KSÖ-RATGEBER

SICHER IM INTERNET

KURATORIUM SICHERES ÖSTERREICH

Tiroler Tageszeitung

AK Tirol

POLIZEI

LAND TIROL

Raiffeisen Meine Bank

Mag. Helmut Tomac
Landespolizeidirektor Tirol

Dr. Johannes Ortner
Vorstandsvorsitzender Raiffeisen-Landesbank Tirol AG

Mag. Hermann Petz
Vorstandsvorsitzender Moser Holding

Günther Platter
Landeshauptmann Tirol

Erwin Zangerl
Präsident Arbeiterkammer Tirol

SICHER DURCH DIE DIGITALE WELT

Es ist längst eine unerfreuliche Tatsache: Die digitale Kriminalität wächst rasant und stellt nicht nur uns einfache User, sondern auch Unternehmen, Institutionen und nicht zuletzt die Exekutive vor ganz neue Herausforderungen.

So wie wir als Kinder schon lernten, Haustüren zu verschließen und Geld bzw. Wertgegenstände nicht offen herumliegen zu lassen, müssen wir uns nun auch im Umgang mit unseren digitalen Devices entsprechende Verhaltensweisen antrainieren. Das fängt ganz lapidar schon bei den Passwörtern an. Wenn Sie zu den Menschen gehören, die nach wie vor die vierfache Eins oder das eigene Geburtsdatum nutzen, sollten Sie sich nach der Lektüre dieser Broschüre schleunigst ein paar Minuten ausklinken, sich ein entsprechendes System überlegen und dieses dann konsequent anwenden. Zu Ihrer eigenen Sicherheit.

Denn – wie ja auch schon unser „Niki Nazionale" einst für sich feststellte – Sie haben ja nichts zu verschenken. Schon gar nicht, was Sie sich über die Jahre hart erarbeitet und erspart haben. Schützen Sie also unbedingt Ihre Daten. Und fangen Sie nicht morgen, sondern jetzt gleich damit an. Der vorliegende Ratgeber, für den KSÖ Tirol, Arbeiterkammer Tirol, Land Tirol, Polizei, Tiroler Tageszeitung und die Tiroler Raiffeisenbanken ihr Know-how in diesem Bereich zusammengetragen haben, möge Sie dabei tatkräftig unterstützen. Der Landesklub Tirol des Kuratoriums Sicheres Österreich (KSÖ Tirol) will als Herausgeber dieser Broschüre mit seinen Aktionen und Aktivitäten rund um das Thema Sicherheit nämlich nicht nur Bewusstsein schaffen, sondern auch ganz konkrete Handlungsanweisungen geben.

Denn Wissen allein genügt nicht. Wer sich im Netz schützen will, muss auch sein Verhalten entsprechend ausrichten. In diesem Sinne wünschen wir Ihnen jetzt nicht nur eine anregende Lektüre, sondern auch das hierfür nötige Quäntchen Disziplin, um das Gelernte sofort umzusetzen.

DAS INTERNET KENNT KEINE GRENZEN

Eine sowohl positive als auch negative Eigenschaft des Internets ist, dass keine natürlichen Grenzen bestehen. Per Klick wechselt man den Ort, den Shop, das Lokal, den Blog, ja sogar Freunde.

Das bringt viel Positives mit sich. Aber auch einige negative Dinge. Dieser Ratgeber soll Ihnen helfen, bewusst mit einem unverzichtbaren Medium unserer Zeit umzugehen. Die wichtigsten Themen werden in kurzer Form von Profis beleuchtet. Tipps und Ratschläge beantworten konkrete Fragen.

Dass in diesem Ratgeber leider nicht alle Themen angesprochen werden können, liegt in der Natur der Sache. Denn wie bereits gesagt: Das Internet kennt keine Grenzen. Dieser Ratgeber ist der Versuch, die wichtigsten und vor allem aktuellsten Themen aufzugreifen.

DREI GOLDENE REGELN

Die drei goldenen Regeln der AK-Tirol-Konsumentenschützer helfen Ihnen dabei, viele Fallen, die im Internet auf Sie lauern, zu erkennen und zu vermeiden.

1 **Niemand schenkt Ihnen was. Denken Sie immer daran!**
Also immer größte Vorsicht bei „Gratis"-Versprechen oder wenn etwas angeblich „ganz, ganz billig" ist. Auch Gewinnmitteilungen kritisch betrachten, vor allem wenn Sie sich gar nicht erinnern können, irgendwo konkret mitgespielt zu haben. Jobangebote im Internet nach dem Motto „Wenig arbeiten – viel Geld verdienen" bitte niemals ernst nehmen!

2 **Wenn jemand Ihre Daten will, dann hat er einen Grund!**
Das Internet bietet viele Informationen, welche meist anonym abgerufen werden können. Vorsicht immer dann, wenn plötzlich persönliche Daten von Ihnen verlangt werden, also z. B. Name, E-Mail-Adresse, Mobilfunknummer, Wohnanschrift. Geben Sie sie nicht ein – außer Sie wissen ganz genau, wofür diese benötigt werden, und wollen das auch! Geiz ist geil, wenn's um Daten geht!

