

WWW **SICHER**
-IM-INTERNET.at



... für ganz Österreich



Password:

EINE INITIATIVE VON

MICROSOFT ÖSTERREICH, BANK AUSTRIA CREDITANSTALT, UPC, NIC.AT UND EBAY AUSTRIA

Microsoft[®]

Bank Austria
Creditanstalt
Ein Mitglied der UniCredit Group

UPC

nic.at
the austrian registry

ebay.AT

 **bmsk: SOZIALES UND
KONSUMENTENSCHUTZ**

WKO
WIRTSCHAFTSKAMMER ÖSTERREICH

JW
Junge Wirtschaft

seniorkom.at

Saferinternet.at
Das Internet sicher nutzen!

Ihre Sicherheit ist uns wichtig – das BA-CA Sicherheitsportal

Noch nie war es so wichtig, den PC vor Wurm und Co. zu schützen – und noch nie so einfach! Das BA-CA Sicherheitsportal bietet umfangreiche Informationen, wie Sie Ihren Computer sicher machen können.

Umfassende Information und konkrete Hilfe.

Die schon fast täglichen Warnungen vor Viren, Würmern und Co. verunsichern immer mehr Menschen. „Worauf muss ich besonders achten?“ und „Wie schütze ich meinen PC?“ sind daher zentrale Fragen vieler Internet-User.

Mit dem BA-CA Sicherheitsportal bietet die Bank Austria Creditanstalt konkrete Hilfe an.

Unter <http://sicherheit.ba-ca.com> erfährt man alles zu den Themen Virenschutz & Firewall, Spyware & Spam, sichere Passwörter und vieles mehr. Verwenden Sie eine Internetfirewall, installieren Sie ein Antivirenprogramm – und halten Sie beides aktuell. So lautet der erste und wichtigste Ratsschlag an alle Anwender.

Wer seinen Computer nicht schützt, macht es Datendieben leicht. Das gilt besonders für die Erstellung von sicheren Passwörtern. Vornamen, Geburtstage oder Filmtitel mögen leicht zu merken sein, sicher sind sie jedenfalls nicht. Im BA-CA Sicherheitsportal geben wir Ihnen wichtige Tipps zur sicheren Passwörterstellung – und sagen Ihnen welche Sie lieber meiden sollten.

Apropos Datendiebe: Mittels „Phishing“ – ein Kunstwort aus „password fishing“ – werden immer mehr vertrauliche Kundendaten wie Kreditkartennummern ausgespäht. Empfehlung der Bank Austria Creditanstalt: Geben Sie niemals vertrauliche Daten an einer für Sie ungewohnten Stelle ein! Mehr zum Thema Phishing finden Sie ebenfalls im BA-CA Sicherheitsportal.

Kinder und Internet. Internet und Online-Spiele sind bei Kindern höchst beliebt. Kinder und Eltern sind sich jedoch oftmals der Gefahren des Internets nicht bewusst. Das BA-CA Sicherheitsportal zeigt, wie man Sicherheit und Datenschutz für Kinder verbessert und bietet Spielregeln für die PC-Nutzung von Kindern.



Sicherheit für Unternehmen. Viele Inhaber kleinerer und mittlerer Unternehmen machen sich nicht allzu viele Gedanken um die IT-Sicherheit. „Meine Firma interessiert doch niemanden“, lautet die Argumentation. Und das ist leider falsch. IT-Sicherheit geht jeden an. Der Sicherheitsleitfaden gibt praktische Tipps, wie sich jeder Unternehmer schützen kann.

Sicherheit für Bankgeschäfte. Die Sicherheit der Kundendaten hat in der Bank Austria Creditanstalt höchste Priorität. „Sicherheit für Ihre Bankgeschäfte“ lautet daher auch ein eigener Bereich im Sicherheitsportal. Hier erfahren Sie, wie die BA-CA in den Bereichen Datenschutz, Datenübertragung und Datenverwahrung aktiv ist. So bietet das BA-CA OnlineB@nking mit der 128bit SSL Verschlüsselung und dem mobileTAN-Verfahren höchste Sicherheitsstandards.

<http://sicherheit.ba-ca.com>



Nur wer sich informiert, ist sicher im Internet

Immmer mehr Menschen surfen im weltweiten Netz – bereits jeder zweite Österreicher ist ein regelmäßiger Internet-Nutzer. Sicherheit im Internet ist daher bereits heute ein zentrales Thema. Gefahren lauern vielerorts und meist wird die Uninformiertheit von Internet-Anwendern ausgenutzt. Daher begrüße ich Initiativen wie Sicher-im-Internet, die zur Information der Bevölkerung beitragen. Es ist wichtig, bei den Internet Anwendern ein Bewusstsein zu schaffen: Der Einsatz von Firewalls und Antiviren Software sowie die Installation von Software-Updates schafft eine sichere Basis.

Das Bundesministerium für Soziales und Konsumentenschutz arbeitet aber auch eng mit der österreichischen Wirtschaft zusammen, um Betrugsfällen vorzubeugen und die Konsumenten im weltweiten Netz durch Aufklärung und Information vor Betrügern zu schützen.

Auf Europäischer Ebene wird es in den nächsten Jahren darum gehen, einheitliche Rahmenbedingungen zu schaffen und gleiche europäischen Standards im Internet zu realisieren. Hier ist die europäische Politik gefordert – dieses Thema ist in Bezug auf Konsumentensicherheit in den nächsten Jahren von besonderer Bedeutung.

