIE IHRE PRIVATSPHÄRE

Das Internet vergisst nichts! Daher persönliche Daten nicht leichtfertig hergeben

GESUNDES MISSTRAUEN

Nicht alle Informationen im Internet entsprechen der Wahrheit. Gerade wenn Angebote sehr verlockend klingen, um wahr zu sein, sollte man besonders vorsichtig sein.

Löschen Sie Nachrichten ungelesen die über Gewinnbeteiligungen, Geldversprechen usw. informieren.

Umsonst gibt es nichts – auch nicht im Internet!

VORSICHT BEI DER NUTZUNG VON FREMDEN INHALTEN

Fremde Fotos, Musik, Videos sind meist urheberrechtlich geschützt. Sollten Sie diese auf der eigenen Website verwenden wollen, holen Sie sich die Erlaubnis schriftlich ein.

ACHTUNG!

Seit dem 25. Mai 2018 gilt die neue DATENSCHUTZ-GRUNDVERORDNUNG (DSGVO). Diese ist besonders streng im Umgang mit der Veröffentlichung von Personen und deren Daten.

DAS INTERNET VERGISST NICHTS

Seien Sie vorsichtig, was Sie im Internet über sich usw. veröffentlichen. Fotos und Statusmeldungen usw. können da schon ein Problem werden. Posten Sie niemals, dass Sie z.B. auf Urlaub sind. Dies könnte manche Kriminelle animieren, dass Sie bei Ihnen zu Hause einbrechen.

KOSTENLOSE SOFTWARE

Seien Sie bei kostenloser Software sehr vorsichtig. Laden sie kostenlose Software nur von offiziellen Seiten der Hersteller herunter.

VORSICHT BEI ABO-FALLEN

Es wird mit kostenlosen Probe-Abonnements gelockt. Wo gratis oder kostenlos draufsteht ist meistens nicht drinnen.

Wenn Abonnements (kostenlos) zur Probe abgeschlossen werden, ist entscheidend wie es nach der Probezeit dann weitergeht. In den meisten Fällen muss man als Kunde aktiv werden und selbst kündigen. Seien Sie sehr vorsichtig mit „tollen“ Aboangeboten.

PHISHING-MAILS

Die beliebtesten Attacken der Hacker sind in der heutigen Zeit nicht mehr die Arten der Malware. Entsprechend der Entwicklungen der heutigen Zeit lassen sich immer mehr Cyberkriminelle Möglichkeiten einfallen, wie sie auf die sensibelsten Daten von Benutzern zugreifen können.

Besonders beliebt sind dabei die sogenannten Phishing Mails geworden, bei denen die Benutzer auf falsche Seiten gelockt werden, um hier z.B. ihre Benutzerdaten vom Onlinebanking einzugeben. Folgen Sie diesen Aufforderungen sind Ihre Daten in den Händen von Kriminellen, die dann Zugriff auf Ihre Bankdaten haben.

ACHTUNG: Diese Mails sind meist im selben Design geschrieben, welches auch Ihre Bank nutzt und sind schwer zu erkennen bzw. zu unterscheiden.

Es gibt aber gewisse Dinge, bei denen man vorsichtig werden sollte und an denen Sie die Phishing E-Mails erkennen können:

- Ihre Bank- oder Kreditkarte sei abgelaufen oder gesperrt und Sie sollen über einen Link eine neue bestellen oder entsperren.
- Sie werden aufgefordert Ihr Passwort erneut zu vergeben.
- In dem Phishing E-Mails wird auch oft vor anderen Phishing E-Mails gewarnt.
- Sie erhalten Mahnungen von Anbietern, von denen Sie noch nie etwas gehört haben.

- Sie erhalten Zahlungsaufforderungen von Anbietern, bei denen Sie Kunde sind, bei denen der Betrag aber utopisch hoch ist.
- Sie sollen auf einer x-beliebigen Website Ihre Daten für Umfragen oder Gewinnspiele bestätigen.