3 **100 Prozent geschützt sind nur jene Daten, die Sie nicht bekannt geben!**
„Das Internet vergisst nicht!" Selbst wenn Sie Daten (Fotos, Kommentare ...) im Internet scheinbar löschen, können diese längst irgendwo auf der Welt zigfach gespeichert sein und bleiben das auch. Unangenehm vielleicht, wenn dann nach Jahren oder gar Jahrzehnten längst vergessen Geglaubtes wieder auftaucht. Denken Sie immer daran, wenn Sie etwas ins Netz stellen wollen, und lassen Sie es im Zweifel lieber!

IMMER NOCH MEHR PASSWÖRTER!

WAS NEHMEN? WIE MERKEN?

Ohne Kenn- und Passwörter im Internet kommt niemand von uns aus. Manche haben Dutzende.

Wir brauchen sie für unseren E-Mail-Account, für diverse Webshops, in denen wir Waren einkaufen oder Dienstleistungen bestellen, für den Zugang zu diversen Social-Media-Kanälen, ja sogar einfache und freie Informationsportale verlangen manchmal schon eine Registrierung mit Kenn- und Passwort.

Hintergrund ist auch immer öfter, dass damit der Einstieg und die Verwendung durch Nutzer statistisch erfasst und angebots- oder marketingtechnisch verwertet werden können. Hier finden Sie einige Tipps rund um das Thema „Passwort“ zusammengestellt:

KONTAKT
AK Tirol, Konsumentenschutz
Kostenlose Hotline: 0800/225522-1818
www.ak-tirol.com

- **Beenden Sie für sich selbst den grassierenden Passwortwahnsinn und registrieren Sie sich bei einem neuen Portal nur dann, wenn Sie den Zugang wirklich benötigen und nutzen möchten.** Vergessen Sie nicht die goldene Regel Nr. 2: „Wenn jemand Ihre Daten will, dann hat er einen Grund!" (siehe S. 5)

- **Die Benutzerkennung ist meistens nicht mehr frei wählbar, sondern mit einer einzusetzenden E-Mail-Adresse vorgegeben.** Überlegen Sie, ob Sie vielleicht eine gesonderte E-Mail-Adresse nur für Ihre Onlinezugänge anlegen, welche Sie nur dafür und nicht für die allgemeine Kommunikation verwenden. Wenn diese E-Mail-Adresse sonst nicht bekannt gemacht wird, reduzieren Sie die Gefahr, gehackt zu werden. Natürlich muss auch dieser (neue) E-Mail-Account künftig regelmäßig auf einlangende Nachrichten kontrolliert werden.

- **Verwenden Sie unterschiedliche Passwörter für unterschiedliche Portale.** Sonst ist die Gefahr sehr groß, dass ein Hacker mit derselben Kenn-und-Passwort-Kombination viele verschiedene Zugänge mit einem Schlag kapert und sich der mögliche Schaden multipliziert.

- **Was aber ist ein gutes Passwort? Zuallererst: Geheim!** Sobald ein Passwort jemandem mitgeteilt oder gar irgendwo in einem Social-Media-Kanal oder im Web bekannt gegeben wurde, ist es nicht mehr sicher. In so einem Fall ist das Passwort sofort zu ändern – bevor es jemand anderer macht und selbst kein Zugang mehr möglich ist. Ebenso ist das Abspeichern als Datei an einem Ort, zu dem möglicherweise andere Zugriff bekommen könnten, ein Risiko. Man geht aktuell davon aus, dass Passwörter in Form von sehr langen Zeichenketten, z. B. Sätzen, die noch dazu keinen (für jeden erkennbaren) Sinn ergeben und auch Fantasiewörter beinhalten, am schwersten zu knacken sind.

- **IT-Experten bestätigen immer wieder, dass jegliche Daten, die in elektronischer Form gespeichert werden, auch entsprechend angreif- und hackbar sind.** In diesem Zusammenhang ist auch der Einsatz von sogenannten Passwortmanagern (auch Passwortsafes, Passworttresore etc. genannt), welche viele Benutzerkennung-Passwort-Kombinationen abspeichern und über ein sogenanntes Generalpasswort abrufbar machen, nicht unkritisch zu sehen. Eine einfache, nichtdigitale Erinnerungshilfe für Passwörter sind handschriftliche Notizen der Passwörter an geheimen Plätzen (z. B. am Seitenrand eines Buches), und zwar ohne weitere Hinweise, zu welchem Zugang das Passwort gehört. Das hat den Vorteil, dass niemand mit einer solchen Notiz allein etwas anfangen kann, der Accountinhaber kann sich aber im besten Fall sofort wieder erinnern, welcher Zugang damit geöffnet werden kann.

DIE WICHTIGSTEN TIPPS

- **Keine Fotos, Videos oder Texte veröffentlichen, die einem selbst oder anderen peinlich sein könnten.** Auch wenn Inhalte nur für eine kleine Nutzergruppe freigegeben sind, ist nicht auszuschließen, dass diese irgendwann in falsche Hände gelangen. Wenn man z. B. ein Foto hochlädt und das nur für seine besten Freunde freigibt, kann es sein, dass es trotzdem für viel mehr Personen sichtbar wird, wenn einer der besten Freunde z. B. „Gefällt mir" klickt oder einen Kommentar dazu schreibt. Achtung: Soziale Netzwerke werden zunehmend auch von (potenziellen) Arbeitgebern durchforstet!

- **Vorsicht bei der Angabe persönlicher Daten** (Adresse, Telefonnummer, Schule etc.), die es Fremden ermöglichen, einen auch außerhalb des Internets aufzuspüren oder zu belästigen.

