Europäisches Verbraucherzentrum Österreich
ECC-Net
www.europakonsument.at

Co-funded by the European Union

Eine Initiative der Europäischen Kommission und des VKI

Perfider Datenklau
Produktfälschungen
Grundlose Mahnungen
Vermeintliche Lottogewinne

So schützen Sie sich vor Internet-Kriminalität

Foto: VKI

Liebe Leserin, lieber Leser,

die Informations- und Netzwerktechnologien haben sich in den letzten Jahren rasant weiterentwickelt: Das Internet ist heute praktisch unverzichtbar und wir dringen immer weiter in die unendlichen Weiten des World Wide Web vor.

Alles geht heute viel schneller, man hat nahezu weltweit Zugriff auf seine Daten und vernetzt sich mit Freunden rund um den Globus. Allerdings hat dieser Fortschritt auch seinen Preis. Wir hinterlassen Spuren im Internet, ohne es zu bemerken, und sind anfällig für „Angriffe" von außen. Firewalls und Virenscanner wiegen uns in Sicherheit, bieten aber nicht in allen Fällen hundertprozentigen Schutz. Bekanntschaft mit Spam-Mails, Phishing oder Trojanern hat heutzutage wohl schon fast jeder Internetuser gemacht. Nicht selten auch mit finanziellen Folgen.

Die EU-Kommission sieht in der organisierten Internet-Kriminalität ein erhebliches Bedrohungspotenzial. Der Kampf gegen Cybergauner hat auf EU-Ebene daher allerhöchste Priorität.

Auf den folgenden Seiten schildern wir die gängigsten Methoden und Tricks von Internetbetrügern. Die Beispiele sind aktuell, aber darüber hinaus von grundsätzlicher Bedeutung. Denn aus unserer Beratungstätigkeit wissen wir, dass viele neue Fallen schon bekannten alten Mustern folgen. Wer die gängigsten Tricks schon kennt und aufmerksam bleibt, kann sich schützen und geht Betrügern nicht so schnell auf den Leim.

Das sieht auch die zuständige Generaldirektion für Gesundheit und Verbraucherschutz (DG SANCO) der Europäischen Kommission so, die diese Publikation finanziell unterstützt.

Sollten Sie dennoch Fragen zum Thema „Gefahren aus dem Internet" haben, dann erhalten Sie beim Europäischen Verbraucherzentrum kompetente und rasche Hilfe.
Weitere nützliche Informationen und Tipps finden Sie auf www.europakonsument.at, der Website des Europäischen Verbraucherzentrums Österreich.

Mag. Georg Mentschl
Europäisches Verbraucherzentrum Österreich

Wo Alarmanlagen machtlos sind

Die schöne weite Welt des Internets ist faszinierend und gefährlich zugleich. Einzeltäter und kriminelle Organisationen betreiben hier anonym und weltumspannend lukrative Geschäfte auf Kosten leichtgläubiger und unvorsichtiger Nutzer.

Kein Vorteil ohne Risiko

Cybercrime – also die Internetkriminalität – ist eine boomende Branche, gegen die Sicherheitstüren und Alarmanlagen machtlos sind, weil sie auf völlig anderen Wegen in unsere Privatsphäre eindringt. Sogar Sicherheitsexperten sind von der früher vertretenen Meinung, man könne ein Computersystem vollständig absichern, abgegangen. So wie in vielen anderen Bereichen unseres Lebens gibt es keine hundertprozentige Sicherheit.
Das Internet vorsichtshalber gar nicht mehr zu nutzen wäre allerdings so, also würde man aus Angst vor einem möglichen Unfall kein Fahrzeug mehr besteigen oder zur Vermeidung eines potenziellen Abhörversuchs nicht mehr mit dem Handy telefonieren. Dies wäre eine Überreaktion und in der Praxis auch gar nicht so leicht umsetzbar. Zu stark hat das Internet unseren beruflichen und privaten Alltag durchdrungen, zu zahlreich sind auch die positiven und nützlichen Seiten, von der einfachen Informationsbeschaffung bis hin zur Beschleunigung von Behördenwegen.
Doch was kann man tun, um nicht bei nächster Gelegenheit in die Falle zu tappen?