PHISHING MAILS SOFORT LÖSCHEN

Banken oder Kreditkartenunternehmen fordern Sie NIE via E-Mail auf, Ihre Daten zu überprüfen! Löschen Sie solche Mails sofort und ungelesen.

Setzen Sie sich mit Ihrer Bank oder dem Anbieter in Verbindung.

Überprüfen Sie regelmäßig Ihre Kontoauszüge und Bewegungen am Konto!



SOZIALE NETZWERKE

Mit Leuten in Kontakt bleiben, die neuesten Fotos z.B. aus dem Urlaub teilen oder einfach mal kurz nachsehen, was sich bei Freunden und Bekannten gerade so tut.

Soziale Netzwerke bieten ihren Usern viele Möglichkeiten, das eigene Leben mit dem virtuellen „ICH“ zu verknüpfen. Damit sind aber auch sehr viele Probleme und Risiken verbunden.

- Sollen wirklich viele wissen, dass man sich auf Urlaub befindet und niemand im Haus bzw. in der Wohnung ist? Posten Sie auch keine Termine wie Konzerte und Veranstaltungen, an denen Sie teilnehmen.
- Vermeiden Sie, dass Sie über andere Personen im Netz etwas verbreiten was vielleicht gar nicht stimmt.
- Beschwerden über den Chef oder Kollegen sind sehr oft der Auslöser für Probleme am Arbeitsplatz. (Kündigung)
- Surfen Sie nie während der Arbeitszeit in sozialen Netzwerken.
- Fotos und Berichte über Partys haben im Netz nichts verloren. Es könnte ein falscher Eindruck über Sie entstehen, was wiederum Probleme am Arbeitsplatz bedeuten könnte.
- Posten Sie keine Fotos wo Sie nicht sicher sind ob Sie dies auch dürfen. Immer wieder werden aufreizende Bilder ins Netz gestellt. Solche haben dort nichts verloren.
- Achten Sie darauf, dass Gesichter unkenntlich gemacht werden, gerade bei Urlaubsfotos kann dies ein Thema sein.
- Veröffentlichen Sie keine Fotos von Ihren und anderen Kindern, dies könnte kriminelle auf den Plan rufen.

**Stellen Sie wirklich nicht alles ins Netz!
Sie ersparen sich sehr viel Ärger!**



CYBERMOBBING

Mit den aus dem Englischen kommenden Begriffen Cyber-Mobbing, auch Internet-Mobbing sowie Cyber-Stalking werden verschiedene Formen der Verleumdung, Belästigung, Bedrängung und Nötigung anderer Menschen oder Unternehmen mit Hilfe elektronischer Kommunikationsmittel über das Internet oder auch mittels Mobiltelefonen bezeichnet.

CYBERMOBBING IST MOBBING!

Es passiert täglich rund um die Uhr und überall. Nicht nur unter Jugendlichen, nicht nur an Schulen oder am Arbeitsplatz, sondern auch über sämtliche digitale Medien.