- **Viele der sozialen Netzwerke bieten ihren Nutzern die Möglichkeit, Einstellungen zur Privatsphäre zu bestimmen.** Nutzen Sie diese Möglichkeit.

- **Sichere Passwörter verwenden und geheim halten – auch vor den besten Freunden!** Damit verhindert man, dass andere Zugriff auf das eigene Profil haben und im eigenen Namen Einträge veröffentlichen.

- **Unerwünschte Personen blockieren: Sollte jemand lästig werden, können Sie diese Personen direkt in der Plattform selbst blockieren und melden.** Wenn das nicht hilft, wenden Sie sich an eine Beratungsstelle für Unterstützung (z. B. rataufdraht.at, zara.or.at, stopline.at, ombudsmann.at). Vergessen Sie nicht, Beweise zu sichern, z. B. in Form von Screenshots.

- **Nehmen Sie Ihre Rolle als AdministratorIn ernst und seien Sie achtsam, wen Sie in Gruppen zusammenbringen:** So können Sie in WhatsApp beispielsweise auf diese Art Telefonnummern weitergeben, ohne dass dies die betroffenen Personen eigentlich wollen. Nehmen Sie nur Personen in eine WhatsApp-Gruppe, die sich auch sonst kennen.

- **Überlegen Sie sich, ob Sie bei jedem neuen Trend mitmachen müssen.** Löschen Sie Ihre Accounts auf Netzwerken, die Sie nicht mehr benutzen. Achtung: Das bloße Löschen der App auf dem Smartphone reicht dazu nicht.

- **Melden Sie irreführende Inhalte wie auch Fake-Accounts und verhindern Sie so, dass auch andere in die Falle tappen.** Greifen Sie ein, wenn Sie sehen, wie andere online fertiggemacht werden – holen Sie sich dafür wenn nötig Hilfe.

VORAUSDENKEN STATT VORAUSZAHLEN

Überraschende Erbschaften, Millionengewinne oder günstige Kredite – solcherart Angebote, die immer wieder im Posteingang auftauchen, scheinen auf den ersten Blick vor allem eines: unglaublich. Und das aus gutem Grund, denn es handelt sich dabei tatsächlich nur um versuchten Betrug, sogenannte Scams.

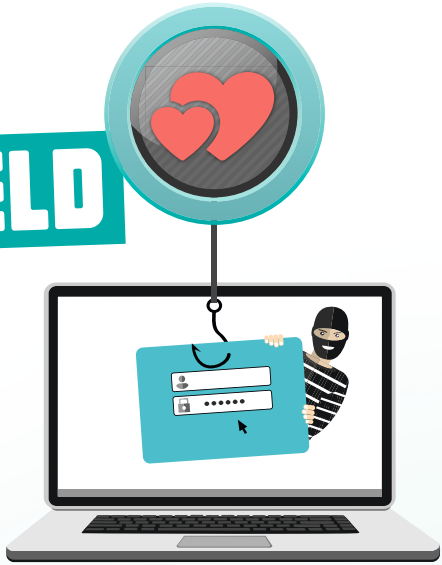
Das Schema dieser im Netz weit verbreiteten Betrugsform ist immer dasselbe: Die Betrüger erfinden eine Geschichte und drängen ihre Opfer unter einem Vorwand zu Vorschusszahlungen, meist für angeblich entstehende oder entstandene Kosten (Spesen, Flugtickets etc.). Dafür versprechen sie eine Gegenleistung, die letztendlich allerdings nie erbracht wird.

Was die erfundenen Geschichten betrifft, zeigen sich die Kriminellen äußerst kreativ: Die Bandbreite reicht von bis dato unbekannten Verwandten, die einem ihr ganzes Vermögen hinterlassen haben, bis hin zu Pechvögeln, die aufgrund einer Notlage Hilfe benötigen. Um glaubwürdiger zu erscheinen, fälschen Betrüger dafür nicht nur Dokumente und Webseiten, sondern sogar Anrufe, wobei die Täter oft nicht nur auf Geld, sondern ebenso auf persönliche Daten aus sind – diese können nämlich im Darknet für hohe Preise weiterverkauft werden.

TIPPS

- Auch im Netz gilt: Niemand hat was zu verschenken, seien Sie bei ungewöhnlichen Angeboten deshalb stets skeptisch.
- Übermitteln Sie Menschen, die Sie nicht persönlich kennen, weder Geld noch private Dokumente.
- Lassen Sie sich nicht unter Druck setzen und wählen Sie keine angegebenen Telefonnummern.
- Geben Sie Teile der Mail, etwa den Betreff, mit dem Zusatz „Scam“ in eine Suchmaschine ein – so lassen sich Betrugsversuche oft schon früh erkennen.

DIE LIEBE UND DAS GELD



Zwei der aktuell verbreitetsten Scamming-Methoden sind der Liebesschwindel (Love-Scam) und der Anlagebetrug (Investment-Scam).

Bei Ersterem spielen Betrüger ihren Opfern insbesondere auf Dating-Plattformen oder via Social Media die große Liebe vor, beim Anlagebetrug wiederum werden lukrative Investitionsmöglichkeiten (Aktien, Bitcoins etc.) vorgegaukelt.

In beiden Fällen werden jedoch früher oder später Geldzahlungen oder Bankdaten der Opfer verlangt. Für Internetnutzer gilt daher die Devise: Bei entsprechenden Angeboten immer misstrauisch sein.

LOVE-SCAM

Was sind die Anzeichen?

