LAND TIROL

InfoEck der Generationen
Infobroschüre für SeniorInnen

Kurse und Anlaufstellen zu Computer und Internet

www.infoeck.at

Vorwort und Impressum

Diese Infobroschüre stellt die Computerias Tirol als Möglichkeit des Austauschs und Lernens von Computerwissen mit Gleichgesinnten vor und listet Einrichtungen auf, welche Computerkurse oder Kurse zu Smartphones oder Tablets anbieten. Des Weiteren finden sich Anlaufstellen, die mit Rat und Hilfe rund um die Themen Sicherheit im Internet, Online-Einkäufe, Internet-Kriminalität und weiteren Themen unterstützend zur Seite stehen. 10 Tipps zur sicheren Internetnutzung und Begriffserklärungen rund um Computer & Co sollen helfen sich in der digitalen Welt zurecht zu finden.

Inhaltsverzeichnis

1. **Computerias Tirol**
2. **Kurse für Computer, Smartphone und Tablet**
3. **Rat & Hilfe – Anlaufstellen und Links**
4. **Sicher im Internet – 10 Tipps**
5. **Begriffe rund um Computer, Internet & Co verständlich erklärt**

InfoEck der Generationen

betrieben durch den Verein Generationen und Gesellschaft, Kaiser-Josef-Str. 1, 6020 Innsbruck

Bozner Platz 5, 6020 Innsbruck.
Web: www.infoeck.at, E-Mail: info@infoeck.at
Info-Hotline: 0800 800 508

Die Auflistungen der Angebote erfolgten alphabetisch und haben trotz sorgfältiger Recherche der InfoEck MitarbeiterInnen keinen Anspruch auf Vollständigkeit oder Verfügbarkeit.

Stand: November 2022 (nr)

FördergeberIn und KooperationspartnerIn des InfoEck der Generationen:

INNS' BRUCK

LAND TIROL

1. Computerias Tirol

Computerias sind Lern- und Begegnungsorte, an denen sich SeniorInnen mit Hilfe von ehrenamtlichen AnleiterInnen mit Computer, Smartphone, Tablet und der digitalen Welt auseinandersetzen können. In entspannter Atmosphäre und im eigenen Tempo lernen die BesucherInnen voneinander. Jugendliche und Studierende helfen an vielen Standorten beim Umgang mit den neuen Technologien mit. Das Angebot ist kostenlos.

Was ist eine Computeria? Wer kann daran teilnehmen? Welche Computeria ist in meiner Nähe?

Informationen zu den verschiedenen Standorten
InfoEck der Generationen Innsbruck
Bozner Platz 5, 6020 Innsbruck
Mo – Fr: 09:00-14:00 Uhr, sowie Di und Do: 15:00-17:00 Uhr
Web: www.infoeck.at/computerias-tirol
Info-Hotline: 0800 800 508 (zu den Öffnungszeiten)

Sie, Ihr Verein, Ihre Gemeinde etc. möchten selbst eine Computeria gründen? Sie haben allgemeine Fragen zum Netzwerk Computerias Tirol?

Informationen zum Netzwerk Computerias Tirol
E-Mail: computerias@infoeck.at
Tel.: 0699 1508 35 15

Die Computerias sind durch das landesweite Netzwerk Computerias Tirol zusammengeschlossen. Die Koordination des Netzwerks liegt beim Verein Generationen und Gesellschaft. Computerias werden von der Abteilung Gesellschaft und Arbeit – SeniorInnen des Landes Tirol gefördert.

2. Kurse für Computer, Smartphone und Tablet

BFI - Berufsförderungsinstitut Ing.-Etzel-Straße 7, 6020 Innsbruck Tel.: 0512 / 596 60 E-Mail: info@bfi-tirol.at Web: www.bfi-tirol.at → Service → Kurssuche oder Kursprogramm *Zweigstellen in ganz Tirol*	□ IT-Schulungen in einer angenehmen Lernatmosphäre □ solide Grundausbildungen für EinsteigerInnen als auch fundiertes Spezialwissen in Fachlehrgängen
Katholisches Bildungswerk Tirol Riedgasse 9, 6020 Innsbruck Tel.: 0512 / 22 30-4801 E-Mail: kbw@bildung-tirol.at Web: www.bildung-tirol.at → Bereiche → SelbA → Handy & Co	□ Kurse „Smart & fit am Handy“ □ Tabletkurse □ tirolweite Kurse von qualifizierten TrainerInnen
Pensionistenverband Tirol Salurner Straße 2, 6020 Innsbruck	□ Computer-, Smartphone- und Tabletkurse