Kritisch bleiben

Es gibt im Computerbereich sehr wohl so etwas wie Sicherheitstüren und Alarmanlagen, nämlich in Form von Firewall und Virenscanner in Kombination mit regelmäßigen Software-Updates. Darüber hinaus ist es ganz wichtig, aufmerksam zu sein und kritisch zu bleiben, selbst wenn ein Angebot noch so verlockend klingt.
Damit Sie wissen, worauf Sie achten müssen und mit welchen oft unglaublichen Dingen Sie konfrontiert werden können, haben wir die gängigsten Spielarten von Cybercrime hier zusammengestellt. Manche dieser Betrugsmaschen sind älter als das Internet selbst, andere wiederum wurden erst durch die modernen Medien ermöglicht. Oft ist keine klare Abgrenzung möglich, denn die einzelnen Tricks kommen in unterschiedlichen Varianten daher. Für weitere Informationen und Hilfestellung im Ernstfall beachten Sie bitte auch die Seiten 7 und 8!

Spam und Scam

Wenn Sie Ihre E-Mail-Adresse verwenden, um sich z.B. bei einem Onlineshop anzumelden oder als Vereinsmitglied in einer Liste im Internet aufscheinen, werden Sie früher oder später mit Massen-E-Mails (Spam oder Junk-Mails genannt) beglückt. Suchroboter (Spambots) durchforsten das Internet nach Mailadressen, die dann automatisch angeschrieben werden. Neben allgemein gehaltenen Werbe-E-Mails ist auch vermehrt Scam im Umlauf. Das ist Spam mit gezielt betrügerischer Absicht. Mittlerweile werden von den Betrügern aber auch persönliche Kontakte über soziale Netzwerke wie Facebook geknüpft. Seien Sie zurückhaltend beim Akzeptieren von Freundschaftsanfragen Ihnen unbekannter Personen!

Wo Bruce Willis Viagra kauft

Aufgrund der Virengefahr ist es empfehlenswert, Spam-Mails nicht zu öffnen und erst recht nicht darauf zu reagieren. Sie enthalten ohnehin nur nutzlose Informationen, wie die Adresse, bei der Bruce Willis Viagra kauft oder Angelina Jolie Schlankheitspillen. Doch weder Willis noch Jolie kaufen dort, und Sie sollten ebenfalls die Finger davon lassen. Nicht nur, dass es verboten ist, Medikamente aus dem Ausland zu bestellen, handelt es sich meist um Fälschungen aus dubiosen Labors. Eine Einnahme kann unabsehbare Folgen für Ihre Gesundheit haben.

Falscher Luxus

Mit Sicherheit gefälscht sind Luxusgüter oder elektronische Waren, wie Uhren oder Smartphones, zu sagenhaft günstigen Preisen. Diesen begegnen Sie im Spam, in Onlineshops oder auf Auktionsplattformen. Die Produkte stammen in der Regel aus Asien, und die Wahrscheinlichkeit ist groß, dass Sie nach der Überweisung des Geldes nicht einmal die billige Fälschung in Händen halten, sofern diese vom Zoll abgefangen und vernichtet wird. Zudem drohen eine Verwaltungsstrafe oder die gerichtliche Verfolgung durch den Markeninhaber.

Gewinn ohne Aussicht

Überraschende Gewinne bei ausländischen Lotterien sind als Betrugsmasche ebenfalls beliebt, doch können Sie sich denken, wie groß die Wahrscheinlichkeit eines tatsächlichen Gewinns ist. Um diesen ausbezahlt zu bekommen, müssen Sie eine Bearbeitungsgebühr, sowie diverse „Steuern" oder Notariatsgebühren überweisen. Doch auf die Auszahlung warten Sie vergeblich. Oder Sie landen in der Endlosschleife einer Mehrwertnummer. Die gleiche Masche gibt es mit Erbschaften, die Ihnen eine entfernte Verwandte im ebenso fernen Ausland hinterlassen hat.