- Eine neue Bekanntschaft spricht schon früh von tiefen Gefühlen Ihnen gegenüber und bittet um private Chats.
- Die Nachrichten des Gegenübers sind in schlechtem Deutsch verfasst, das Onlineprofil stimmt nicht mit den getätigten Aussagen überein.
- Man bittet Sie, intime Bilder oder Videos von sich zu übermitteln, verlangt schließlich Geld oder versucht, Sie zu erpressen.

INVESTMENT-SCAM

Was sind die Anzeichen?

- Sie werden mehrmals unaufgefordert angerufen.
- Man versichert Ihnen, dass die Investition sicher sei, und verspricht eine rasche Rendite.
- Man teilt Ihnen mit, das Angebot sei nur für begrenzte Zeit und ausschließlich für Sie verfügbar, und bittet Sie, es mit niemandem zu teilen.

WEITERE INFORMATION

auf der Homepage **www.bmi.gv.at/praevention** und auch per **BM.I-Sicherheits-App**.

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

ELEKTRONISCHE ERPRESSUNG

Epressungsversuche über Mails gibt es schon länger, die Methoden werden aber zunehmend dreister. Seit einiger Zeit wird etwa häufig mit der Veröffentlichung angeblicher Masturbationsvideos gedroht.

„Hohe Gefahr. Konto wurde angegriffen" – diesen oder einen ähnlich formulierten Betreff findet man heutzutage häufig bei Massenmails, die behaupten, dass der eigene Computer gehackt und in der Folge ein Masturbationsvideo des jeweiligen Nutzers erstellt wurde. Wolle man nicht, dass das Video veröffentlicht werde, so heißt es in derartigen Mails, müsse man einen Geldbetrag auf ein Bitcoinkonto überweisen.

In vielen Fällen scheinen diese Nachrichten nicht zuletzt deshalb glaubhaft, weil die eigene Mail-Adresse als Absender aufscheint – doch es handelt sich dabei nur um eine Manipulation, bei der mittels eines Programms der E-Mail-Header ausgetauscht wurde. Ganz egal, wie plausibel diese Behauptungen auch sein mögen, am Ende sind diese Mails meist nur Fakes.

Darauf deuten vor allem zwei Anzeichen hin: wenn die Mail keine konkrete Anrede mit Namen aufweist und wenn es keinerlei Hinweise auf ein mögliches Video (etwa Screenshots) gibt.

TIPPS

Die Kriminalprävention gibt folgende Tipps:

- Öffnen Sie keine E-Mail-Anhänge unbekannter Absender und klicken Sie auf keine Links.
- Verwenden Sie Virenschutzprogramme sowie Firewalls und scannen Sie regelmäßig Ihren Rechner.
- Nutzen Sie Ihre Webcams bewusst und greifen Sie gegebenenfalls auf Webcamblocker zurück.
- Achten Sie auf die Wortwahl und die Anrede in entsprechenden Erpressungsmails.
- Informieren Sie sich über gängige Betrugsversuche im Internet, etwa auf **www.watchlist-internet.at**.

HALLO, WER SPRICHT? BETRÜGER AM TELEFON

Beim sogenannten Call-ID-Spoofing geben sich Anrufer als jemand anderes, meist als Polizisten oder Beamte, aus. Ihr Ziel: den Opfern Daten oder Geld zu entlocken.

Durch technische Tricks ist es heutzutage möglich, auf dem Display angerufener Personen jede Nummer anzeigen zu lassen, die man möchte. Von diesem Call-ID-Spoofing genannten Verfahren machen vor allem Betrüger Gebrauch: Sie geben sich etwa als Polizisten aus und versuchen, ihre Opfer unter einem Vorwand zur Herausgabe von sensiblen Daten, Geld oder Wertgegenständen zu bewegen. Das häufigste Szenario, das diese falschen Beamten anführen: Man habe bei der Verhaftung eines Täters Name und Anschrift des Angerufenen gefunden und stelle deshalb entsprechende Ermittlungen an.

TIPPS

- Niemals über Telefon vertrauliche Informationen an Unbekannte weitergeben, auch wenn sie vorgeben, Mitarbeiter offizieller Stellen zu sein.
- Die Polizei wird Sie niemals auf telefonischem Weg auffordern, Geld zu überweisen oder Wertsachen herauszugeben.
- Lassen Sie sich nicht von der angezeigten Rufnummer täuschen, verlangen Sie Namen, Telefonnummer und Dienststelle und rufen Sie selbst auf dieser an. Suchen Sie dazu die Nummer im Telefonbuch oder Internet.

FALSCHE MICROSOFT-MITARBEITER

Häufig geben sich Betrüger auch als Microsoft-Mitarbeiter aus: Sie behaupten, ein angebliches technisches Problem am PC beheben zu wollen, und versuchen ihre Opfer zur Installation eines Fernwarteprogramms zu überreden. Mit diesem (Fernwartetool) erhalten sie Zugriff auf den Rechner, können Eingaben mitverfolgen und Zahlungsinformationen und persönliche Daten auslesen. Meistens werden Betroffene im Anschluss auch zu Zahlungen wegen der vermeintlichen Hilfe aufgefordert.

Die Polizei rät:

- Derartige Anrufe sofort beenden oder am besten gleich ganz ignorieren.
- Sollten Sie bereits auf einen falschen Microsoft-Mitarbeiter hereingefallen sein, trennen Sie Ihren Rechner vom Netz und ändern Sie Ihre Passwörter.
- Erstatten Sie gegebenenfalls Anzeige bei der Polizei.