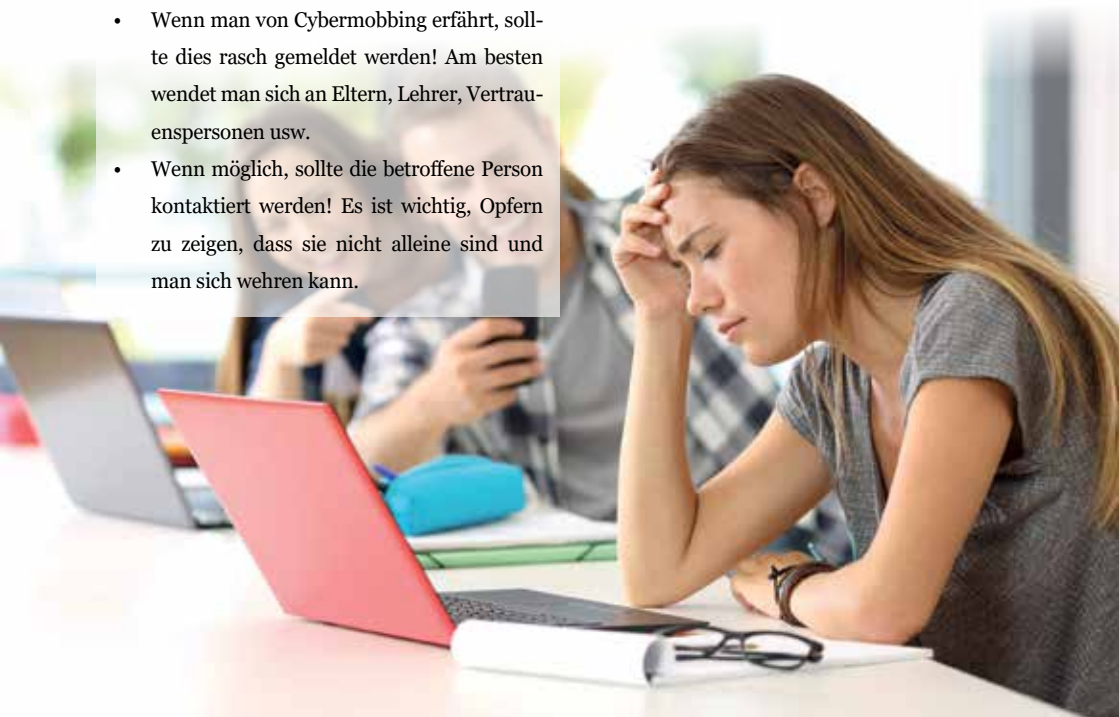
Betroffene können nicht mehr abschalten und sind sehr schnell in der Rolle des Opfers, in der sie sich selbst als Schuldigen für diese Situation sehen.

Cybermobbing kann bis hin zum Selbstmord führen.

- Wenn man von Cybermobbing erfährt, sollte dies rasch gemeldet werden! Am besten wendet man sich an Eltern, Lehrer, Vertrauenspersonen usw.
- Wenn möglich, sollte die betroffene Person kontaktiert werden! Es ist wichtig, Opfern zu zeigen, dass sie nicht alleine sind und man sich wehren kann.

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!



MALWARE

Im Allgemeinen ist Malware eine Software, die das Ziel verfolgt, auf einem anderen Computersystem unerwünschte Aktionen auszuführen um Ihnen zu schaden. Diese Programme werden oft auch als Schadprogramme und Schadsoftware bezeichnet.

Malware lauert überall – ob im Netz beim Surfen, beim Öffnen von Downloads oder auch beim Anschluss eines USB-Stick!

Eine große Gefahr ist auch kostenlose Software aus dem Internet. Dies sind nur einige Beispiele.

Was können die Ziele von Malware sein:

- Spionage
- Verbreitung von illegalen Daten (Kinderpornografie)
- Anonymisierung von illegalen Tätigkeiten
- Diebstahl von Daten (Infos über Kreditkarten, Online-Banking, usw.)

So schützen Sie sich vor Malware

- Halten Sie Ihren Computer und Ihre Software immer auf dem aktuellsten Stand.
- Überlegen Sie gut, ehe Sie auf einen Link klicken oder etwas herunterladen.
- Öffnen Sie nicht unbedacht Anhänge von Mails oder Bildern – SCHAUEN Sie genau.
- Seien Sie misstrauisch bei Pop-up-Fenstern.
- Tauschen Sie wenigen Dateien mit anderen.
- Verwenden Sie Antivirenprogramme.

Bedenken Sie: Würden Sie von jeder Person auf der Straße Schokolade annehmen und sofort essen, oder hätten Sie bedenken. Dies würde Sie sicherlich misstrauisch machen! Genau mit diesem Misstrauen sollten Sie sich auch im Netz bewegen. Keiner der Ihnen solche Mails sendet will Ihnen etwas schenken, genau das Gegenteil ist der Fall.

HILFREICHE LINKS:

www.onlinesicherheit.gv.at
www.saferinternet.at
www.ombudsmann.at

Der Internet Ombudsmann informiert auf der Informationsplattform Watchlist Internet www.watchlist-internet.at zu aktuellen Betrugsfällen und Online-Fällen. www.stopline.at ist eine Meldestelle gegen Kinderpornografie und Nationalsozialismus in Internet

SMARTPHONES

Zur Anwendung von Smartphones sei gesagt, dass auch diese wie ein PC funktionieren. Dies bedeutet, dass diese Geräte im Prinzip genau so zu schützen sind wie ein Computer.