Tel.: 0512 / 589 113 E-Mail: tirol@pvoe.at Web: pvoe.at/tirol/ → Kursangebote *Ortsgruppen in ganz Tirol*	◻ (Nur mit Mitgliedschaft möglich!)
Tiroler Seniorenbund Adamgasse 9, 6020 Innsbruck Tel.: 0512 / 580 168 E-Mail: office@tiroler-seniorenbund.at Web: www.tiroler-seniorenbund.at → Kursprogramm *Zweigstellen in ganz Tirol*	◻ Computer- und Smartphonekurse (Einzelkurse) ◻ Tabletkurse (Gruppenkurse) (Nur mit Mitgliedschaft möglich!)
Volkshochschule Tirol Marktgraben 10, 6020 Innsbruck Tel.: 0512 / 588 882-0 E-Mail: innsbruck@vhs-tirol.at Web: www.vhs-tirol.at *Zweigstellen in ganz Tirol*	◻ Computer-, Smartphone- und Tablet-kurse ◻ EinsteigerInnen- und Fortgeschritte-nenkurse verschiedene Themen wie digitales Amt, Bezahlfunktionen im Internet, Online-Shopping, Werk-zeuge der Online-Kommunikation (Zoom & Co) und Weiteres ◻ spezielle Kurse für die ältere Genera-tion
WIFI Tirol Kundenservice Egger-Lienz-Straße 116, 6020 Innsbruck Tel.: 05 / 909 05-7777 E-Mail: info@wktirol.at Web: www.tirol.wifi.at *Zweigstellen in ganz Tirol*	◻ verschiedenste Kurse zum Thema EDV und IT ◻ EinsteigerInnen- und Fortgeschritte-nenkurse ◻ Kurse für iPhone und Android-Smart-phones

3. Rat & Hilfe – Anlaufstellen und Links

AK Tirol Maximilianstraße 7, 6020 Innsbruck Tel.: 0800 22 55 22-1818 E-Mail: konsument@ak-tirol.com Web: tirol.arbeiterkammer.at/index.html → Beratung → Konsumentenschutz *Zweigstellen in ganz Tirol*	◻ Tipps rund um eine sichere Internet-Nutzung zum effektiven Schutz vor Gaunereien ◻ Bezahlen im Internet ◻ Watchlist-App (Warnung vor Internet-Betrug) ◻ Rechtsberatung bei Internet-Betrug ◻ Hilfe bei Rechtsfragen und Kostenfal-len im Internet
Bundesministerium Inneres **Bundeskriminalamt** Josef-Holaubek-Platz 1, 1030 Wien Tel.: 01 / 248 36 985025, 985026 oder 985027	◻ Präventionstipps zur Kriminalität im Netz ◻ Infos zu Kinderpornografie, Grooming, Sexting ◻ Tipps für soziale Netzwerke