KEIN DEPP IM WEB!

Wenig arbeiten und viel verdienen? Das funktioniert auch im Internet nicht.

Jobangebote im Web gibt es wie Sand am Meer. Neben seriösen Portalen, welche tatsächlich existierende Arbeitsstellen im Auftrag von Unternehmen bewerben oder vermitteln, gibt es auch viel Bauernfängerei.

Manchmal handelt es sich dabei dann um „Angebote", bei deren Annahme man sich strafbar macht (Stichwort Geldwäsche – z. B. sollen Beträge auf das eigene Girokonto überwiesen und gegen Provision vom Opfer weiterüberwiesen werden), oder es soll z. B. zuerst Geld irgendwohin überwiesen werden, das sich dann angeblich quasi von selbst vermehrt.

Aktuell nehmen Angebote von Tradingportalen zu, welche hohe Gewinne versprechen, wenn man zunächst mehrere Monate lang Geld in Wertpapiere und begleitende Onlinekurse steckt. Diese sitzen meist im Ausland, haben oftmals keine Lizenz der österreichischen Finanzmarktaufsicht und handeln illegal.

TIPPS

- Bei angeblich unglaublich tollen Arbeitsangeboten immer sofort den Hausverstand einschalten. Und da einem ja normalerweise nichts geschenkt wird (siehe S. 5), lieber Finger weg, wenn's zu einfach oder zu verlockend klingt.
- Trading mit Wertpapieren ist komplex und finanziell meist hochriskant. Viel Erfahrung und Geld, das man jederzeit entbehren könnte (weil man es nicht für den Lebensunterhalt benötigt), gehören dazu, denn Verluste passieren schnell. Wenn eine Tradingplattform das Gegenteil behauptet – Finger weg! Wen Traden interessiert, der kann aus einer Vielzahl von praktischen Fach- und Lehrbüchern erste Kenntnisse über den (riskanten) Handel an den Börsen erwerben.

KONTAKT

AK Tirol, Konsumentenschutz
Kostenlose Hotline: 0800/225522-1818
www.ak-tirol.com

8 SICHERHEITSTIPPS FÜR KLEINE COMPUTER-NETZE

1. Sicherheitsupdates einspielen: Dies gilt für jegliche Soft- und Hardware, die Sie benutzen – Windows, macOS, Android, iOS, diverse installierte Programme und Geräte wie WLAN-Router oder auch Smart-TVs. Damit werden bisher bekannt gewordene Schwachstellen vom Hersteller korrigiert, um Angriffe aus dem Internet abzuwehren.

2. Administratorrechte einschränken: Der durch einen Angriff oder eine Malware verursachte Schaden ist unter den Rechten eines Administrator-Accounts um ein Vielfaches größer als im Kontext eines Minimalbenutzers. Daher macht es Sinn, im Alltag niemals mit Admin-Rechten im Internet zu surfen oder Mails zu beantworten und diesen Account nur für die seltenen administrativen Aufgaben separat kurz anzumelden.

3. Schutz gegen Schadsoftware: Privatanwender sind mit dem in Windows bereits inkludierten Microsoft Defender inzwischen relativ gut geschützt. Wer ein paar Euro mehr investiert, bekommt bei Kaspersky, ESET & Co. noch weitere Schutzmodule.

4. Datensicherung: Für den Fall der Fälle müssen alle Daten so gesichert sein, dass diese bei einem Angriff nicht gelöscht oder verschlüsselt werden können. Idealerweise regelmäßig, in mehreren Versionen und auf physikalisch getrennten Medien.

5. Passwörter: Verwenden Sie für jeden Dienst ein anderes – komplexes – Pass-/Kennwort. Sollte eines Ihrer Pass-/Kennwörter irgendwo auf der Welt gestohlen werden, bleiben so alle anderen Zugänge geschützt. Passwortmanager helfen beim sicheren Speichern all dieser Logins.

6. Awareness aufbauen: Hacker nehmen sehr oft das schwächste Glied ins Visier – und das ist meist der Mensch. Machen Sie sich mit den Maschen der Angreifer vertraut. Wie erkennt man eine Phishing-Mail? Etc.

7. Verschlüsseln von sensiblen Daten: Aktivieren Sie die ebenfalls bei Microsoft inkludierte Festplattenverschlüsselung (Bitlocker) auf allen Geräten. Damit vermeiden Sie den Verlust all Ihrer Daten z. B. beim Diebstahl eines Notebooks, das Auslesen des Passworts oder das Ändern von sensiblen Konfigurationsdateien.

8. Perimeter: Perimeter sind die aus dem Internet erreichbaren IT-Schnittstellen des Netzwerkes. Diese werden von Hackern und Scannern ständig auf Schwachstellen hin untersucht. Veröffentlichen Sie interne Dienste und Rechner nur per VPN.

KONTAKT
Ing. David Winkler, Ethical Hacker/CEO
www.strong-it.at

KAUFEN UND ZAHLEN IM INTERNET – ABER SICHER!

Onlineshopping ist sehr beliebt. Dennoch gibt es immer wieder Probleme bei Bestellungsabwicklung, Zahlung, Lieferung und dann vor allem, wenn keine oder eine mangelhafte Ware geliefert, aber schon im Voraus bezahlt wurde. Ein paar Grundregeln zu berücksichtigen, kann Sie vor unangenehmen Erfahrungen und vielleicht teuren Fallen bewahren.