Freunde in Geldnot

Ein weiterer perfider Trick: Freunde, die im Ausland ohne Geld und Ausweis gestrandet sind und Sie per E-Mail um einen helfenden Geldbetrag bitten. In diesem Fall stammt die E-Mail von einem Ihnen bekannten Absender. Was weder er noch Sie wissen, ist, dass sein E-Mail-Konto gehackt wurde, d.h. ein Unbefugter hat sich Zugang verschafft und kontaktiert unter fremdem Namen die im Adressbuch gespeicherten Personen. In der E-Mail angegebene Telefonnummern führen unter Umständen zu einer Mehrwertnummer.

From Russia with love

Scam macht auch vor Kontaktanzeigen bzw. Online-Partnerbörsen nicht halt. Oft sind es deutschsprachige Männer, die dort z.B. russische Frauen kennenlernen, welche ihnen bald schon ewige Liebe schwören und sie dann bitten, ihnen mit Geld auszuhelfen. Hier wird mit Gefühlen Schindluder getrieben, denn diese Frauen existieren nicht. Selbst wenn sie Fotos bzw. Kopien von Dokumenten schicken, handelt es sich um Symbolfotos bzw. Fälschungen, hinter denen oft Betrüger stecken.

Spam zum Frühstück

Während Scam übersetzt Betrug und Junk Abfall bedeutet, hat der Begriff Spam eine eigene Geschichte: Eigentlich meint er Frühstücksfleisch in der Dose, bekannt als „Spiced Ham" (Kurzform: Spam). Zur Bezeichnung für die Flut an unerwünschten E-Mails wurde er über den Umweg eines Sketches der britischen Komikertruppe Monty Python, in dem das Wort innerhalb weniger Minuten mehr als hundert Mal fällt.

Bestellt und nicht geliefert

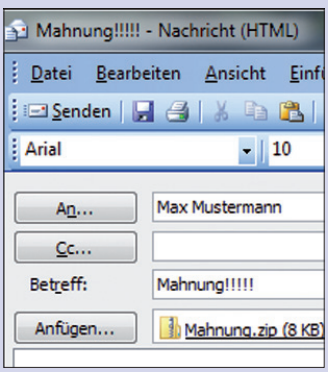
Die Nichtlieferung bestellter Waren ist ein weiteres Problem beim Online-Handel. Ein solches Risiko besteht nicht nur bei Anbietern, die über eine Online-Auktionsplattform (wie z.B. eBay) verkaufen oder auf einer Kleinanzeigenplattform inserieren. Betrüger stellen ganze Shops z.B. mit Elektronikartikeln online, die per Vorauskasse bezahlt werden müssen, aber niemals geliefert werden. Nach einiger Zeit wird der Shop wieder aus dem Netz genommen.

Unerwartete Zusatzkosten

Die Masche mit der Nichtlieferung funktioniert auch bei Autos oder Tieren, die sich im Ausland befinden. Für die Überstellung fallen diverse Gebühren an bzw. tauchen Probleme auf, die aber mit Geld aus der Welt geschafft werden können. Herr S. entdeckte z.B. auf einer österreichischen Kleinanzeigenseite ein Inserat mit Katzenbabys. Als er sein Interesse bekundete, erhielt er eine E-Mail aus London mit dem Hinweis, dass die Überstellung über eine Tiertransport-Agentur abgewickelt werde. In der Folge waren mehrere Überweisungen für Transfer, Versicherung, Futterkosten etc. nötig. Als Zweifel aufkamen, wurde Herr S. durch Androhung eines Gerichtsverfahrens unter Druck gesetzt. Am Ende hatte er mehr als 300 Euro bezahlt, ohne ein Kätzchen erhalten zu haben.

