KSÖ-RATGEBER

SICHER IM INTERNET

KURATORIUM SICHERES ÖSTERREICH

POLIZEI

tirol Unser Land

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

UNSER ZIEL: EIN SICHERES ONLINE-LEBEN

Auf dem Smartphone als ständigem Begleiter, der oftmals morgens unser erster und abends letzter Kontakt zur Außenwelt ist, befinden sich zahlreiche private Informationen. Umso wichtiger ist es, diese sensiblen Daten vor unbefugtem Zugriff zu schützen. Vor allem auch aus dem Internet. Denn längst gilt es nicht mehr nur, „offline" auf unsere Sicherheit zu achten.

Der Landesklub Tirol des Kuratoriums Sicheres Österreich (KSÖ Tirol) hat es sich zur Aufgabe gemacht, mit zahlreichen Aktivitäten und Aktionen rund um das Thema Sicherheit die Verständigung zwischen Bevölkerung, der Exekutive, Politik, Wirtschaft und den Medien weiter zu stärken und den Dialog zu fördern. Das KSÖ Tirol rund um die Präsidenten Mag. Helmut Tomac (Landespolizeidirektor Tirol), Dr. Johannes Ortner (Vorstandsvorsitzender der Raiffeisen-Landesbank Tirol AG) und Mag. Hermann Petz (Vorstandsvorsitzender der Moser Holding AG) ist ein überparteilicher und unabhängiger Verein und versteht sich als eine Vernetzungs- und Informationsplattform im Bereich innere Sicherheit.

Die Sicherheit im Land ist vielen Personen und Institutionen ein bedeutendes Anliegen. Aus diesem Grund haben sich diese unter dem Dach des KSÖ und unter Mitwirkung des Bundesministeriums für Inneres zusammengefunden, um gemeinsame Projekte zu realisieren. So wie diesen Ratgeber, der in enger Zusammenarbeit von KSÖ Tirol, Arbeiterkammer Tirol, Land Tirol, Polizei, Tiroler Tageszeitung und den Tiroler Raiffeisenbanken entstanden ist.

Mobile Endgeräte, Applikationen und virtuelle Welten bereichern unser modernes Leben auf vielfältige Weise, beruflich wie privat. Was jeder Einzelne tun kann, um im Umgang damit stets auch für die nötige persönliche Sicherheit zu sorgen, erfahren Sie in kompakter Form in diesem Ratgeber.

Denn: Sicherheit geht uns alle an und größtmögliche Sicherheit ist unser gemeinsames Ziel.

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 gewisse 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. Wir haben aber versucht, die wichtigsten Themen aufzugreifen.

DREI GOLDENE REGELN

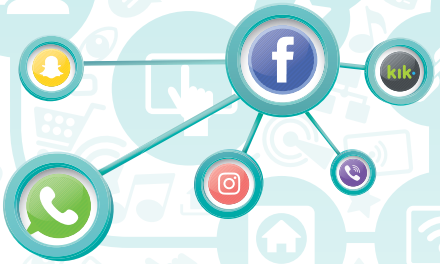
Die Konsumentenschützer der AK Tirol haben drei goldene Regeln für Sie zusammengestellt, mit denen Sie viele Fallen im Internet erkennen und vermeiden können:

1 **Niemand schenkt Ihnen was. Denken Sie immer daran!**
Also bitte Vorsicht bei „Gratis"-Versprechen, „Gewinn"-Mitteilungen, Krediten, die „sich von selbst zurückzahlen", u. v. a. m.

2 **Wenn jemand Ihre Daten will, dann hat er einen Grund!**
Geiz ist geil, wenn's um Daten im Internet geht. Das Web bietet viele Informationen, die grundsätzlich jeder anonym abrufen kann. Wenn dann plötzlich Ihr Name, Geburtsdatum, Wohnadresse, Telefonnummer u. Ä. ohne erkennbaren und nachvollziehbaren Grund verlangt werden, geben Sie sie nicht ein!