EINIGE TIPPS ZUR SICHERHEIT VON SMARTPHONES

Bildschirm sperren

Um das Smartphone zumindest vor schnellem unbefugtem Zugriff zu schützen, sollten Sie eine Displaysperre verwenden.

Daten verschlüsseln

Sensible Daten sollten deshalb immer verschlüsselt werden. Viele Smartphones bieten eine entsprechende Funktion in den Bordmitteln, die jedoch erst aktiviert werden muss.

Updates laden & installieren

Nicht nur das Betriebssystem, auch Apps sollten Sie immer auf dem aktuellsten Stand halten.

Apps aus sicherer Quelle

Installieren Sie Apps nur aus vertrauenswürdigen Quellen, denn hier sorgen die Betreiber für einen Mindeststandard an Sicherheit. Dennoch sollten Sie sich vor dem Download über die App informieren, Bewertungen lesen und die Zugriffsberechtigungen prüfen.

Regelmäßige Backups

Damit die auf dem Smartphone gespeicherten Daten nicht verloren gehen, sollten sie regelmäßig gesichert werden. Am komfortabelsten ist die automatische Sicherung: Dabei werden alle Daten in der Cloud gespeichert und können bei Bedarf abgerufen werden.

Funkschnittstellen abschalten

Schalten Sie drahtlose Schnittstellen wie WLAN oder Bluetooth nur bei Bedarf ein – dann ist das Smartphone weniger anfällig für Cyber-Angriffe.

Handyortung aktivieren

Mittels Standortermittlung ist es möglich, das Smartphone über das integrierte GPS-Modul zu lokalisieren. Geht das Mobilgerät verloren oder es wird gestohlen, lässt sich dessen Standort auf einer Karte anzeigen.

Vorsicht vor fremden WLANs

Um den Datenverbrauch des Smartphones zu senken, bieten sich öffentliche Hotspots an. Doch Vorsicht: Alle übermittelten Daten können vom Betreiber des Funknetzwerkes ausgelesen werden, vor allem dann, wenn der Zugang unverschlüsselt erfolgt. Deshalb sollten Sie sensible Webseiten, bei denen Sie ein Passwort eingeben müssen (beispielsweise beim Onlinebanking), nie über ein öffentliches WLAN aufrufen.

Anonym surfen

Der Incognito-Modus des Browsers hilft dabei, beim Surfen keine Spuren im Internet zu hinterlassen. Suchabfragen, Browserverläufe etc. werden nicht gespeichert und sind damit für andere Personen nicht nachvollziehbar

SEXTING

Unter Sexting versteht man den „privaten Austausch“ selbst produzierter erotischer Fotos per Handy oder Internet. Eine große Gefahr von Sexting ist das Ende einer Beziehung. Endet eine Beziehung im Streit, können solche Fotos sehr gefährlich werden. Sehr werden dann häufig dann im Internet (Pornoseiten) usw. verbreitet.

Dabei kann ein versendetes Bikinifoto oder ein „oben ohne Sixpack-Bild“ ebenso als Sexting durchgehen wie ein Bild, auf dem sich ein Mädchen mit tiefem Ausschnitt in lasziver Pose oder gar oben ohne zeigt. Sind solche Bilder einmal in Umlauf gebracht, besteht jedenfalls so gut wie keine Möglichkeit mehr, deren Verbreitung zu stoppen.

Was viele nicht wissen: Das Verbreiten und Veröffentlichen erotischer Fotos Minderjähriger gilt als Kinderpornografie und ist somit illegal.

Gerade bei jungen Menschen spielt die Selbstdarstellung im Internet eine große Rolle. Jugendliche zeigen sich oft in sehr auffälligen Fotos.

