



INTERNET SICHERHEIT

Worauf sollte beim
Surfen und Chatten
geachtet werden.



www.zivilschutz.steiermark.at

Klar ist, dass das Internet nicht mehr aus unserem Leben wegzudenken ist. Es hat unsere Gesellschaft grundlegend verändert, vom Beruf, Schule bis zur Familie, da immer mehr Menschen das Internet auch über das Smartphone und Tablet nutzen.

- Weltbevölkerung 7,8 Mrd.

- Internetseiten ca. 1,8 Mrd.

- Google 100 Mrd. Suchanfragen pro Monat

- Internet 4,54 Mrd. Nutzer

- Whatsapp 1,6 Mrd. Nutzer

- Facebook 2,449 Mrd. Nutzer

- Youtube 1,9 Mrd. Nutzer

- 145 Millionen Leute twittern täglich

- Auf Instagram gibt es monatlich 1 Mrd.

aktive Nutzer wobei täglich 95 Mio Fotos verschickt werden

- Über Facebook, Messenger und WhatsApp werden täglich 60 Mrd. Nachrichten verschickt



Das Internet wird heute von rund 88% der ÖsterreicherInnen ab dem 14. Lebensjahr genutzt. Durchschnittlich verbringen die ÖsterreicherInnen 118 Minuten an einem normalen Wochentag im Internet. Die Mehrheit verwendet das Internet hauptsächlich zum Senden und Empfangen von E-Mails sowie zur Nutzung von Suchmaschinen und zum Austausch via Messenger. Im Jahr 2019 dominierte WhatsApp vor Facebook das Ranking der beliebtesten Messenger. Skype, Snapchat oder Telegram werden deutlich weniger genutzt.

Im August 2019 erfolgte 71% der Internet-Nutzung in Österreich mit Endgeräten, die mit einem mobilen Betriebssystem ausgestattet sind. 20% der Internetnutzer konsumieren täglich Videos via Computer. Die bekanntesten Plattformen sind Amazon Prime, Netflix und YouTube.

4,4 Millionen Internet-User in Österreich nutzen Social Media Plattformen. Deutlicher Sieger dabei ist Facebook mit einem Marktanteil von über 76% (2020).

Internetkriminalität (Cybercrime) ist mittlerweile eine große Herausforderung und weist in der Kriminalstatistik ein sehr starkes Wachstum auf.

Spam
Phishing
Social Engineering
Datendiebstahl
DDoS
Cybercrime
Onlinebetrug
Cyberstalking
Viren
Hacking
Ransomware
Romance Scam
Trojaner

Größte Deliktsgruppe sind Onlinebetrügereien

Der Großteil, $\frac{1}{3}$ der Anzeigen im Zusammenhang mit Cyberkriminalität, entfällt auf Betrügereien. Bei den angezeigten Delikten handelt es sich vor allem um Gewinnspiele, Onlineshopping oder Anlage- und Liebesbetrügereien.

Zunahme von Hackerangriffen durch Datenlecks

Beim klassischem „Hacking“, also Angriff auf Daten oder Computersysteme, verdoppeln sich die Zahlen jährlich. Diese starke Zunahme ist auf die zahlreichen Datenlecks zurückzuführen, bei denen Hacker Zugangsdaten erbeuten und diese dann im Darknet verkaufen.

Drogen- und Falschgeldhandel wandern ins Darknet

Beim Darknet handelt es sich um einen verborgenen Teil des Internets, der nur mit Anonymisierungsdiensten wie TOR zugänglich ist und von Suchmaschinen nicht erfasst wird. Auch mit Kinderpornografie, Kreditkartendaten oder gefälschten Dokumenten und Schadsoftware wird im Darknet gehandelt.

Was ist ein BotNet?

Ein Botnet ist eine Gruppe automatisierter Schadprogramme, sogenannter Bots. Bots kann man sich als kleine Roboter (Programme) mit 2 Aufgaben vorstellen:

1. Selbständige und unbemerkte Verbreitung auf weltweite Computer und IT Komponenten (z.B. Fernseher).
2. Zeitliche oder ferngesteuerte Aktivierung einer Schadsoftware mit dem Zweck, das Angriffsziel (z.B. Server einer Regierung, Bank usw.) gänzlich lahmzulegen.