3 **100 % geschützt sind nur jene Daten, die Sie nicht bekannt geben!**
„Das Internet vergisst nicht!" Selbst wenn Sie über Sie im Web gespeicherte Informationen „löschen", können auf Servern irgendwo auf der Welt noch alle Daten gespeichert bleiben, und zwar über Jahrzehnte! Denken Sie daran!

SOZIALE NETZWERKE



Soziale Netzwerke sind beliebt. Die vielfältigen Möglichkeiten des Austauschs mit Freunden und Bekannten machen vor allem Facebook zum weltweit größten und bekanntesten sozialen Netzwerk. In Österreich sind schon 3,7 Mio. Personen bei Facebook angemeldet (Stand: August 2016). Weitere in Österreich genutzte soziale Netzwerke sind Instagram, Snapchat oder Twitter, dazu kommen noch Messenger wie WhatsApp oder Viber, die wie soziale Netzwerke genutzt werden.

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. Einerseits will man sich selbst präsentieren, um andere an seinem Leben teilhaben zu lassen, andererseits gilt es zu verhindern, dass persönliche Angaben missbraucht werden.

TIPPS

Das InfoEck – Jugendinfo Tirol bietet in Kooperation mit Saferinternet.at Veranstaltungen für Schüler, Lehrer und Eltern zum Thema „Umgang mit sozialen Netzwerken“ an:

- In Workshops für Schulklassen oder Vereine wird der sichere Umgang mit sozialen Netzwerken und persönlichen Daten erarbeitet.
- Informationsabende für Eltern und Fortbildungen für Lehrer runden das Angebot ab.

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

Grundsätzlich gilt: Je vorsichtiger man bei der Veröffentlichung von persönlichen Daten und Fotos ist und je genauer man sich im Vorfeld überlegt hat, wozu man das soziale Netzwerk nutzen will, desto sicherer ist das Social Networking! Eine komplette Verweigerung kann aber bedeuten, dass man von wichtigen Dingen im persönlichen Umfeld ausgeschlossen wird und dadurch nicht nur den Anschluss an den Freundeskreis verliert, sondern auch wichtige Dinge für das spätere (Berufs-)Leben nicht erlernt.

„BIST DU DAS IM VIDEO?"

Wer auf dem Facebook-Messenger von einem vermeintlichen Freund diese oder eine ähnliche Frage gestellt bekommt, sollte keinesfalls auf den angefügten Link klicken, den der Fragesteller mitgeschickt hat.

Denn damit würde man sich vermutlich einen Virus einfangen, mit dem man z. B. ungewollt ein Abo für Erotik-Seiten abschließt, der persönliche Daten absaugt oder mit dem Internet-Täter das Facebook-Konto „hacken" können.

©Alexey Boldin / Shutterstock.com

TIPPS

Wichtig! Auf sichere Facebook-Einstellungen achten:

- Nur sichere Passwörter verwenden
- Kontaktlisten, Profilbilder, Fotos etc. nicht öffentlich einsehen lassen!

Woran erkennt man Fake-Profile?

- Eine Person, mit der man bereits auf Facebook befreundet ist, sendet erneut eine Freundschaftsanfrage.
- Das Profil weist Unstimmigkeiten auf (z. B. hat die Person nur sehr wenige Freunde und Freundinnen).
- Man wird aufgefordert, eine SMS an eine Nummer zu senden und auf eingehende Textnachrichten mit „JA" zu antworten.
- Nachrichten sind sehr allgemein und unpersönlich formuliert und enthalten meist Rechtschreibfehler.