Abgemahnt

Früher einmal war die Zusendung unbestellter Billigwaren ein beliebter Trick, heute schicken die Betrüger per E-Mail Mahnschreiben, in der Hoffnung, dass möglichst viele Betroffene aus Furcht vor Konsequenzen bezahlen, obwohl sie die Bestellung nie getätigt haben. Es handelt sich bewusst um geringe Beträge, die hier eingefordert werden, damit die Bereitschaft zur Zahlung, um Ärger zu vermeiden, eher gegeben ist. Aktuell enthalten solche Mahnschreiben auch eine Zipdatei im Anhang. Wird diese angeklickt, dann nistet sich ein Trojaner (= eine Virusart) auf dem PC ein, der den Betrügern unter Umständen persönliche Informationen liefert oder ihnen den Zugriff auf den Computer ermöglicht.



Rip-Deals

Kehren wir zu den Inseraten zurück. Herr M. wollte über eine Immobilienplattform sein Haus verkaufen. Prompt meldete sich der Mitarbeiter eines wohlhabenden Interessenten aus dem Ausland. Zur Besprechung der Details sollte Herr M. nach Italien reisen. Dies ist ein typisches Beispiel für die Anbahnung von Rip-Deals, also Geldwechselbetrug. Beim persönlichen Treffen wird dem Verkäufer entweder vorgeschlagen, das Geschäft in bar abzuwickeln, er soll möglicherweise eine Vermittlungsgebühr entrichten, oder das Thema wird überhaupt auf den Devisentausch gelenkt und es wird für die Hilfsdienste eine hohe Provision in Aussicht gestellt, weil es sich um Schwarzgeld handelt und das Geschäft unter der Hand ablaufen muss. Wer gutgläubig zahlt, lässt sich nicht nur bewusst auf eine Straftat ein, sondern erhält im Gegenzug Falschgeld, präparierte Geldbündel oder überhaupt einen leeren Koffer.

Nigeria Connection

Nichts anderes als Rip-Deals sind auch die per Spam versandten Bitten um Unterstützung beim Transferieren eines hohen Geldbetrages ins Ausland. Bei diesem unter dem Namen „Nigeria Connection" bekannten Trick muss der Betrogene in Vorleistung treten, von der versprochenen Provision sieht er nichts.

Überweisung ins Nirgendwo

Geldtransfers via Western Union oder bargeldloses Bezahlen mittels Ukash-Code sind beim Internetbetrug sehr beliebt, weil das Geld der Gegenseite sofort zur Verfügung steht und nicht mehr zurückgefordert werden kann. Damit sollen die beiden Bezahlmöglichkeiten nicht grundsätzlich in Verruf gebracht werden, aber sie sind in diesem Zusammenhang ein Merkmal dafür, dass Vorsicht angebracht ist. Auch ein zwischengeschalteter Treuhänder oder ein Treuhandkonto sind keine Garantie dafür, dass alles mit rechten Dingen zugeht. Der Treuhänder existiert entweder nicht oder spielt bei der Sache mit.

Phishing im Trüben

E-Mails von Banken und Kreditkartenunternehmen dienen keinesfalls dazu, um die geheimen Kontodaten abzufragen oder bestätigen zu lassen, um „Testüberweisungen" durchzuführen oder um die Kreditkarte zu verifizieren. Password Fishing, kurz: Phishing, ist der Versuch, gutgläubigen Computernutzern diese Daten freiwillig herauszulocken, z.B. indem sie mittels Hyperlink auf eine täuschend echt wirkende Internetseite geleitet werden. Manchmal werden Sie auf diese Weise auch zum Software-Download aufgefordert. Es handelt sich dann um einen Trojaner, welcher Ihren Computer ausspioniert und darauf gespeicherte Daten an Unbefugte übermittelt.

Typosquatting

Ein an sich harmloser Fehler kann ähnliche Folgen wie das Phishing haben. Die Rede ist von Tippfehlern, wodurch eine Internetadresse falsch eingegeben wird (also z.B. Googel statt Google). Betreiber von betrügerischen Seiten (z.B. Download gefälschter Virenschutzprogramme, die selbst Viren sind) bzw. Abzock-Seiten haben sich solche täuschend ähnlichen Adressen gesichert, die sich minimal von den seriösen und bekannten unterscheiden. Man spricht hier von Typosquatting (englisch typo = Tippfehler; squatting = Hausbesetzung).