Vor dem Einkauf in einem Internetshop, den Sie nicht bereits als vertrauenswürdig kennen, schauen Sie nach, ob ein Impressum vorhanden ist. Hier sollten die genaue Firmenbezeichnung, die Unternehmensanschrift sowie weitere Kontaktdaten zu finden sein. Falls ein Shop kein Impressum hat, verstößt er gegen das Gesetz.

Ebenso sollten Sie von einem Einkauf dort Abstand nehmen, wenn keine oder kaum Kontaktdaten vorhanden sind. Zumindest Firmenanschrift, Telefonnummer und eine E-Mail-Adresse sollten angegeben sein, sodass Sie im Fall einer Frage oder eines Problems einfach und rasch Kontakt mit dem Verkäufer aufnehmen können.

Ist ein Webformular zum Ausfüllen die einzige Kontaktmöglichkeit – Finger weg! Meistens hat es einen Grund, wenn ein Unternehmen seine Herkunft verschleiert oder die Kontaktmöglichkeiten einschränkt. Übrigens: Wenn eine Internetadresse die Endung .at trägt, heißt das noch lange nicht, dass das betreffende Unternehmen seinen Firmensitz in Österreich hat. Alle diese

Internetseiten können z. B. in China, den USA, der Türkei oder sonst wo auf der Welt registriert sein. Wer Inhaber einer Internetadresse mit der Endung .at ist, können Sie jederzeit auf der Internetseite www.nic.at überprüfen.

Bewertungen prüfen
Bevor Sie bei einem Ihnen (noch) unbekannten Shop bestellen, sollten Sie die Bewertungen anderer Kunden lesen. Googeln Sie dazu den Namen des Shops oder die Internetadresse gemeinsam mit einem Signalwort wie z. B. „Erfahrungen" oder „Bewertungen".

Ein gutes Bild vom Kundenservice und der Reaktionsgeschwindigkeit können Sie sich machen, indem Sie eine Anfrage z. B. zu einem Produkt stellen. Wenn Sie gerade keine haben, denken Sie sich eine aus! Wenn die Mitarbeiter nämlich dann schnell, freundlich und kompetent antworten, können Sie jedenfalls einen besseren Eindruck gewinnen, als wenn langsam und widerwillig geantwortet wird, denn das wird dann voraussichtlich auch im Falle einer Reklamation so sein.

Sicher bezahlen
Vereinbaren Sie nach Möglichkeit Zahlung auf Rechnung. D. h., Sie bekommen die Ware mit einer Rechnung geliefert, haben Zeit, alles zu prüfen, und zahlen erst dann, wenn alles passt. Das ist die sicherste Variante für Sie. Bei Zahlung durch Bankeinzug haben Sie nach der Abbuchung acht Wochen Zeit, den Betrag von Ihrer Bank zurückbuchen zu lassen, sollte z. B. gar keine oder eine falsche Ware geliefert werden. Zahlungen mit Kreditkarte oder per Nachnahme sind schon riskanter. Auf keinen Fall sollten Sie bei einem Ihnen unbekannten Shop eine Rechnung begleichen, bevor Sie die Ware erhalten haben. Wenn der Shop nicht oder falsch liefert und nachher dort keiner mehr erreichbar ist, ist Ihr Geld mit hoher Wahrscheinlichkeit für immer weg. Dann bleibt nur noch die Anzeige bei der Polizei.

Wenn die Bezahlung per Geldtransferdienst (z. B. Western Union oder MoneyGram) gefordert wird, verzichten Sie auf den Einkauf bei einem solchen Shop. Solche Zahlungen sind nicht nachverfolgbar und werden von keinem seriösen Shop gefordert. Überhaupt sollten die Alarmglocken läuten, wenn ein Unternehmen auf einer einzigen Bezahlform besteht, Hände weg!

Überlegt verkaufen
Wenn Sie selbst auf einer privaten Verkaufsplattform kaufen oder verkaufen, gilt es ebenfalls, vorsichtig zu sein. Am besten, Sie vereinbaren – wann immer es möglich ist – vor Kaufabschluss die persönliche Übergabe von Ware und Geld. Wenn Sie eine Ware verkaufen, verwenden Sie immer ein selbst gemachtes Foto des Produkts – niemals eines aus dem Internet, an dem Sie keine Rechte haben. Das kann nämlich teuer werden, wenn der Fotograf Schadenersatzforderungen wegen der unerlaubten Verwendung an Sie stellt – was oft passiert.

KONTAKT
AK Tirol, Konsumentenschutz
Kostenlose Hotline: 0800/225522-1818
www.ak-tirol.com

SICHERES MOBILE BANKING

Mobile Banking ist stark im Kommen und wird durch die neuen, zweifach abgesicherten Authentifizierungsverfahren wie etwa pushTAN noch weiteren Aufwind erfahren. Trotzdem nützen auch die sichersten Verfahren reichlich wenig, wenn die Nutzer ihr Smartphone nicht vor fremdem Zugriff zu schützen wissen.