Dadurch kann man sich in eine sehr große Gefahr bringen! Reden Sie mit Ihren Kinder darüber und weisen sie darauf hin, dass es kein „Safer Sexting“ gibt. Sehr schnell kann man dann Opfer von einer Erpressung werden.

In so einem Fall sollte man sofort Kontakt mit der Polizei aufnehmen auf gar keinen Fall auf die Forderungen der Täter eingehen.

Gerade hier gilt: DAS INTERNET VERGISST NICHTS!!!



KINDER IM INTERNET

Das Internet ist eben nicht mehr wegzudenken. Auch bei den Kindern hat es seinen Einzug gehalten. Daher ist es besonders wichtig, dass Kinder einen sehr verantwortungsbewussten Umgang mit diesem Medium lernen und immer misstrauisch bleiben.

Meiden Sie in den ersten beiden Lebensjahren des Kindes den Umgang mit digitalen Medien. Achten Sie darauf, dass Ihr Kind immer nur altersgerechte Websites besucht. Lassen Sie Ihr Kind nicht alleine im Internet surfen. Digitale Medien sind eben keine Babysitter oder Aufsichtspersonen. Die Gefahr durch Suchmaschinen auf nicht altersgerechte und verbotene Seiten zu kommen ist sehr groß.

BEDENKEN SIE:

Nur SIE entscheiden wie und wie viel Ihr Kind im Internet surft und welche Seiten besucht werden. Sie können Filterprogramme einrichten, um ein gefahrloses Surfen zu unterstützen. Eine 100%ige Sicherheit ist dies aber auch nicht. Weisen Sie Ihr Kind auch auf die Gefahren in der Kommunikation mit Freunden (Chats usw.) hin. Ihr Kind muss lernen, dass das Internet viel Interessantes bietet. Lernen Sie ihm einen vertrauten Umgang mit diesem Medium. Hier ist ein gegenseitiges Vertrauen Eltern und Kind sehr wichtig.



Kindern müssen den richtigen Umgang mit dem Internet erlernen

GEFAHR FÜR DIE PRIVATSPHÄRE

Internet der Dinge - Internet of Things

Der Begriff “Internet of Things” (übersetzt: “Internet der Dinge”) bezeichnet die zunehmende Vernetzung zwischen “intelligenten” Gegenständen. Verschiedene Objekte, Alltagsgegenstände oder Maschinen werden dabei mit Prozessoren und eingebetteten Sensoren ausgestattet, sodass sie in der Lage sind, via IP-Netz miteinander zu kommunizieren. (Autos, Kühlschränke, ...)

Durch die Verbindung mit dem Internet sind die smarten Geräte in der Lage, selbstständig zu agieren, sich Situationen anzupassen und auf bestimmte Szenarien zu reagieren.

Das stellt einen großen Unterschied zum Internet und dem Computer als Endgerät dar!

Eine große Gefahr des Internet of Things ist und bleibt die Datensicherheit. Durch die große Vielzahl an miteinander vernetzten Geräten z.B. im Haushalt steigt auch die Gefahr für Hackerangriffe bzw. können Sie von Kriminellen überwacht werden ob sie zu Hause sind oder nicht.

VERNETZTE SPIELZEUGE

Über vernetzte Spielzeuge können Fremde in die Kinderzimmer eindringen. Diese Spielzeuge stellen ein sehr großes Sicherheitsrisiko dar. Diese Spielwaren sind z.B. mit dem Handy oder Tablet vernetzt. Vielfach verfügen sie auch noch über Kameras und Mikrofone. Sprachdaten könnten so z.B. übertragen werden. Durch diese Verbindungen zu Servern ist es möglich, dass sich Kriminelle Zugang zu Daten verschaffen und so Sie und Ihre Umgebung ausspionieren.

Die Gefahr besteht darin, dass Kinder vieles über sich preisgeben, bzw. auch Kriminelle z.B. in das Haus (die Wohnung) lassen.

Es ist daher besonders wichtig, dass auf dem Spielzeug eine Verschlüsselungs-Software läuft und Passwörter eingerichtet werden müssen. Informieren Sie sich darüber ob dieses bestimmte Spielzeug erlaubt oder verboten ist.