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 diese Personen oft in der Plattform blockiert werden. Wird jemand unerträglich lästig, so melden Sie dies in der Plattform selbst und überlegen mithilfe von Vertrauten, wie dem ein Ende bereitet werden kann. Vergessen Sie nicht, Beweise zu sichern, z. B. in Form von Screenshots.**

- **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.**

- **Jeder neuer Hype? Überlegen Sie, ob Sie bei jedem neuen Hype mitmachen müssen. Und löschen Sie Accounts von Netzwerken, die Sie nicht mehr benutzen. Vor allem dann, wenn diese mit Ihrer Telefonnummer verknüpft sind. Ein Löschen der App am Smartphone reicht dazu nicht.**

VOM NOTFALL-E-MAIL BIS ZUM IDENTITÄTSDIEBSTAHL

Der Einfallsreichtum von Kriminellen scheint besonders im Internetbereich kaum Grenzen zu kennen. Es gibt nur wenige Produkte, die von Betrügern noch nicht im World Wide Web zu besten Konditionen angeboten, jedoch nach der erfolgten Bezahlung nicht geliefert wurden.

Oft sind die Täter aber nicht nur auf das Geld ihrer Opfer aus. Auch die persönlichen Daten zählen zur begehrten Beute der Kriminellen.

NOTFALL-E-MAIL

Beim Betrug mit sogenannten Notfall-E-Mails versuchen die Täter mittels „Hacking"- oder „Phishing"-Attacken an die Zugangsdaten von E-Mail-Accounts zu gelangen. Sobald ihnen der Einstieg in die fremden Konten gelungen ist, senden sie an die im Adressbuch vorhandenen Kontakte eine Notfall-E-Mail. Darin geben sie vor, dass sich der Besitzer des Kontos im Ausland in einer Notlage befindet und dringend Geld benötigt, das per Bargeldtransferdienst übermittelt werden sollte.

TIPP

Sollten Sie eine „Notfall-E-Mail" erhalten haben, nehmen Sie unbedingt persönlich (z. B. telefonisch) mit dem vermeintlichen Absender Kontakt auf, um zu überprüfen, ob tatsächlich eine Notlage vorliegt bzw. ob die Nachricht tatsächlich von ihm stammt.

IDENTITÄTSDIEBSTAHL

Beim Identitätsdiebstahl oder Identitätsmissbrauch versuchen Kriminelle an persönliche Daten ihrer Opfer wie beispielsweise Führerschein- oder Reisepassdaten zu gelangen, um diese dann missbräuchlich zu verwenden. Von der Diskreditierung durch Namensmissbrauch in Internetforen und Blogs bis zum Anlegen falscher Accounts, von der Vortäuschung falscher Tatsachen bis zum Bestellbetrug – persönliche Daten sind für Kriminelle äußerst wertvoll.

TIPP

Überlegen Sie sorgfältig, wem Sie im Internet welche Daten übermitteln wollen. Seien Sie besonders vorsichtig bei Angeboten, bei denen Sie aufgefordert werden, Kopien ihrer Dokumente zu übersenden.

KONTAKT

Verdächtige Sachverhalte im Internet melden Sie bitte an die Internetmeldestelle im Bundeskriminalamt, E-Mail: **against-cybercrime@bmi.gv.at**

Weitere Information erhalten Sie auf der nächsten Polizeiinspektion, auf der Homepage **www.bmi.gv.at/praevention** und auch per **BM.I-Sicherheits-App**.

Die Spezialisten der Kriminalprävention des Landeskriminalamtes Tirol stehen Ihnen kostenlos für Beratungsgespräche unter der Telefonnummer **059133/703333** zur Verfügung.

VON VERKLEIDETEN VERBRECHERN & KETTENBRIEFEN INTERNET-HOAXES

Soziale Medien bieten eine perfekte Plattform, um verschiedene Informationen rasch erhalten und diese auch ebenso rasch weiterleiten bzw. mit anderen teilen zu können.

Was im ersten Moment nur positiv erscheint, birgt aber auch eine Gefahr. Viele Meldungen auf Internet-Plattformen werden in kürzester Zeit millionenfach geteilt, obwohl es sich schlichtweg um Falschmeldungen, sogenannte Hoaxes, handelt.