Zugegeben, nur als Hochbegabter ist man vermutlich in der Lage, alle seine Passwörter im Kopf zu behalten. Trotzdem sollten Sie Zugangsdaten unter keinen Umständen am Handy abspeichern und sie auch nicht an Dritte weitergeben. Auch Ihr Display sollten Sie unbedingt unter Verschluss halten. Bitte bedenken Sie des Weiteren, dass Sie in offenen, sprich ungesicherten WLAN-Netzen für jeden Hacker ein offenes Buch sind. Deaktivieren Sie also unbedingt WLAN oder Bluetooth, wenn Sie ein gesichertes WLAN-Netz verlassen. Installieren Sie unbedingt ein Virenschutzprogramm, sollte Ihr Smartphone nicht standardmäßig

über eines verfügen. Führen Sie zudem regelmäßig Software-Updates durch, um etwaige Sicherheitslücken zu schließen. Vorsicht auch beim Herunterladen von Apps, nutzen Sie hierfür nur bekannte App-Stores und prüfen Sie zuvor die Bewertungen und Kommentare anderer User.

Doppelt abgesichert

Für das Internetbanking gelten innerhalb der EU mittlerweile einheitliche Sicherheitsstandards. Durch eine neue EU-Richtlinie, die seit 14. September 2019 in Kraft ist, haben alle Finanzinstitute und Zahlungsdienste im EU-Raum beim Internet- und Mobile Banking verpflichtend ein zweifaches Authentifizierungsverfahren anzuwenden. Das heißt: Neben den bis dato schon üblichen Passwörtern müssen nun auch die vom Kunden genutzten mobilen oder stationären Geräte mitautorisiert bzw. registriert werden. Bei mobil ausgeführten Transaktionen hat man sich also entweder über einen entsprechenden neuen Zahlencode, Fingerprint oder Face-ID auszuweisen.

Raiffeisen hat für sein Electronic Banking zudem die neue Signaturtechnologie pushTAN eingeführt. Das heißt: Für die Zeichnung der Aufträge müssen keine smsTANs mehr eingegeben werden, die Freigabe-TAN wird für jeden Auftrag automatisch über einen eigenen sicheren Kanal eingespielt. Diese Freigabe-TAN wird immer auftragsgebunden vergeben und ist auch nur 5 Minuten gültig.

SICHERES MOBILE BANKING

60 %

der **Raiffeisen-Kunden**, die Mein ELBA nutzen, arbeiten auch mit der **Mein ELBA-App**.

Das Bezahlen mit **Smartphone** ist genauso sicher wie mit **Bankomatkarte**.

90 %

aller **Kassenterminals** in Österreich sind auf die kontaktlose **NFC-Technologie** bereits umgestellt.

Wer kein Smartphone besitzt oder dieses auch nicht fürs Internetbanking nutzen möchte, dem stehen natürlich noch andere Signaturvarianten zur Verfügung, wie etwa ein spezielles cardTAN-Gerät oder auch die pushTAN-Desktop-Lösung. Wichtig ist nur, dass sichergestellt ist, dass man sich für jede Transaktion zweifach, sprich doppelt gesichert, authentifiziert.

SÜCHTIG NACH HANDY & INTERNET?

War das Handy vor Jahren noch ein möglichst kleines Gerät zum Telefonieren, ist es heute nicht nur Kommunikationsgerät, sondern auch Spielzeug, Geldtasche, Ausweis, Kamera, Kreativtool, Wecker usw. Dadurch schaut man zwangsläufig häufig auf das Display. Eltern machen sich deshalb oft Sorgen um ihr Kind: Ist es handysüchtig?

Die gute Nachricht vorweg: Nur sehr wenige Menschen, die viel Zeit am Computer oder mit dem Handy verbringen, sind wirklich krankhaft süchtig. Sucht ist eine Krankheit, keine Inkonsequenz im eigenen Verhalten. Nicht die Dauer und die Intensität der Nutzung entscheiden über Sucht oder Nicht-Sucht, sondern eher die Gründe, die jemanden veranlassen, dauernd an Handy, Computer, Tablet und Co. zu kleben. So können etwa Mobbing in der Schule oder Probleme zu Hause dazu führen, beispielsweise bei exzessivem Spielen und Surfen Ablenkung zu finden.

HILFE HOLEN

147 Rat auf Draht: Kostenloser, anonymer 24-h-Notruf für Kinder, Jugendliche und deren Bezugspersonen (Tel.-Nr. 147 ohne Vorwahl). Auf **www.rataufdraht.at** auch Online-Beratung oder Chat (Mo., Mi. & Fr., 18–20 Uhr) möglich.

Bin ich handysüchtig? **www.saferinternet.at/news-detail/bin-ich-handysuechtig/**

Selbsttest unter: **www.ins-netz-gehen.de/check-dich-selbst/bin-ich-suechtig**

Wann sollten Sie professionelle Hilfe holen?

- **Ihr Kind verbringt den Großteil des Tages am Computer oder mit dem Handy.** Wichtige Lebensbereiche Ihres Kindes, wie z. B. Schule oder Freizeitaktivitäten, leiden bereits darunter. Es wird in Kauf genommen, dass es zu Konflikten mit Familie, Schule etc. kommt.
- **Kontrollverlust.** Ihr Kind kann sich nicht von Computer bzw. Handy lösen, auch wenn es ihm durchaus bewusst ist, dass es eigentlich zu viel ist.
- **Die „Dosis" muss gesteigert werden.** Es wird immer häufiger und länger am Computer oder am Handy gespielt und gesurft.
- **Entzugserscheinungen.** Ist einmal kein Zugang zum Computer bzw. Internet möglich, treten klassische Entzugserscheinungen wie Nervosität, Unzufriedenheit, Gereiztheit und Aggressivität auf.