E-Mail: bundeskriminalamt@bmi.gv.at Web: www.bundeskriminalamt.at/ → Prävention & Opferhilfe → Prävention-stipps → Internet kennen *Bei Verdacht auf Internetkriminalität wenden Sie sich bitte per E-Mail an:* against-cybercrime@bmi.gv.at	□ Dokument „10 Tipps, wie Sie sich vor Gefahren schützen können“
InfoEck der Generationen Bozner Platz 5, 6020 Innsbruck Tel.: 0800 800 508 E-Mail: info@infoeck.at Web: www.infoeck.at	□ Informationen über aktuelle Trends und Gefahren im Internet □ App-Check (Einstellungen der Privatsphäre) □ Informationen über Fake & Betrug im Internet □ Informationen über Schutz im Internet
Saferinternet.at Ungargasse 64-66, 1030 Wien Tel.: 01 / 595 21 12-51 E-Mail: office@saferinternet.at Web: www.saferinternet.at	□ Infos zu sicherem und kompetentem Umgang mit digitalen Medien □ Computerschutz □ Sicheres Online-Shopping □ Datenschutz □ Viren, Spam & Co □ Internet-Betrug □ Online-Banking □ Privatsphäre-Leitfäden für Soziale Netzwerke □ Workshops für SeniorInnen-Gruppen □ eigener Bereich für SeniorInnen
Correctiv E-Mail: info@correctiv.org Web: correctiv.org/	□ Faktencheck: Aufdecken von Falschinformationen, Gerüchten und Halbwahrheiten
Internet Ombudsstelle Tel.: 01 / 595 2112-0 E-Mail: kontakt@ombudsstelle.at Web: www.ombudsstelle.at	□ Kostenlose Schlichtung und Hilfe bei Problemen im Internet □ Anlaufstelle bei Problemen mit Datenschutz, Online-Shopping, Abo-Fallen, Internetbetrug, Bildern im Netz
Konsumentenfragen Bundesministerium für Soziales, Gesundheit, Pflege und Konsumentenschutz Tel.: 01 / 711 00-862501, 862504 oder 862548 E-Mail: konsumentenfragen@sozialministerium.at Web: www.konsumentenfragen.at → Kommunikation und Medien → Übersicht Kommunikation und Medien	□ Telefon, Internet und Rundfunk □ Vertragsabschlüsse □ Probleme mit der Rechnung □ In-App-Käufe und Weiteres
Mimikama Web: www.mimikama.at	□ Internationale Koordinationsstelle zur Bekämpfung von Internetmissbrauch

→ Meldeformular auf der Website	□ Meldestelle für verdächtige Internetinhalte □ Aufdeckung von Falschmeldungen
oesterreich.gv.at Tel.: 01 / 71123-884466 Web: www.oesterreich.gv.at → Themen → SeniorInnen → Internet für SeniorInnen	□ Die ersten Schritte im Internet □ Reisen buchen über das Internet □ Tipps zur sicheren Nutzung des Internets
Österreichisches E-Commerce-Gütezeichen Tel.: 01 / 595 2112 E-Mail: office@guetezeichen.at Web: www.guetezeichen.at	□ Auflistung seriöser Online-Shops
RTR – Rundfunk- und Telekom-Regulierungsbehörde Tel.: 01 / 58058-0 E-Mail: rtr@rtr.at Web: www.rtr.at/schlichtungsstelle	□ kostenlose Streitschlichtung bei Problemen mit der Handyrechnung
Seniorencenter.at – SeniorInnen Portal www.seniorencenter.at/weiterbildung.htm	□ Weiterbildung, digitale Medien und PC Kurse für SeniorInnen
STOPline E-Mail: office@stopline.at Web: www.stopline.at	□ anonyme Internet-Meldestelle für illegale Inhalte zu Kinderpornografie und nationalsozialistische Wiederbetätigung im Internet □ Website auch in Englisch → Meldeformular auf der Website
Watchlist Internet Tel.: 01 / 595 211 275 E-Mail: kontakt@watchlist-internet.at Web: www.watchlist-internet.at	□ Infos und Hilfe zu Internet-Betrug, Fallen und Fakes □ Listen „unseriöser Internetseiten“ □ Erklär-Videos zu verschiedenen Themen
ZARA Tel.: 01 / 929 13 99 E-Mail: office@zara.or.at Web: www.zara.or.at/de/beratung	□ Beratung zu und/oder Meldung von Rassismus und Hass im Netz □ kostenlos und auf Wunsch anonym