Beim „Rauchmelder-Hoax" wurde beispielsweise vor Verbrechern gewarnt, die als Feuerwehrmänner verkleidet vorgeben würden, Rauchmelder zu überprüfen, um sich in fremde Wohnungen zu schleichen. Der Bitte, diese Warnung möglichst oft zu teilen, kamen tausende beunruhigte Nutzer von sozialen Medien nach, obwohl die als Feuerwehrmänner verkleideten Verbrecher niemals existiert hatten.

Generell sollte man bei Informationen aus unbekannter Quelle vorsichtig sein und den Inhalt entsprechend kritisch prüfen, bevor man die Infos teilt. Bei der Prüfung können auch entsprechende Internetseiten hilfreich sein, auf denen Hoaxes aufgelistet werden. Auch wenn es gut gemeint ist, es ist wichtiger, verdächtige Wahrnehmungen rasch bei der Polizei zu melden, als diese ungeprüft sofort in sozialen Medien zu teilen.

Auch Kettenbriefe eignen sich offensichtlich gut für das Internet. Vor allem Kinder und Jugendliche glauben oftmals E-Mails mit den meist bedrohlichen Inhalten weitersenden zu müssen, um zum Beispiel nicht das Opfer eines im World Wide Web ausgesprochenen Fluchs zu werden. Eltern, Erziehungsberechtigte und Lehrer sollten die jungen Computer-User unbedingt entsprechend aufklären.

MONEY MULE

VON DER „GUTEN VERDIENSTMÖGLICHKEIT“ ZUR GELDWÄSCHEREI!

Per E-Mail werben Kriminelle mit vermeintlich guten Verdienstmöglichkeiten für Personen, die für Geldtransaktionen ihr Konto zur Verfügung stellen. Da durch diese Überweisungen illegale Zahlungsströme verschleiert werden sollen oder Internetbetrugshandlungen begangen werden, machen sich diese Personen oft der Geldwäscherei oder als Mittäter bei Betrugshandlungen strafbar.

ACHTUNG

Die Täter stellen diese Tätigkeit meist als legal dar, was nicht der Fall ist! Es drohen möglicherweise Verwaltungsstrafen nach den geltenden Finanzmarktgesetzen.

Das Bundeskriminalamt warnt daher:

- Gehen Sie keinesfalls auf solche Angebote ein!
- Seien Sie misstrauisch, wenn Ihnen ein unbekannter Absender viel Geld für eine scheinbar leichte Arbeit anbietet!
- Denken Sie daran, dass die Täter die Kontodaten ihres „Money Mule“ erlangen, was auch eine Gefahr für Ihre monetäre Sicherheit bedeuten kann.

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.

DAS RICHTIGE PASSWORT

Fast jeder Konsument besitzt mehrere Passwörter. Manche zwanzig und mehr. Passwörter verleihen Zugang zu persönlichen Bereichen, manchmal auch hochsensiblen Dokumenten und Bankkonten. Entsprechend gefährlich wird es, wenn Passwörter in fremde Hände geraten. Immer wieder passiert es, dass (einfache) Passwörter ausspioniert werden. Man stelle sich nur vor, jemand bekommt Zugang zu einem fremden Facebook-Account und ändert als Erstes – richtig – das Passwort. Ab diesem Zeitpunkt ist dem wahren Inhaber der Zutritt zum Account verwehrt und der Fremde kann mit dessen Identität öffentlich auftreten. Noch dramatischer ist die Situation, wenn ein und dasselbe Passwort für mehrere Webzugänge verwendet wird und der Passwortdieb so gleichzeitig Eintritt zu allen Accounts erhält.