Internetabzocke

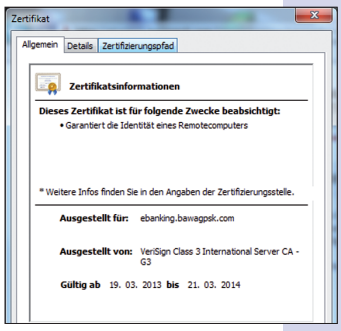
Klassiker des Internetbetrugs sind Abzock-Seiten. Ahnenforschung, Routenplaner, kostenlose Downloads, Gratis-Gedichte, Bastelanleitungen, Lebenserwartungsprognosen etc. – die Liste der Themen ist lang, die Masche immer die gleiche: Hier werden Ihnen Leistungen verkauft, die Sie auf anderen Seiten kostenlos bekommen. Durch unklare Angaben werden Sie dazu gebracht, sich voreilig anzumelden, ohne zu bemerken, dass Sie dadurch einen kostenpflichtigen Vertrag abschließen. Die böse Überraschung folgt in Form von Rechnungen bzw. Anwaltsbriefen, die Teil einer gezielten Zermürbungstaktik sind. Ob der Vertrag tatsächlich rechtsgültig ist, hängt von vielen Faktoren ab und muss im Einzelfall geprüft werden. Die Abzocker rechnen aber damit, dass die Betroffenen entnervt und eingeschüchtert das Handtuch werfen und bezahlen. Ausführliche Informationen und Musterbriefe dazu finden Sie auf www.europakonsument.at unter dem Punkt „Vorsicht Falle!/Internetabzocke".

Polizeitrojaner

Von Schadsoftware in Form von Trojanern war hier schon mehrfach die Rede. Seit einiger Zeit ist im Netz der so genannte Polizeitrojaner im Umlauf, der häufig über ein Java-Update auf den Computer gelangt und bisher nur Windows-PCs befallen hat. Er macht sich in Form eines plötzlich auftauchenden Fensters auf dem Bildschirm bemerkbar, während diverse Funktionen des Computers blockiert werden. Unter dem Deckmantel einer Behörde, der real nicht existierenden „Internet-Polizei", werden Sie eines Vergehens beschuldigt und dazu aufgefordert, durch Überweisung eines Geldbetrags die Computersperre rückgängig zu machen. Dies ist ein glatter Betrugsversuch. Sollte Ihr Computer von einem solchen Virus betroffen sein, wenden Sie sich am besten an ein Computerfachgeschäft oder suchen Sie – auf einem anderen Computer – auf der Internetseite des deutschen Bundesamts für Sicherheit in der Informationstechnik (http://bka-trojaner.de) nach erster Hilfe!

Verschlüsselt und zertifiziert

Online-Banking sowie Zahlungen jeder Art sollten im Internet ausschließlich über verschlüsselte Seiten erfolgen. Die Verschlüsselung samt Zertifikat ist auch eine Kontrolle für Sie, ob die Internetseite echt ist. Eines der Kennzeichen ist der Zusatz https statt nur http in der Adresszeile, ein anderes das Vorhängeschloss-Symbol. Manche Unternehmen verwenden Zertifikate mit erweiterter Überprüfung, dann ist die Adresszeile zusätzlich grün eingefärbt. Auf jeden Fall erhalten Sie durch Klick auf das Vorhängeschloss zusätzliche Informationen zur Zertifizierungsstelle sowie zum Unternehmen, das hinter der Internetseite steht.



Unsicheres Smartphone

Als Handys noch herkömmliche mobile Telefone waren, galten Mehrwertrufnummern als größte Bedrohung für die Geldbörsen der Besitzer. Dieses Risiko gibt es noch immer, doch in der Nutzung moderner Smartphones schlummern noch andere Gefahren. Immerhin handelt es sich bei diesen Geräten um (beinahe) vollwertige Computer, die aufgrund ihrer Verbreitung verstärkt zum Angriffsziel betrügerischer Aktivitäten werden. Dasselbe gilt für Tablets.