SOZIALE NETZWERKE

Soziale Netzwerke sind beliebt. Nach wie vor ist Facebook das größte soziale Netzwerk der Welt. In Österreich sind bereits 3,8 Mio. Personen angemeldet (Statista, Dez. 2018). Bei Jugendlichen zwischen 11 und 17 Jahren führen die Netzwerke WhatsApp, YouTube, Instagram und Snapchat die Rankingliste an (Jugend-Internet-Monitor, 2019).

TIPPS

Das InfoEck – Jugendinfo Tirol bietet Workshops für Jugendliche sowie Einzelinformationsgespräche zum Thema Internet und Social Media an. Dabei wird die eigene Rolle in digitalen Medien und sozialen Netzwerken reflektiert und durch Übungen und Tipps werden Kompetenzen für den sicheren Umgang gewonnen.

Das InfoEck ist auch Koordinationsstelle für Saferinternet.at. Die Saferinternet-Trainerinnen und -Trainer bieten ein breites Spektrum an Workshops für Gruppen in allen Altersstufen, Pädagoginnen und Pädagogen sowie für Eltern an.

Doch nicht jeder, der einem in einem sozialen Netzwerk eine Freundschaftsanfrage sendet, ist auch ein Freund. Vor allem im Umgang mit persönlichen Daten ist Vorsicht geboten, damit die vielen positiven Möglichkeiten, die soziale Netzwerke bieten, nicht plötzlich einen bitteren Nachgeschmack bekommen. Der Schutz der eigenen Privatsphäre ist in sozialen Netzwerken eine Herausforderung.

KONTAKT

InfoEck – Jugendinfo Tirol
Tel.: 0512/57 17 99
E-Mail: info@infoeck.at
www.mei-infoeck.at

INFO
Unsere aktuellen Tipps an Eltern finden Sie hier:
www.saferinternet.at/zielgruppen/eltern/

WENN MEIN KIND ONLINE IST

TIPPS FÜR ELTERN

1. **Entdecken Sie das Internet gemeinsam mit Ihrem Kind.** Begleiten Sie Ihr Kind bei seinen Entdeckungsreisen im Netz. Gemeinsame Erfahrungen erleichtern es, über positive und negative Erlebnisse bei der Internetnutzung zu sprechen.

2. **Vereinbaren Sie Regeln.** Regeln über die Internet- und Handynutzung können z. B. den zeitlichen Umfang, die genutzten Inhalte, den Umgang mit Bildern und persönlichen Daten oder die Kosten betreffen. Regeln sind nur dann wirksam, wenn Ihr Kind diese versteht und akzeptiert.

3. **Schützen Sie Ihre digitalen Geräte.** Treffen Sie Vorkehrungen für die technische Sicherheit Ihres Computers, z. B. Anti-Viren-Programm, Firewall und regelmäßige Software-Updates, Backup des PCs, Sperre von Mehrwertdiensten.

4. **Thematisieren Sie die Weitergabe von persönlichen Daten.** Sprechen Sie mit Ihrem Kind über die Risiken einer leichtfertigen Datenweitergabe im Internet. Name, Adresse, Telefonnummer und persönliche Fotos sollte Ihr Kind nur nach Absprache mit Ihnen weitergeben.

5. **Vorsicht bei Treffen mit Online-Bekanntschaften.** Es ist o. k., sich mit Bekanntschaften aus dem Netz zu treffen – aber nur an öffentlichen Orten (z. B. Café) und in Begleitung (zumindest Freund/Freundin). Sprechen Sie mit Ihrem Kind über mögliche Risiken.

6. **Diskutieren Sie den Wahrheitsgehalt von Online-Inhalten.** Zeigen Sie Ihrem Kind, wie die Richtigkeit von Inhalten aus dem Internet durch Vergleiche mit anderen Quellen überprüft werden kann.

7. **Machen Sie auf Regeln im Internet aufmerksam.** Auch im Internet gibt es Regeln. Was im realen Leben erlaubt oder verboten ist, ist auch im Internet erlaubt oder verboten.

8. **Die Chancen des Internets übertreffen die Risiken!** Seien Sie bei den Online-Aktivitäten Ihres Kindes nicht zu kritisch. Das Internet ist ein ausgezeichnetes Medium, das sowohl zum Lernen als auch in der Freizeit sinnvoll eingesetzt werden kann. Ermutigen Sie Ihr Kind, das Internet bewusst zu nutzen. Unter Anleitung können die Risiken sehr gut eingeschränkt werden.

Quelle: www.saferinternet.at/tipps/fuer-eltern

KSÖ-RATGEBER

SICHER IM INTERNET

Impressum

Medieninhaber, Herausgeber und Verlag: Raiffeisen Werbung Tirol, Adamgasse 1-7, 6021 Innsbruck
Redaktion: Mag. Christine Hofer, Mag. Christine Frei (alle Raiffeisen-Landesbank Tirol AG), Mag. Helmuth Lichtmannegger (AK Tirol), Obst Manfred Dummer, B.A., Chefinspektor Hans-Peter Seewald (alle Landespolizeidirektion Tirol), Barbara Buchegger (saferinternet.at), Dr. Kurt Berek (Land Tirol) · **Konzept:** Raiffeisen-Kommunikation · **Layout und Grafik:** TARGET GROUP Publishing GmbH, Brunecker Straße 3, 6020 Innsbruck · **Fotos (sofern nicht anders gekennzeichnet):** Raiffeisen, shutterstock.com
Drucklegungsdatum: November 2019 · **Druck:** onlineprinters.at