TIPPS

- Verwenden Sie möglichst lange Passwörter (mindestens 8, besser 12 oder mehr Zeichen).
- Verwenden Sie für jeden neuen Account ein eigenes Passwort.
- Kombinieren Sie Buchstaben und Zahlen, Groß- und Kleinschreibung, Satz- und Sonderzeichen wild durcheinander.
- Verwenden Sie niemals Wörter oder Wortteile, die in einem Lexikon oder Wörterbuch stehen.
- Speichern Sie Passwörter nicht auf einem PC oder Handy, wenn dort (auch nur zeitweise) Zugang zum Internet besteht.
- Wenn notwendig notieren Sie sich Passwörter nur an einem geheimen Ort als Merkhilfe, aber keine weiteren Log-in-Daten oder sonstige Angaben zum Account. Sollte jemand irgendwann doch das Passwort lesen, wird er mit der Zeichenkette alleine kaum etwas anfangen können.

PERSÖNLICHKEITS- UND URHEBERRECHTE IM WEB

Internet und darauf basierende soziale Netzwerke und Nachrichtendienste machen es sehr einfach, Inhalte zu vervielfältigen. Wie schnell man dabei aber in rechtliche Schwierigkeiten kommen kann, wird den meisten erst dann bewusst, wenn sich ein Rechtsanwalt mit Schadenersatzforderungen und Klagsdrohungen meldet.

TIPPS

- Beachten Sie das Recht am eigenen Bild und fragen Sie Personen immer um ihre Zustimmung vor Veröffentlichung eines Fotos z. B. auf Facebook. Wenn jemand das nicht will, ist das jedenfalls zu akzeptieren. Ansonsten könnte diese Person gerichtlich gegen Sie vorgehen.

- Wenn Sie auf Tausch- oder Verkaufsplattformen im Internet Waren anbieten, verwenden Sie keine Fotos zur Präsentation, an welchen Sie nicht die entsprechenden Rechte besitzen.

- Wenn Sie ein Handy in einer Annonce im Web anbieten und hierfür ein Foto verwenden, das Sie auf der Website des Herstellers gefunden haben, kann ein üblicherweise internationaler Konzern rechtlich mit Schadenersatz- und Unterlassungsklage gegen Sie vorgehen. Das kann sehr teuer werden! Auch ist die Gefahr, erwischt zu werden, recht groß. Meist sind nationale Rechtsanwaltskanzleien mit der Überwachung des Internets wegen solcher Rechteverletzungen beauftragt.

KONTAKT
AK Tirol, Konsumentenschutz
Kostenlose Hotline: **0800/22 55 22-1818**
Homepage: **www.ak-tirol.com**

GEFÄHRLICHE VIREN PER MAIL

TIPPS

- Gehen Sie nur mit einem PC online, auf dem ein gutes und stets aktualisiertes Virenscanprogramm läuft. Dasselbe gilt, wenn Sie mit Ihrem Handy online gehen. Auch hier sollte stets für maximalen Virenschutz gesorgt werden. Jeden Tag entstehen weltweit 100.000e (!) neue Varianten von Computerviren.

- Wenn Sie E-Mails bekommen, die auf eine Rechnung/Datei im Anhang verweisen oder bei denen Sie einen Link für weiterführende Rechnungsinformationen anklicken sollen – höchste Vorsicht! Überlegen Sie gut, ob Sie den angeführten Absender (auch der kann gefakt sein) überhaupt kennen und auch eine Rechnung erwarten. Im Zweifel aber sollten Sie zunächst das Unternehmen telefonisch oder unter einer schon früher verwendeten E-Mail-Adresse kontaktieren, um herauszufinden, ob die Nachricht echt ist.

- Niemals dürfen Sie solche Anhänge einfach öffnen oder die Links anklicken! Es drohen ideelle und finanzielle Schäden.

© Alexey Boldin / Shutterstock.com

Täglich werden unzählige PCs und Mobiltelefone von Viren befallen. Dabei ist festzustellen, dass diese Viren immer zerstörerischer vorgehen oder aber sich so hinterhältig auf dem befallenen Gerät einnisten, dass sie zunächst nicht bemerkt werden.