4. Sicher im Internet – 10 Tipps

1. Sicheres Passwort: Verwendung von mindestens zehn Zeichen. Groß- und Kleinschreibung, Zahlen und Sonderzeichen sollten im Passwort enthalten sein. Passwörter vermeiden, die den Namen, das Geburtsdatum oder die Adresse beinhalten. Tipp: Einen Satz überlegen, den man sich gut merken kann, und davon die Anfangsbuchstaben + zwei Ziffern verwenden. Beispiel: Ich gehe jeden Freitag in den Supermarkt einkaufen → IgjFidSe38.
2. Schutz des PC: Anti-Viren-Programm und eine Firewall installieren, um vor schädlichen Dateien zu schützen. Ein Virenprogramm soll den PC und wichtige Dokumente vor Schadsoftware und z.B. auch Spionageprogrammen schützen. Betriebssystem, Firewall, Virenscanner und weitere Programme immer mit den aktuellen Updates aktualisieren, um Sicherheitslücken zu schließen.
3. Datenpreisgabe: Daten, die einmal im Internet sind, können so gut wie nicht mehr gelöscht werden, nach dem Motto: Das Internet vergisst nicht. Nur das angeben, was am nächsten Tag auf der Titelseite einer jeden Tageszeitung stehen dürfte. Je weniger von der eigenen Privatsphäre frei zugänglich ist, desto weniger Angriffsfläche wird BetrügerInnen oder unbefugten NutzerInnen geboten.
4. Privatsphäre schützen: In sozialen Netzwerken immer die Privatsphäre-Einstellungen beachten. Dabei ist es wichtig, Freundesgruppen anzulegen und Regeln über die Freigabe der Daten zu definieren. Zum Beispiel, wer mich auf Bildern markieren darf, wer die persönlichen Fotos sieht und anderes. Safer-Internet stellt „Privatsphäre-Leitfäden für Soziale Netzwerke“ zur Verfügung www.saferinternet.at.
5. Sicheres Surfen: Wichtige Daten sollten nur verschlüsselt übertragen werden. Bei einer Verschlüsselung werden die Daten „konvertiert“ d.h. von einem lesbaren in ein verschlüsseltes Format übertragen, z.B. beim Online-Banking. Beim Surfen darauf achten, dass ein grünes Schloss-Symbol in der Adresszeile im Browser aufscheint und davor https:// steht. Zudem kommt manchmal eine Zwei-Phasen-Authentifizierung vor: Zum Passwort muss beim Login eine weitere Sicherheitskomponente eingegeben werden, z.B. ein PIN-Code. Zeichen für die Seriosität eines Online-Shops sind ein Impressum mit Nennung und Anschrift der Firma, der Geschäftsführung oder einer UID-Nummer sowie klare Geschäftsbedingungen (AGB). Überlegen, ob die angegebenen Preise realistisch sind.
6. Abzocker-Fallen, Apps und Abofallen: Für den Download von kostenlosen Programmen keine Adressdaten angeben. Vorsicht beim Klicken auf unbekannte Links. Seien Sie sich bewusst, dass Apps Kosten verursachen sowie sensible Nutzerdaten übertragen können. Apps nur über die offiziellen App-Shops installieren. Neben vielen seriösen Werbeangeboten gibt es auch Fallen, bei denen versteckt Bestellungen oder Abo-Verträge abgeschlossen werden. Hilfestellungen hierbei bietet die „Watchlist“ (www.watchlist-internet.at) oder die Internet Ombudsstelle (www.ombudsstelle.at).
7. Sichere Downloads, E-Mails: Programme nur von sicheren Websites (siehe Punkt 5) herunterladen. Informationen über den Entwickler einholen. Achtung vor „Phishing-Mails“ (von Passwort und fishing – engl. Angeln) – beschreibt Versuche, bei denen Leute über gefälschte Websites, E-Mails oder Kurznachrichten den Usern sensible Daten entlocken. Ziel ist es, an persönliche Daten zu gelangen um Kontoplünderungen oder auch Identitätsdiebstahl zu betreiben. Oft werden ähnlich klingende Mails verschickt, z.B. wie tiroll.com → ein Buchstabe zu viel. Vorsicht bei E-Mail Anhängen – keine unbekannten Anhänge öffnen. Dubiose Mails von Unbekannten sofort löschen.
8. Smartphone schützen: Moderne Handys sind Multimediazentralen und vereinen alle unsere Daten. Bluetooth abschalten, keine dubiosen Downloads machen, genau überprüfen, welche Daten Apps weitergeben und immer einen PIN festlegen. Auch beim Verwenden von öffentlichen WLAN Hotspots ist Vorsicht geboten. Diese sind oftmals nicht gesichert, daher sollten keine sensiblen Daten preisgegeben werden