Distributed Denial of Service (DDoS):

Denial of Service (DoS; engl. für „Verweigerung des Dienstes“) bezeichnet in der Informationstechnik die Nichtverfügbarkeit eines Internetdienstes, der eigentlich verfügbar sein sollte. Obwohl es verschiedene Gründe für die Nichtverfügbarkeit geben kann, ist die häufigste Art die Folge einer Überlastung des Datennetzes. Dies kann durch einen konzentrierten Angriff auf die Server oder sonstige Komponenten des Datennetzes erreicht werden.

Im Fall einer durch eine Unmenge von Anfragen verursachten Dienstblockade spricht man von einer durch Vielanfragen verbreiteten Verweigerung des Dienstes (engl. Distributed Denial of Service; DDoS).



FAKKE NEWS

Hoax

Als Hoax (engl. für Jux, Scherz, Schabernack; auch Schwindel) wird heute meist eine Falschmeldung bezeichnet, die in Büchern, Zeitschriften oder Zeitungen, per E-Mail, Instant Messenger oder auf anderen Wegen (z. B. SMS, MMS oder auf den sozialen Netzwerke) verbreitet, von vielen für wahr gehalten und daher an Freunde, Kollegen, Verwandte und andere Personen weitergeleitet wird.

Wie erkennt man einen Hoax?

Eigentlich ist es ganz einfach: Vor dem Teilen kurz nachdenken. Denn wer glaubt wirklich daran, dass er mit einem einzigen Posting ein Luxusauto gewinnen kann? Oder, dass eine in einem Glas eingesperrte Katze tatsächlich überleben kann? Oder, dass ein Migrant „einfach so“ viele tausend Euro bekommt? Niemand! Genau! Und doch wird dieser Unsinn tausendfach geteilt.

Social Engineering

Social Engineering („soziale Manipulation“) nennt man zwischenmenschliche Beeinflussungen mit dem Ziel, bei Personen bestimmte Verhaltensweisen hervorzurufen, sie zum Beispiel zur Preisgabe von vertraulichen Informationen (Passwörter), zum Kauf eines Produktes oder zur Freigabe von Finanzmitteln zu bewegen. Social Engineers spionieren das persönliche Umfeld ihres Opfers aus, täuschen Identitäten vor oder nutzen Verhaltensweisen wie Autoritätshörigkeit aus, um geheime Informationen zu erlangen. Häufig dient Social Engineering dem Eindringen in ein fremdes Computersystem, um vertrauliche Daten einzusehen.

Phishing

Unter dem Begriff Phishing (Neologismus von fishing, engl. für ‚Angeln‘) versteht man Versuche, über gefälschte Webseiten, E-Mails oder Kurznachrichten an persönliche Daten eines Internetbenutzers zu gelangen und damit Identitätsdiebstahl durchzuführen.

Ziel des Betrugs ist es, mit den erhaltenen Daten beispielsweise Kontoplünderung zu begehen und den entsprechenden Personen zu schaden.

Die Schreibweise mit „Ph-“ entstammt dem Hacker-Jargon Phishing-Webseite: Sie sieht aus wie die Seite eines Geldinstitutes, ist jedoch eine vom Phisher präparierte Webseite. Der Klick auf die Schaltfläche in der Mitte würde den nichts ahnenden Besucher auffordern, persönliche Daten einzugeben, die der Phisher dann abfängt. Typisch ist dabei die Nachahmung des Internetauftritts einer vertrauenswürdigen Stelle, etwa der Internetseite einer Bank. Um keinen Verdacht zu erregen, wird das Corporate Design der betroffenen Stelle nachgeahmt, so werden etwa dieselben Firmenlogos, Schriftarten und Layouts verwendet.

Der Benutzer wird dann auf einer solchen gefälschten Seite etwa dazu aufgefordert, in ein Formular die Login-Daten oder auch Transaktionsnummern für sein Onlinebanking einzugeben. Diese Daten werden dann an den Betrüger weitergeleitet und dazu missbraucht, das Konto zu plündern.