Bei der ersten Variante werden z. B. sämtliche Dateien auf dem PC unbrauchbar gemacht. In der Folge versuchen Unbekannte per Mitteilung auf dem Bildschirm „Lösegeld" zu erpressen. Die zweite Variante, sog. Trojaner, installiert sich unbemerkt im Hintergrund. Aktiv werden diese z. B. beim Aufruf von Online-Banking-Seiten, dann spionieren sie die Zugangsdaten aus, um später betrügerische Überweisungen auszulösen. Sehr oft werden solche gefährlichen Viren durch E-Mails eingeschleppt.

KONTAKT
AK Tirol, Konsumentenschutz
Kostenlose Hotline: **0800/22 55 22-1818**
Homepage: **www.ak-tirol.com**

VORAUSZAHLUNGS-BETRUG

TIPPS

- Viele Firmen bieten Kauf auf Rechnung an. D. h., Sie erhalten zuerst die Ware und zahlen einige Tage später z. B. per Banküberweisung. Bevorzugen Sie solche Angebote gegenüber jenen, bei denen im Voraus gezahlt werden muss! Auch bei Kreditkartenzahlungen kommen Sie bei Streitigkeiten nicht mehr so leicht an ihr Geld.

- Auch bei Privatangeboten auf Verkaufsplattformen vorsichtig vorgehen! Wenn Sie für eine Ware im Voraus zahlen, haben Sie immer ein gewisses Risiko, eine kaputte oder überhaupt keine Ware geliefert zu bekommen.

- Vorsicht bei Internetshops, die Sie noch nicht als seriös und kundenfreundlich kennen. Googeln Sie den Shopnamen mit dem Stichwort „Erfahrungen“ und lernen Sie aus den Fehlern, die andere bereits gemacht haben.

- Achten Sie bei Internetshops darauf, ob ein Gütesiegel vorhanden ist, das die Streitschlichtung bei Auseinandersetzungen mit dem Shopbetreiber anbietet (z. B. das Österreichische E-Commerce-Gütezeichen, www.guetezeichen.at).

- Vergessen Sie nicht: Zahlungen per Überweisung oder Bargeldtransfer können in der Praxis kaum, Zahlungen per Kreditkarte nur schwer und nur unter bestimmten Umständen erfolgreich rückgefordert werden.

KONTAKT
AK Tirol, Konsumentenschutz
Kostenlose Hotline: **0800/22 55 22-1818**
Homepage: **www.ak-tirol.com**

NEPP PER APP

Apps am Smartphone sind cool und bei vielen, vor allem jungen Konsumenten sehr beliebt. Ob sie unseren Alltag immer bereichern, steht auf einem anderen Blatt. Auf alle Fälle sind viele dieser Apps kostenlos herunterzuladen.

Aber, wie bereits aus der goldenen Regel Nr. 1 bekannt: Niemand schenkt Ihnen was! Selbstverständlich möchten die Vertreiber von Apps auch was verdienen. Sehr oft funktioniert das über sogenannte „In-App-Käufe", d. h., bei Verwendung der App kommen immer wieder Kaufangebote für Tools, Spielgeld oder erweiterte Funktionalitäten der App. Häufig sind diese Features zwar gar nicht unbedingt notwendig, aber immerhin oft verlockend. Der Kauf kann manchmal durch einen einzelnen Klick ausgelöst werden. Der beste Schutz dagegen ist es, In-App-Käufe in den Einstellungen des Mobiltelefons zu deaktivieren und mit einem geheimen Passwort zu sichern.