(z.B. nicht für ein Online-Banking geeignet) und sich nicht auf Seiten einloggen, welche persönliche Informationen enthalten (auch nicht z.B. auf Facebook – obwohl die meisten „automatisch“ verbunden sind).
9. Bezahlung im Web: Beim Kauf von Waren im Internet ist allgemein Vorsicht geboten, insbesondere bei Vorauszahlung. Zur Bezahlung sollten Konto- und Kreditkartendaten über eine verschlüsselte, sichere Verbindung (siehe Punkt 5) übertragen werden. Zahlungen können per Lastschrift, Kreditkarte oder Rechnung erfolgen. Es gibt auch seriöse Bezahldienste, bei denen die Bankdaten einmalig hinterlegt werden. Vorkasse per Überweisung ist zwar weit verbreitet, gilt aber generell als sehr viel riskanter. Kettenbriefe, Aufforderungen Bankdaten per Mail zuzusenden etc. auch nicht weiterleiten. Achtung „Neffentrick“! Tipp: Österreichisches E-Commerce-Gütezeichen (www.guetezeichen.at).
10. Misstrauisch sein: Es gilt: Erst denken, dann klicken!

Quelle: InfoEck Jugendinfo (www.infoeck.at/) und Polizei Kriminalprävention „Schutz vor IT-Kriminalität“ (www.bundeskriminalamt.at), 19.05.2021.

5. Begriffe rund um Computer, Internet & Co verständlich erklärt

App	Als Apps werden Programme für Smartphones und Tablets bezeichnet. Der Begriff stammt aus dem Englischen und ist eine Kurzform von „Applications“ (Anwendungen). Es werden unzählige kostenlose und kostenpflichtige Apps zum Download angeboten. Tipp: nur vom offiziellen App-Store downloaden.
Attachment	Attachment ist ein englisches Wort und bedeutet auf Deutsch „Anhang“. Anhänge können beliebige Dateien wie Bilder, Videos, Texte, Programme und vieles mehr sein.
Bluetooth	Unter Bluetooth wird eine Datenübertragung zwischen zwei Geräten über kurze Distanz mit Hilfe von Funktechnik (WPAN, Wireless Personal Network) verstanden. Über das Einstellungsmenü kann die Funktion aktiviert werden.
Cyber-Crime	Unter dem Begriff Cyber-Crime wird die Computerkriminalität verstanden. Alle Straftaten, die mit Hilfe der Nutzung des Informations- und Kommunikationssystems begangen werden, sind unter dem Begriff Cyber-Crime zusammengefasst.
Cyber-Grooming	Cyber-Grooming beschreibt die Anbahnung sexueller Kontakte durch Erwachsene an Kinder und Jugendliche über digitale Medien, also Chatrooms, WhatsApp oder anderen sozialen Netzwerken. Dabei geben sie sich oftmals als Gleichaltrige aus.
Download (von Dokumenten, Apps etc.)	Download ist der englische Begriff für Herunterladen und bezeichnet die Übertragung von Daten aus dem Internet auf den eigenen Computer, das Smartphone oder das Tablet.

eBook	Der Begriff eBook kommt aus dem Englischen und heißt übersetzt „elektronisches Buch“. eBooks sind Bücher in digitaler Form, die auf eBook-Readern (z.B. Kindle, Archos, Kobo, Tolino, Trekstor etc.) gelesen werden können.
E-Commerce	Electronic Commerce ist eine elektronische Geschäftsabwicklung, die den Kauf und Verkauf von Waren und Leistungen über elektronische Verbindungen umfasst.
Fake News	Bei Fake News handelt es sich um Nachrichtenartikel, die bewusst falsche Informationen verbreiten um LeserInnen in die Irre zu führen. Manchmal handelt es sich bei Falschnachrichten aber um unbeabsichtigte Fehler, Gerüchte, Satire oder irreführende Berichte, die nicht gänzlich falsch, aber aus dem Zusammenhang gerissen wurden.
Fake Profil	In sozialen Netzwerken, wie z.B. bei Facebook, kommt es vor, dass Leute in ihrem Profil falsche Angaben über sich selbst machen. Manche geben sich als ganz andere Personen aus, andere laden geklaute Bilder hoch oder schummeln bei ihrem Geburtsjahr.
Firewall	Hard- oder Software, die zwischen Rechner oder lokale Netzwerke und öffentliche Netze geschaltet wird, um den Zugriff auf Rechner von außen durch unbefugte Dritte zu verhindern und so interne Daten zu schützen.
In-App-Käufe	Kostenlose Apps finanzieren sich oft über Werbeeinschaltungen oder so genannte „In-App-Käufe“. In-App-Käufe ermöglichen es innerhalb der Anwendung z.B. Zusatzfunktionen, Abos oder Spielguthaben zu kaufen, ohne einen klassischen Bestellvorgang zu durchlaufen. Zusatzinfo: Kann man auf dem Handy manuell ausschalten (bei iPhone) und bei Android mit einem Passwort bestätigen lassen.
IT	IT ist die Abkürzung von Informationstechnik und ist der Oberbegriff für alle mit der elektronischen Datenverarbeitung in Berührung stehenden Techniken.
Online und Offline	Online beschreibt den Zustand, dass man mit einem anderen Computer oder mit einem Kommunikationsnetz (z.B. Internet) verbunden ist. Offline beschreibt genau das Gegenteil. Man ist weder mit einem anderen Computer verbunden, noch mit einem Kommunikationsnetz.
Online-Banking	Online-Banking bedeutet Bankgeschäfte online durchzuführen, beispielsweise Kontostand abfragen, Überweisung absenden oder Dauerauftrag einrichten.
Online-Shopping	Online-Shopping bedeutet Einkaufen im Internet (über die Onlineshops bestimmter Geschäfte, Marken, AnbieterInnen).
Phishing Mail	Hierbei versuchen die Betrüger und Betrügerinnen über falsche E-Mails an die Zugangsdaten der Opfer zu gelangen.