RANSOMWARE

Ransomware auch als Erpressungstrojaner, Erpressungssoftware, Kryptotrojaner oder Verschlüsselungstrojaner bekannt

Ransomware auch Erpressungstrojaner, Erpressungssoftware, Kryptotrojaner oder Verschlüsselungstrojaner, sind Schadprogramme, mit deren Hilfe ein Eindringling den Zugriff des Computerinhabers auf Daten, deren Nutzung oder auf das ganze Computersystem verhindern kann. Dabei werden private Daten auf dem fremden Computer verschlüsselt oder der Zugriff auf sie verhindert, um für die Entschlüsselung oder Freigabe ein Lösegeld zu fordern.

Grundsätzlich kommen als Ziel alle Dateien in Frage, die für den Besitzer des Computers sehr wichtig und unwiederbringlich sind, wozu u. a. auch E-Mails, Datenbanken, Archive und Fotos zählen können. Diese Dateien werden nun so verschlüsselt, dass der Benutzer keinen Zugriff auf ihre Inhalte mehr hat.

Um wieder Zugriff auf die von der Ransomware verschlüsselten Daten zu erhalten, wird der geschädigte Benutzer von dem Eindringling aufgefordert, eine E-Mail an eine bestimmte E-Mail-Adresse zu senden, eine Webseite aufzurufen oder eine Formularmaske auszufüllen.

Bevor Sie Antworten oder Lösegeld bezahlen wenden Sie sich sofort an die Polizei, nur diese kann Ihnen professionelle Hilfe anbieten.

BEDENKEN SIE:

In so einem Fall sind Sie in Kontakt mit Kriminellen und da kann man absolut kein Vertrauen haben, dass Sie z.B. Ihre Daten wieder erhalten.

Tipps:

- Wichtige Daten sollten in regelmäßigen Abständen auf externen Datenträger gesichert werden, damit Kriminelle keinen Zugriff haben.
- Achten Sie darauf, dass die Anti-Viren-Software immer aktuell ist.
- Ständige Aktualisierung des verwendeten Betriebssystems und Webbrowsers.
- E-Mail-Anhängen sollte grundsätzlich Misstrauen entgegengebracht werden. Dies gilt für bekannte und unbekannte Absender, da die Absenderadresse gefälscht werden kann. E-Mail-Anhänge sollten nur geöffnet werden, wenn die Kombination aus Absender und Inhalt ein sehr hohes Maß an Plausibilität innehat, beispielsweise also erwartet wurde.
- Vermeiden der Anmeldung und Arbeit mit Administrator-Rechten.

... bedenken Sie...

Schweigen hilft Ihnen nicht weiter. Gehen Sie zur Polizei!

CYBER-GROOMING

Schutz vor (Cyber-)Grooming

WAS IST GROOMING?

Bei Grooming handelt es sich um das gezielte Ansprechen von Kindern, um sexuelle Kontakte anzubahnen. Kinder und Jugendliche fühlen sich in Chatträumen im Internet oft anonym und sicher. Doch immer öfter werden sie Opfer von „Cybergrooming“, der gezielten Anmache im Netz. Die Täter sind meist ältere Männer, die sich in der virtuellen Welt das Vertrauen ihrer Opfer erschleichen - nicht selten mit dem Ziel, das Opfer zu treffen und zu missbrauchen.

Anbahnung durch fremde Personen:

- Auf bekannten, vertrauten Strecken sollte Ihr Kind „Rettungsinseln“ kennen, wie z.B. Geschäfte oder Lokale.
- Das Kind sollte Erwachsene um Hilfe bitten, wenn es ein Gefühl von Angst verspürt.
- Das Kind sollte keine Auskünfte an Fremde geben - weder persönlich noch am Telefon oder im Internet.
- Ihr Kind sollte fremden Personen nicht die Wohnungstür öffnen, nicht mit ihnen mitgehen und sich nichts von ihnen versprechen lassen.