Apps als Spione

Eine potenzielle Sicherheitslücke sind Apps, die von den jeweiligen Plattformen heruntergeladen werden (Google Play/ Android, iTunes Store/iPhone, Windows Phone Store). Manche Entwickler versuchen sie für Spionagezwecke zu missbrauchen und wie die Erfahrung zeigt, ist nicht garantiert, dass die Sicherheitsvorkehrungen in den App-Stores einen solchen Versuch rechtzeitig erkennen. Das tendenziell größte Risiko besteht bei Android, weil dieses Betriebssystem aufgrund seiner weiten Verbreitung für Cybercrime-Attacken am interessantesten ist.

Im Zweifelsfall verzichten

Grundsätzlich gilt aber für alle Smartphones: Installieren Sie keine Apps, die wenige oder gar keine Bewertungen durch andere Nutzer haben bzw. die erst wenige Male heruntergeladen wurden. Achten Sie weiters darauf, welche Berechtigungen eine App einfordert. Einige davon möchten auf alle möglichen Bereiche Ihres Smartphones zugreifen dürfen, ohne dass die Notwendigkeit für die versprochene Funktion der App einsichtig ist. Im Zweifelsfall ist es besser, auf die Installation einer solchen App zu verzichten. Mittlerweile ist es weiters ratsam, auf Android-Smartphones eines jener Virenschutz-Apps zu installieren, die kostenlos bzw. – ausgestattet mit diversen Zusatzfunktionen wie etwa der Datensicherung – kostenpflichtig auf Google Play bereitstehen. Noch ein Tipp: Apps, die Sie nicht mehr verwenden, sollten Sie besser löschen.

Zurückhaltung beim Online-Banking

Online-Banking am Smartphone ist ein heikles Thema, insbesondere wenn Sie die elektronischen TANs, mit denen Sie Ihre in Auftrag gegebenen Überweisungen bestätigen, auf das selbe Gerät zugesandt bekommen. Auch wenn dies die praktischste Lösung ist, muss man aus Sicherheitsgründen davon abraten bzw. dazu, ihre Nutzung auf das notwendige Minimum zu beschränken. Wann immer es möglich ist, sollten Sie besser zu Hause über einen mit Virenschutz und Firewall ausgestatteten Computer ins Online-Banking einsteigen und sich die elektronischen TANs auf das Smartphone senden lassen. Durch die Aufteilung der beiden Schritte auf zwei Geräte minimieren Sie das Missbrauchsrisiko durch Angreifer von außerhalb.

Freizügiges WLAN

Ob Smartphone, Tablet, Netbook oder Notebook – kostenloses öffentliches WLAN in Flughäfen, Kaffeehäusern etc. ist praktisch

für unterwegs. Allerdings ist es ein Leichtes, die Kommunikation zwischen den einzelnen eingebuchten Geräten und dem Internet abzufangen, weil solche Netze in der Regel nicht abgesichert sind. Eine andere Variante ist, dass jemand in betrügerischer Absicht z.B. in einer dem Kaffeehaus benachbarten Wohnung ein paralleles Netz betreibt und man sich unbemerkt in dieses einbucht. Um es kurz zu machen: Über ein öffentliches WLAN-Netz sollten Sie niemals Überweisungen mittels Online-Banking durchführen oder Zahlungen tätigen, bei denen Sie z.B. Ihre Kreditkartendaten eingeben.

Hackerville

Wussten Sie schon? Die rumänische Stadt Râmnicu Vâlcea (rund 110.000 Einwohner) trägt auch den Spitznamen „Hackerville" und gilt als internationale Cybercrime-Hauptstadt. Tatsache ist, dass von hier aus ein großer Teil der professionell betriebenen Betrugsgeschäfte mit nichtgelieferten Waren und falschen Onlineshops gelenkt wird. Außerdem beschäftigten sich hier ansässige Hacker – immer wieder erfolgreich – mit der Beschaffung von Kreditkartendaten.

Risiken minimieren

Es gibt zwar nationale und internationale Einrichtungen, die sich mit der Bekämpfung von Cybercrime befassen, doch beim Schutz vor konkreten Betrugsversuchen ist jeder Nutzer persönlich gefordert. So sollte kein Computer ohne Virenscanner und Firewall ans Netz gehen. Die Firewall, die dazu dient, den ein- und ausgehenden Datenverkehr zu überwachen, ist sowohl unter Windows als auch unter Mac OS vorinstalliert. Vergewissern Sie sich, dass sie aktiviert ist.