TIPPS

- Deaktivieren Sie In-App-Käufe in den Einstellungen Ihres Mobiltelefons, wenn Sie wissen, dass diese nicht benötigt werden, oder Sie sich vor unbemerkten Käufen schützen wollen. Wenn Kinder mit dem Handy spielen, ist dies besonders zu empfehlen.
- Android: Play Store > Einstellungen > Nutzersteuerung > Authentifizierung für Käufe erforderlich > Häkchen setzen bei: „Für alle Käufe bei Google Play auf diesem Gerät“; iPhone und iPad: Einstellungen > Allgemein > Einschränkungen aktivieren > PIN-Code eingeben > In-App-Käufe deaktivieren (Regler nach links). Es muss u. U. zusätzlich festgelegt werden, dass die PIN vor jedem In-App-Kauf abgefragt wird.
- Sollten Sie auf Ihrer Mobilfunkrechnung Kosten für In-App-Käufe finden, welche von Ihnen nicht (bewusst) oder möglicherweise von minderjährigen Kindern ausgelöst wurden, so erheben Sie so rasch wie möglich schriftlich Einspruch bei Ihrem Mobilfunkprovider.

KONTAKT
AK Tirol, Konsumentenschutz
Kostenlose Hotline: **0800/22 55 22-1818**
Homepage: **www.ak-tirol.com**

WIE SCHÜTZE ICH MEIN SMARTPHONE

Wichtige Daten besser IM KOPF speichern

Speichern Sie keine Passwörter oder Zugangsdaten auf dem Handy.

Unbemerktes AUSSPIONIEREN

Deaktivieren Sie Datenverbindungen wie Bluetooth oder WLAN, wenn Sie diese gerade nicht verwenden.

Ungeliebte
EINBLICKE

Aktivieren Sie die Display-Sperre und nutzen Sie Schutzmechanismen wie PIN-Abfrage, Passwörter oder Sperrmuster bzw. Fingerprint-Abfrage.

Regelmäßige Software-
UPDATES

Führen Sie regelmäßig die für Ihre Apps angebotenen Software-Updates durch, um etwaige Sicherheitslücken zu schließen.

Unbemerkte
ÜBERTRAGUNG
persönlicher Daten

Viele Apps übertragen sensible Nutzerdaten, ohne dass dies für die Funktion der Anwendung notwendig ist. Überprüfen Sie daher idealerweise bereits vor dem Installieren von Apps, welche Zugriffsrechte diese einfordern. Eine Taschenlampen-App etwa benötigt keinen Zugriff auf das Adressbuch.

Achten Sie bei der Verbindung zu öffentlichen bzw. ungesicherten WLAN-Netzwerken darauf, keine sensiblen Daten zu senden.

Schadsoftware und
VIREN

Laden Sie Apps nur über die offiziellen App-Shops wie Google Play Store, App Store (Apple) oder Microsoft Store herunter. Anwendungen von Drittanbietern sind mit Vorsicht zu genießen – diese können mit Schadsoftware infiziert sein. Werden auf dem Smartphone oder Tablet sehr viele Apps installiert (mehr als fünf pro Woche), ist die Verwendung von Schutzsoftware empfehlenswert. Nicht mehr benötigte Apps sollten regelmäßig gelöscht werden.

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 Ihren Computer.** Treffen Sie Vorkehrungen für die technische Sicherheit Ihres Computers, z. B. Anti-Viren-Programm, Firewall und regelmäßige Software-Updates, Backup des PCs.

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 ok, 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. Christian Bevelander, Katharina Fesl, B.A., (alle Raiffeisen-Landesbank Tirol AG), Mag. Helmuth Lichtmannegger (AK Tirol), Obstlt Manfred Dummer, B.A., KontrInsp Stefan Eder, ChefInsp Hans-Peter Seewald (alle Landespolizeidirektion Tirol), Barbara Buchegger (saferinternet.at) **Konzept:** Raiffeisen-Kommunikation **Layout und Grafik:** TARGET GROUP Publishing GmbH, Brunecker Straße 3, 6020 Innsbruck **Fotos und Grafiken**: Raiffeisen, Shutterstock
Drucklegungsdatum: September 2016 **Druck:** flyeralarm