A screenshot of a phishing website for 'easybank'. The page has a green header with the 'easybank' logo and a language dropdown set to 'deutsch'. The date 'Donnerstag, 02.04.2020 - 15:16' is in the top right. The main content area is divided into several sections: 1. 'Login mit Zugangsdaten' with a form for 'Vorlegernummer' (containing '58924709') and 'PIN', and a 'Login' button. 2. 'Warnung' with a red triangle icon and text: 'März 2020 bzgl. Phishing: Die easybank fordert Sie niemals per E-Mail auf, Zahlw., Telefontexte, Konto- oder Kreditkartendaten anzugeben bzw. zu bestätigen! Weitere Informationen...'. 3. 'Hilfe/Hotline' with a list: 'PIN vergessen?', 'Vorleger gesperrt?', '05 70 09-500', 'Mo-Fr 08:00-18:00 Uhr'. 4. 'Info' with a list: 'Bestellung PIN-Code für Bankomatkarte', 'Die neue easybank App ist da!'. At the bottom, there is a 'COVID-19: Achtung vor Phishing' notice: 'Wir fordern Sie niemals per E-Mail oder SMS auf, über einen direkten Link in Ihr e-banking einzusteigen.' and a red circular badge that says 'Aktuelle Phishing-Warnung'. The footer contains 'Impressum', 'AGB', 'Datenschutz', 'Nutzungsbedingungen', 'Betreiber', '© BAWAG P.S.K.', and social media icons.

Scamming

Scamming heißt frei übersetzt „betrügen“ und wird von zahlreichen Internet-Gaunern fabriziert. Scammer haben das primäre Ziel, Sie um Ihr Geld zu erleichtern.

Es gibt viele verschiedene Formen von Scamming. (Sex -Scamming, Scamming auf dem Wohnungsmarkt, Scamming mit falschen Geldversprechen). Eine der am weitesten verbreiteten Form ist das „Romance-Scamming“.

Das ist eine Betrugsmasche, die auf Dating-Portalen, in Foren und auf anderen Chat-Portalen angewendet wird. Dem Opfer wird über einen längeren Zeitraum hinweg vorgegaukelt, dass es für den Scammer das liebenswerteste Lebewesen auf der Erde sei. Das ist allerdings nur bis zu dem Zeitpunkt schön, bis der Scammer Geld von Ihnen möchte. Über diesen Zeitraum hinweg ist oftmals bereits eine emotionale Abhängigkeit entstanden und die Opfer fühlen sich dazu verpflichtet, dem Scammer Geld zu überweisen. Meistens befinden sich die Betrüger im Ausland und wollen Geld für ein Flugticket, eine Operation für das eigene Kind oder für andere ausgedachte Unterfangen.

Das Geld ist überwiesen und dem Opfer wird versprochen, dass es das Geld in naher Zukunft zurück bekommt - doch dem ist nicht so. Sobald der Scammer das Geld hat, ist er und das Geld weg oder verlangt sogar zu einem späteren Zeitpunkt noch eine weitere Summe.



Kinder nutzen das Internet immer früher!

- In Österreich liegt der Durchschnitt bei 10 Jahren!
- 40% der 3 - 6 Jährigen in Österreich nutzen das Internet regelmäßig!

Cybermobbing

Cybermobbing ist jegliche Form wiederholter, verbaler, psychischer oder körperlicher Belästigung durch einzelne oder mehrere Personen z.B. durch Beleidigen, Bedrohen, Bloßstellen oder Belästigen.

Unterschiede zu normalem Mobbing: 24 Stunden – keine „Schutzzonen“, keine Pausenzeiten.

Cybermobbing Selbsttest (Wer kennt diese 6 Begriffe?)



Bullying

Unter Bullying (Mobbing in der Schule) versteht man ein gegen Schüler gerichtetes Drangsalieren, Gemeinsein, Ärgern, Angreifen und Schikanieren – auch und im Besonderen ONLINE – ohne Schutzzone und Pausen. 24 Stunden am Tag!