Virenschutz und Updates

Vorinstallierten Virenschutz gibt es bisher nur unter Windows 8. Für alle anderen Computer empfiehlt sich der Download der „Microsoft Security Essentials" bzw. anderer kostenloser Virenscanner, wie „AntiVir – Avira Free Antivirus", „AVG Free Antivirus" oder „avast! Free Antivirus", um den Basisschutz zu gewährleisten. Kostenpflichtiger Virenschutz bietet darüber hinausgehende Sicherheitsfunktionen. Für Smartphones und Tablets gibt es zwar bisher keine Firewall, aber jene mit Android-Betriebssystem sollten ebenfalls mit einer Virenschutz-App versehen werden. Hinzu kommt dann noch in jedem Fall die Notwendigkeit regelmäßiger Updates der installierten Software bzw. des Betriebssystems, denn damit werden immer wieder auch neu entdeckte Sicherheitslücken geschlossen.

Besser mit Hausverstand

Neben den technischen Schutzvorkehrungen sollten Sie schlicht und einfach den Hausverstand einsetzen, wachsam sein und allzu blumige Versprechungen hinterfragen. Im Leben wird einem nichts geschenkt, warum sollte es also in der virtuellen Welt des Internets so sein?

Tipps für den Online-Kauf

Hundertprozentige Sicherheit, dass beim Online-Kauf von Waren oder Dienstleistungen immer alles reibungslos klappt, kann es nicht geben. Zum Schutz der Verbraucher hat die EU allerdings die sogenannte Fernabsatzrichtlinie erlassen. Diese fordert von den Online-Händlern die folgenden Angaben direkt auf der Internetseite:

1. die Kontaktdaten (zumindest Firmenname und Postanschrift, nicht nur E-Mail-Adresse)
2. die Beschreibung der wesentlichen Eigenschaften der Ware oder Dienstleistung
3. den Preis inklusive aller Steuern, Gebühren und Lieferkosten
4. die ausführliche Belehrung über das Rücktrittsrecht
5. die Einzelheiten zur Zahlung und Lieferung
6. die Gültigkeitsdauer des Preises oder Angebotes
7. die Mindestlaufzeit des Vertrages, wenn dieser eine dauernde oder wiederkehrende Leistung beinhaltet

Sind diese Angaben sowie zusätzlich die Allgemeinen Geschäftsbedingungen (AGB = „das Kleingedruckte") vollständig und leicht auffindbar, dann ist dies ein wichtiger Anhaltspunkt dafür, dass es sich um einen seriösen Händler handelt. Ein solcher verwendet weiteres eine verschlüsselte Verbindung zur Übertragung von persönlichen oder Kreditkartendaten und setzt Sie auch nicht zeitlich unter Druck.

Gemeinsam gegen Cybercrime

Seit Jänner 2013 ist bei der europäischen Polizei-Agentur Europol in Den Haag das Europäische Zentrum zur Bekämpfung der Cyberkriminalität (EC3) angesiedelt (www.europol.europa.eu/ec3). Seine Aufgaben sind die Analyse von kriminellen Aktivitäten im Internet sowie die Information und aktive Unterstützung der Mitgliedsstaaten bei deren Bekämpfung.

In Österreich wurde vom Innenministerium beim Bundeskriminalamt die Meldestelle Against Cybercrime eingerichtet. Haben Sie einen konkreten Verdacht, dass Sie mit kriminellen Aktivitäten konfrontiert sind, können Sie sich auch als Privatpersonen jederzeit dorthin wenden.

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

Sie können die Straftat auch auf jeder Polizeidienststelle melden und zur Anzeige bringen.