Das Bundeskriminalamt empfiehlt:

- Kinder und Jugendliche sollten darauf vorbereitet werden, dass der Gesprächspartner im Internet oft nicht der ist, für den er sich ausgibt. Erklären Sie ihnen, dass sie diesen Umstand in Chatträumen und in sozialen Netzwerken stets bedenken sollten. Niemand weiß, wer sich hinter den Benutzernamen, wie z.B. „cool15“ oder „sportlich16“ versteckt.
- Interessieren Sie sich für die neuen Medien und erläutern Sie Ihrem Kind, wie „soziale Netzwerke“, Chatträume usw. funktionieren. Besprechen Sie mit Ihrem Kind das Verhalten im Internet. Wo liegen mögliche Gefahren?
- Informieren Sie sich über die Technik und Umgangsweise in Chatträumen, damit Sie mitreden und Fragen stellen können. Auf diese Weise gelten Sie für ihre Kinder viel eher als Ansprechperson.
- Diskutieren Sie darüber, welche Bilder ins Netz gestellt werden. Erotische Fotos können Auslöser für Grooming, Cybermobbing oder Erpressung sein!
- Üben Sie mit Ihrem Kind konkrete Möglichkeiten, wie es sich vor sexueller Belästigung über das Internet schützen kann. Verbale sexuelle Belästigung sollen Kinder und Jugendliche mit einem klaren Nein beenden.

- Überprüfen Sie die Sicherheitseinstellungen Ihres Computers. Auch Virenschutzprogramme bieten keinen hundertprozentigen Schutz.
- Mädchen und Burschen sollten wissen, welches Verhalten das Risiko einer sexuellen Ausbeutung erhöht und was sie auf jeden Fall unterlassen sollten - wie etwa Informationen über die eigene Identität zu geben, erotische Fotos zu veröffentlichen und sich mit nicht persönlich bekannten Chatfreunden ohne Begleitung von Erwachsenen zu treffen.

BEDENKEN SIE:

Weitere Information erhalten Sie in der nächsten Polizeiinspektion, auf der Homepage www.bmi.gv.at/praevention und auch per BMI-Sicherheitsapp.

Die Spezialisten der Kriminalprävention stehen Ihnen kostenlos und österreichweit unter der Telefonnummer 059133 zur Verfügung.

Gesetzliche Lage:

§ 208a StGB Anbahnung von Sexualkontakten zu Unmündigen

(1) Wer einer unmündigen Person in der Absicht, an ihr eine strafbare Handlung nach den §§ 201 bis 207a Abs. 1 Z 1 zu begehen

1. im Wege einer Telekommunikation, unter Verwendung eines Computersystems oder

2. auf sonstige Art unter Täuschung über seine Absicht ein persönliches Treffen vorschlägt oder ein solches mit ihr vereinbart und eine konkrete Vorbereitungs-handlung zur Durchführung des persönlichen Treffens mit dieser Person setzt, ist mit Freiheitsstrafe bis zu zwei Jahren zu bestrafen.
(Auszug aus dem Strafgesetzbuch)



HTTPS VS. HTTP

Für solche Zwecke existiert darum ein dem HTTP verwandtes Protokoll, das HTTPS. HTTPS steht für „Hypertext Transfer Protocol Secure“. „Secure“, also sicher, ist HTTPS wegen einem bedeutenden Unterschied zu normalem HTTP. Alle Daten werden nämlich verschlüsselt an den jeweils anderen Computer gesendet.

Ein weiteres Problem bei sicheren HTTPS-Verbindungen ist, dass diese auch vorgetäuscht werden können. Durch geeignete Programmiertechniken, welche durchaus allesamt im Bereich üblicher Programmierkenntnisse liegen, lassen sich Teile des Browserfensters nachbilden. So kann zum Beispiel auch das „Schlosssymbol“ in der Statuszeile des Browsers sowie das „https“ am Anfang der Adresszeile gefälscht werden.



SPAM

Stop dem SPAM

Als SPAM oder JUNK (aus dem englischen für „Müll“) werden unerwünschte Nachrichten bezeichnet, die jemand auf elektronischem Wege zugestellt werden.