Smack Cam

Das Phänomen SMACK CAM ist als Trend unter Jugendlichen schon länger bekannt. Dabei werden gewalttätige Angriffe auf Personen mit dem Handy mitgefilmt und anschließend in den sozialen Medien verbreitet. Was aus Spaß mit gestellten Szenen begann, ist längst realen Gewalttaten gewichen. Mittlerweile gibt es viele Smack Cam Videos, bei denen weder Opfer noch Zuschauer viel zu lachen haben. Doch je echter und brutaler die Szene ist, desto höher die Klickzahlen, desto größer der Hype. Ein Faustschlag für mehr Aufmerksamkeit!

Posing

„Aufreizende Selbstdarstellung“: Werden für das Profil im Sozialen Netzwerk Bilder erstellt, probieren Kinder und Jugendliche gerne vor dem Spiegel unterschiedlichste Posen aus, bis ein optimales Foto mittels Handy-Kamera entstanden ist. Viele Kinder und Jugendliche ahmen bei diesen Bildern ihre Idole auf YouTube, Instagram & Co. zwischen Darstellungen aus der Popmusik nach und bilden sich entsprechend aufreizend ab. Sehr oft sind sie auf solchen Fotos leicht bekleidet (Mädchen z. B. im „Spaghetti-Leibchen“, Burschen „oben ohne“). Die Kinder und Jugendlichen nutzen dazu alle Möglichkeiten der Kamera – von Filtereffekten bis hin zu besonderen Einstellungen – und leben dabei ihre Kreativität aus.

Häufig wird vergessen, dass aufreizende Bilder, die als Profildaten in Sozialen Netzwerken dienen, von einer größeren Öffentlichkeit gesehen werden und oft in weiterer Folge die Basis für „Grooming“ sind.



Sexting

Sexting (engl. für das Senden von erotischen Bildern) – ist heute unter Jugendlichen weit verbreitet und gehört für viele zum Flirten oder zur Beziehungspflege einfach dazu. Immer mehr Jugendliche machen von sich selbst erotische Fotos bzw. Nacktaufnahmen und versenden diese per Handy an Freundinnen und Freunde oder Bekannte. Oft landen die Bilder auch im Internet – z. B. in Sozialen Netzwerken oder Foto-Communitys – und werden von dort aus an ein großes Publikum verbreitet.

In vielen Fällen werden die anzüglichen Bilder vorerst „nur“ zwischen Pärchen oder besten Freundinnen und Freunden verschickt. Wenn die Beziehungen oder Freundschaften aber in die Brüche gehen, landen möglicherweise einige der Fotos aus Rache auf diversen Handys bzw. öffentlich im Web oder werden zur Erpressung verwendet.

Sind solche Bilder einmal im Umlauf, besteht so gut wie keine Möglichkeit mehr, deren Verbreitung zu stoppen. Auch wenn Fotos im Internet z. B. nur für Freundinnen und Freunde freigegeben sind, kann nicht ausgeschlossen werden, dass diese in falsche Hände geraten. So können einmal verbreitete Aufnahmen auch

Jahre später wieder auftauchen und künftigen beruflichen Karrieren und privaten Beziehungen massiv schaden.



Cyber-Grooming

Erwachsene suchen „freundschaftlichen“ Kontakt zu Kindern, um sie später sexuell zu missbrauchen. Erwachsene – in den meisten Fällen sind dies Männer – nutzen dabei zwei unterschiedliche Strategien: Entweder sie geben sich als Gleichaltrige aus und erwerben so das Vertrauen der Kinder, oder sie machen aus ihrem eigenen Alter kein Hehl und sind besonders aufmerksam und freundlich zu ihren späteren Opfern. Manche „Groomer“ geben sich auch als Modelagenten oder Talentsucher aus und versprechen den Jugendlichen, sie berühmt zu machen.