Rat & Hilfe

Europäisches Verbraucherzentrum Österreich
Mariahilfer Straße 81
A-1060 Wien
www.europakonsument.at

EUROPA-HOTLINE: 0810 810 225
Mo bis Fr von 9 bis 15 Uhr
(zum Regionaltarif von max. 0,0676 € pro Minute aus ganz Österreich)
E-Mail: info@europakonsument.at

10 Grundregeln gegen Internetbetrug

- Wählen Sie Passwörter sorgfältig aus, wechseln Sie diese gelegentlich und geben Sie Passwörter nicht weiter!
- Für Zahlungen im Internet nur sichere Verbindungen (https://...) verwenden, kein öffentliches WLAN benutzen.
- Seien Sie grundsätzlich sparsam bei der Weitergabe von persönlichen Daten, besonders bei Kontodaten.
- Alle Kontoauszüge regelmäßig kontrollieren!
- „Sie haben gewonnen …" sollte Sie grundsätzlich skeptisch machen. Besonders, wenn Sie an keinem Gewinnspiel teilgenommen haben.
- Keine Überweisungen an Unbekannte ohne Gegenleistung, etwa eine „Bearbeitungsgebühr", um einen „Gewinn" zu erhalten.
- Mails von unbekannten Absendern am besten ignorieren und auch bei neugierig machendem Betreff löschen.
- Zip-Dateien und Links in Mails von unbekannten Absendern nicht öffnen, sie können Viren und Trojaner enthalten.
- Grobe Rechtschreib- und Grammatikfehler und abenteuerliche Geschichten in E-Mails sind ein Hinweis auf dubiose Geschäftsanbahnung.
- Hausverstand walten lassen: „Zu schön, um wahr zu sein" – was unglaublich gut klingt, ist meist auch im Internet mit einem Haken verbunden.

Hilfreiche Adressen

www.europakonsument.at
Europäisches Verbraucherzentrum Österreich; Hilfe bei grenzüberschreitenden Verbraucherproblemen sowie Unterstützung bei Problemen mit Betrug im Internet und Internetabzocke

http://onlinesicherheit.gv.at
Österreichisches Portal mit Informationen zum Thema Sicherheit in der Informations- und Kommunikationstechnologie

http://bka-trojaner.de
Deutsches Bundesamt für Sicherheit in der Informationstechnik; Informationen und Hilfestellung rund um das Thema Polizei-Trojaner

www.europol.europa.eu/ec3
Europäisches Cybercrime-Zentrum; Informationen zum europaweiten Vorgehen gegen Cybercrime

www.bmi.gv.at/cms/BK/meldestellen/internetkrimina/start.aspx
Österreichische Meldestelle Against Cybercrime – bei konkretem Verdacht auf kriminelle Aktivitäten

http://ec.europa.eu/consumers/ecc/index_de.htm
Europäische Kommission; Netz der Europäischen Verbraucherzentren

www.konsumentenfragen.at
Das Konsumentenportal des Bundesministeriums für Arbeit, Soziales und Konsumentenschutz

www.konsument.at/onlineshopping
Verein für Konsumenteninformation; Tipps zum sicheren Onlineshopping

www.verbraucherrecht.at
Verein für Konsumenteninformation;
Informationen zum Verbraucherrecht in Österreich

www.saferinternet.at
ÖIAT; unterstützt vor allem Kinder, Jugendliche, Eltern und Lehrende beim sicheren Umgang mit digitalen Medien

Impressum

Herausgeber und Medieninhaber Verein für Konsumenteninformation,
Mariahilfer Straße 81, 1060 Wien, ZVR-Zahl 389759993
Verlags- und Herstellungsort Wien
Text Mag. Gernot Schönfeldinger
Fotos Titelseite: Hans-JoachimRoy / Shutterstock.com
Seite 4–5: Jiri Hera, Denis Opolja / Shutterstock.com
Seite 6: rangizz / Shutterstock.com, alle anderen Abbildungen: VKI
Druck Leykam Druck GmbH & Co KG, 7201 Neudörfl

Weitere Informationen zum ECC-Net finden Sie im Internet unter:
http://ec.europa.eu/consumers/ecc/index_de.htm

Europäisches Verbraucherzentrum Österreich ECC-Net
www.europakonsument.at

Co-funded by the European Union