Diese „Nachrichten“ verursachen an Ihrem PC einen erheblichen Schaden.

Auch hier gilt: Achten Sie auf Ihre Passwörter, Browsereinstellungen, geben Sie Ihre E-Mail Adresse nicht immer und überall an, Antworten sie nicht auf solche Nachrichten, ...



HILFE & UNTERSTÜTZUNG

Die Bekämpfung von Internetkriminalität ist ein Schwerpunkt der kriminalpolizeilichen Arbeit. Dazu wurde eigens eine Meldestelle eingerichtet, die Ihnen rund um die Uhr Auskunft gibt. Wenn Sie einen Verdacht auf Internetkriminalität haben und über die weitere Vorgangsweise Informationen benötigen, wenden Sie sich bitte an das Bundeskriminalamt:

MELDESTELLE FÜR INTERNETKRIMINALITÄT.

E-Mail: against-cybercrime@bmi.gv.at

<https://www.watchlist-internet.at>

<https://www.onlinesicherheit.gv.at>

<https://ombudsmann.at>

Kindersextourismus

Wenn Sie auf einer Web-Seite oder in einer „News-Group“ Texte oder Bilder entdecken, die Kinderpornografie enthalten, oder wenn auf einer Seite Sextourismus mit Kindern angeboten wird, melden Sie bitte den Fund an folgende Stelle:

MELDESTELLE KINDERPORNOGRAPHIE UND SEXTOURISMUS MIT KINDERN

Telefax: +43-(0)1-24836-951310

E-Mail: meldestelle@interpol.at





Österreichischer Zivilschutzverband - Bundesverband
Spiegelgasse 6/13, 1010 Wien
office@zivilschutzverband.at
Tel. 01/5339323

www.zivilschutzverband.at
www.siz.cc

ADRESSEN UND TELEFONNUMMERN DER LANDESVERBÄNDE:



Burgenländischer Zivilschutzverband

Hartlsteig 2, 7000 Eisenstadt
Tel. 02682/63 62 0
Mail: office@bzsv.at
Web: www.bzsv.at

Kärntner Zivilschutzverband

Haus der Sicherheit
Rosenegger Straße 20, 9020 Klagenfurt
Tel. 050/536 570 80
Fax: 050/536 570 81
Mail: zivilschutzverband@ktn.gv.at
Web: www.siz.cc/kaernten

Niederösterreichischer Zivilschutzverband

Langenlebarner Straße 106, 3430 Tulln
Tel. 02272/61 820
Fax: 02272/61 820 13
Mail: noezsv@noezsv.at
Web: www.noezsv.at

Oberösterreichischer Zivilschutzverband

Petzoldstraße 41, 4020 Linz
Tel. 0732/65 24 36
Mail: office@zivilschutz-ooe.at
Web: www.zivilschutz-ooe.at

Salzburger Zivilschutzverband

Karolingerstraße 32, 5020 Salzburg
Tel. 0662/83 999
Fax: 0662/83 999 20
Mail: office@szsv.at
Web: www.szsv.at

Steirischer Zivilschutzverband

Florianistraße 24, 8403 Lebring
Tel. 03182/7000 733
Fax: 03182/7000 730
Mail: zivilschutz.office@stzsv.at
Web: www.zivilschutz.steiermark.at

Tiroler Zivilschutzverband

Eduard-Wallnöfer-Platz 3, 6020 Innsbruck
Tel. 0512/508 2262
Fax: 0512/508 2265
Mail: katschutz@tirol.gv.at
Web: www.siz.cc/tirol

Vorarlberger Zivilschutzverband

Landhaus, Römerstraße 15, 6900 Bregenz
Tel. 05574/511 211 60
Fax: 05574/511 211 65
Mail: zivilschutz@vorarlberg.at
Web: www.siz.cc/vorarlberg

Die Helfer Wiens

Selbstschutz - Zivilschutz
Hermannsgasse 24, 1070 Wien
Tel. 01/522 33 44
Fax: 01/522 33 44 5
Mail: office@diehelferwiens.at
Web: www.diehelferwiens.at