Eine beliebte Strategie der Täter ist es, den Kindern plausibel zu machen, wie „hübsch“ sie sind und dass sie sich sehr freuen würden, noch mehr so nette Bilder sehen zu können. Haben Kinder das Gefühl, dass sie in ihrer „realen“ Umgebung wenig Aufmerksamkeit oder positive Unterstützung erhalten, so können sie leicht auf diese Masche hereinfallen. Ziel der Täter ist es in der Regel, ein reales Treffen zu vereinbaren, wo es dann unter Umständen zu sexuellem Missbrauch kommen könnte. Weiters geht es Tätern immer wieder darum, aufreizende und pornografische Bilder von Minderjährigen zu erhalten und diese zu verbreiten oder für Erpressungsversuche nutzen zu können.

Sextortion

Sextortion bezeichnet eine Erpressungsmethode, bei der eine Person (oft ein Jugendlicher) mit Bild- und Videomaterial erpresst wird, dass sie nackt und/oder beim Vornehmen sexueller Handlungen (Masturbation) und/oder nackt zeigt. Der Begriff Sextortion setzt sich aus «Sex» und «Extortion» (engl. Erpressung) zusammen. Man wird später von Erpressern kontaktiert und zu einer Geldzahlung oder zu einem PERSÖNLICHEN TREFFEN (ÜbergriffsGEFAHR!) aufgefordert.

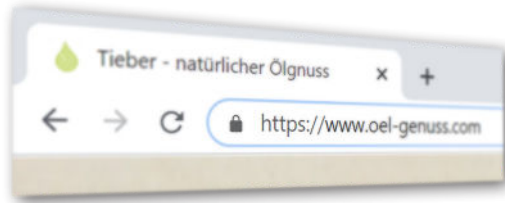
Man droht, die Aufnahmen mit Namen auf Youtube zu veröffentlichen, sie per E-Mail an Familienangehörige, Freunde oder dem Arbeitgeber zu schicken oder den Link auf Facebook zu veröffentlichen.

Hyper Text Transfer Protocol Secure (HTTPS)

HTTPS ist ein Kommunikationsprotokoll im World Wide Web, um Daten abhörsicher zu übertragen.

- <http://www.> - Keine Datenverschlüsselung implementiert
- <https://www.> - Verschlüsselte Verbindungen

In den neuen Browsern ist ein Schloss neben der Homepage zu sehen, wenn eine gesicherte Verbindung hergestellt ist.



Tipps für ihr Handy

- Das Handy sollte auf „automatisch“ sperren sein!
- Mit einem Code gesichert sein!
- Das Handy nie unbeaufsichtigt lassen!
- Regelmäßige Sicherung hilft vor Datenverlust!



Grundregeln für den Umgang mit Social Media!

- Bei jeder Äußerung auf einen angemessen, neutralen und höflichen Ton achten.
- Muss ich das wirklich posten?
- Muss das wirklich geteilt werden?
- Das Internet ist kein rechtsfreier Raum!
- Trage Streitigkeiten und Unstimmigkeiten nie online aus!
- Das Internet vergisst nicht!

Da kann ich mir Hilfe holen

<https://ombudsmann.at/>
<https://www.onlinesicherheit.gv.at/>
<https://www.watchlist-internet.at/>
<https://www.mimikama.at/>
<https://www.saferinternet.at/>

Cybercrime-Competence Center C4
against-cybercrime@bmi.gv.at



Saferinternet.at

Das Internet sicher nutzen!



Notrufnummern im Überblick

Euronotruf 112

Feuerwehr 122

Polizei 133

Rettung 144

Bergrettung 140

Landeswarnzentrale 130

Gesundheitsnummer 1450

Vergiftungsnotruf 01 406 43 43

Impressum:
Medieninhaber, Herausgeber und Verleger: Zivilschutzverband Steiermark,
Florianstraße 24, 8403 Lebring. Fotos: pixabay.com, Dipl.-Ing. Michael Tieber

Befolgen Sie bitte bei der telefonischen Alarmierung folgende Punkte:
Wer? ruft an! / **Wo?** ist was passiert! / **Was?** ist passiert! / **Wieviele?** Verletzte!



www.zivilschutz-shop.at



Zivilschutzverband Steiermark

Florianstraße 24, 8403 Lebring

Tel. 03182/7000 733

Mail: zivilschutz.office@stzsv.at

Web: <https://www.zivilschutz.steiermark.at>