	Wenn ein sogenannter „Phishing“-Angriff erfolgreich verläuft, wird von den gehackten Konten aus eine E-Mail an alle dort gespeicherten Konten verschickt. In dieser Notfall-E-Mail wird dann vorgegeben, dass der eigentliche Besitzer oder die eigentliche Besitzerin des E-Mail-Accounts Hilfe braucht und meist Bargeld benötigt.
Sexting	Unter „Sexting“ – zusammengesetzt aus „Sex“ und „Texting“ versteht man das Verschicken und den Austausch intimer Nachrichten bzw. selbstproduzierter Fotos und Videos.
Sextortion	Sextortion – zusammen gesetzt aus „Sex“ und „Extortion“ (engl. Erpressung) bezeichnet eine Erpressungsmethode, bei der eine Person mit Bild- und Videomaterial erpresst wird, dass sie beim Vornehmen sexueller Handlungen und/oder nackt zeigt.
Smartphone	Ein Smartphone ist ein Mobiltelefon mit erweitertem Funktionsumfang. Ähnlich einem Computer verfügt es über ein eigenes Betriebssystem und ermöglicht dadurch die Bedienung einer breiten Palette von Anwendungen.
Soziale Netzwerke/Social Media Plattform	Soziale Netzwerke dienen dazu sich mit anderen NutzerInnen zu unterhalten, Fotos, Videos und Links zu teilen, Interessensgruppen zu bilden und Kontakte zu knüpfen. NutzerInnen präsentieren sich darin mit einem eigenen Profil und können sich untereinander virtuell vernetzen. Beispiele sind Facebook, Instagram, …
Spam	Spam, oder auch Junk genannt, sind elektronisch übertragene Nachrichten, welche von der Empfängerin oder vom Empfänger nicht erwünscht sind. Meist enthalten solche Nachrichten Werbung und werden von der E-Mail-Software erkannt und in einen separaten Ordner gespeichert bzw. auffallend markiert.
Tablet / Tablet-PC / Tablet-Computer	Ein Tablet ist ein mobiler Computer (auch Tablet-Computer oder Tablet-PC), der über einen berührungsempfindlichen Bildschirm, dem sogenannten Touchscreen bedient wird. Die Bedienung und die Möglichkeiten sind meist denen von Smartphones ähnlich.
Viren	Ein Computervirus ist ein sich selbst verbreitendes Computerstörprogramm, das sich unkontrolliert in andere Programme einschleust und sich reproduziert.
WLAN / Wi-Fi / Wireless Local Area Network	WLAN (Wireless Local Area Network) ist die häufig synonym verwendete Abkürzung für ein lokales, drahtloses Funknetz, das den Zugang zum Internet ermöglicht.

Quellen: www.infoeck.at, www.mobiseniora.at, www.wirtschaftslexikon.gabler.de, www.saferinternet.at, 24.11.2022.