Erwin Buchinger

Bundesminister für Soziales
und Konsumentenschutz

www.Sicher-im-Internet.at

Um die Nutzung des Internets sicherer zu machen, haben sich namhafte Partner aus Politik und Wirtschaft zu dieser österreichweiten Allianz zusammengeschlossen. Jeder Partner unserer Initiative bringt seine individuellen Erfahrungen und Kompetenzen ein und stellt Ihnen diese mittels der vorliegenden Broschüre und im Internet unter www.Sicher-im-Internet.at zur Verfügung. So stellen wir uns gemeinsam der Verantwortung für das zentrale Thema Online-Sicherheit.

Allerdings kann es im Internet ebenso wie im realen Leben keine hundertprozentige Sicherheit geben. Darum ist unsere Initiative auch und vor allem **eine Initiative für Ihre Eigen-Initiative.**

Nur wenn Sie als Internet-Nutzer das ganze Gefahrenpotenzial im Web erkennen und Ihr Verhalten darauf abstimmen, können Sie künftig das Web und all seine Möglichkeiten mit einem Höchstmaß an persönlicher Absicherung nutzen. Außerdem steht Ihnen Ihr Internet Service Provider gerne mit Rat und Tat zur Seite. Seriöse Internetprovider halten sich an die Regeln der ISPA (Internet Service Providers Austria), die z.B. den Umgang mit Spam genau festgelegt hat. So werden lästige E-Mails von vornherein blockiert, ohne dass Sie sich damit befassen müssen. Bei einigen Providern sind Schutzprogramme gegen Spam und Viren auch kostenlos im Produktpaket enthalten und bieten

Möglichkeiten, den persönlichen Schutz genau den individuellen Bedürfnissen anzupassen.

Wir zeigen Ihnen auf den nächsten Seiten, mit welchen Risiken Sie rechnen sollten, und wie Sie sich dagegen schützen können. Gleich vorne weg die wichtigsten drei Tipps für Ihre Sicherheit im Internet:

- 1. Verwenden Sie eine Internet Firewall**
- 2. Nutzen Sie aktuelle Software und laden Sie die Aktualisierungen herunter**
- 3. Verwenden Sie aktuelle Anti-Viren-Software**

Eine Orientierungshilfe durch den Fachbegriff-Dschungel

Auch wenn wir hier versuchen, Ihnen technische Begriffe möglichst gut zu erklären, kann es vorkommen, dass Ihnen das eine oder andere Wort nicht geläufig ist. Für diesen Fall haben wir ein „Glossar“ zusammengestellt. Es soll Ihnen Hilfe im Fachbegriff-Dschungel bieten. Sie finden es unter: www.Sicher-im-Internet.at

Herausgeber: Microsoft Österreich, Bank Austria Creditanstalt, Computer Associates, a.trust, eBay Austria und Inode.

Kontakt: Microsoft Österreich InfoService
0 8000 123-345, austria@microsoft.com
Alle Rechte, insbesondere Verbreitung, Übersetzung, Nachdruck, Wiedergabe auf photomechanischem Weg sowie elektronische Datenspeicherung bleiben ohne Zustimmung nur den Partnern der Initiative vorbehalten.

Erstauflage: Mai 2005, **2. Auflage:** Oktober 2007
2. Auflage: November 2007

Benutzen Sie eine Firewall!

Lassen Sie bei Ihrem Auto den Schlüssel stecken, den Motor laufen und die Türen geöffnet, wenn sie in den Supermarkt zum Einkaufen gehen? Natürlich nicht. Mit derselben Selbstverständlichkeit, mit der Sie Ihr Auto vor unbefugter Benutzung sichern, sollten Sie auch Ihren Computer vor fremden Zugriffen schützen. Eine Firewall erledigt das für Sie. Mit einer Firewall schützen Sie Ihren PC vor Angriffen aus dem Internet: Sie ist in der Lage, zwischen gewünschtem und unerwünschtem Datenverkehr zu unterscheiden. Eine Firewall gestattet nur jene Datenübertragungen, die Sie ausdrücklich zugelassen haben. Mit diesem Instrument können Sie daher den Computer vor Sicherheitsrisiken wie etwa dem Diebstahl Ihrer persönlicher Daten schützen.

Was ist eine Firewall?

Eine Firewall funktioniert wie ein Wächter, der jeweils prüft, was aus dem Internet abgerufen oder ins Internet übertragen wird. Gefährliche Daten oder Zugriffsversuche von verdächtigen Quellen können diese Barriere nicht überwinden. Das bedeutet auch, dass Hacker durch eine Firewall nur mehr sehr schwer auf Ihren Computer zugreifen können - Ihre vertraulichen Daten sind damit geschützt. Firewalls gibt es in unterschiedlichen Ausführungen. Für Private und kleine Unternehmen gibt es Firewalls als preiswerte Software, die im Computerfachhandel

als „Personal Firewall“ erhältlich ist. Im kostenlosen Windows XP Service Pack 2 ist bereits eine solche Personal Firewall enthalten. Diese wird bei der Installation auch gleich automatisch aktiviert. So sind Sie von Anfang an gut geschützt.



Durch eine Firewall sind Ihre vertraulichen Daten besser geschützt.

Für größere Unternehmen gibt es Unternehmensfirewalls. Diese gibt es als Server Software oder als Hardware in Form einer so genannten Appliance. Eine solche Unternehmensfirewall ist z.B. der Microsoft ISA Server.

Mehr Informationen zum Thema „Firewall“ finden Sie im Internet unter: www.Sicher-im-Internet.at

Hier wache ich.

Für mehr Sicherheit im Internet: Die Produkte von UPC.



Aktualisieren Sie Ihre Software - das schützt Sie und Ihren PC!

Heute wird in immer kürzeren Zeitabständen neue oder verbesserte Software auf den Markt gebracht. Dieses Tempo ist wichtig, um Ihnen Innovationen zu bieten und auch um bisher unbekannte Schwachstellen so rasch wie möglich zu beseitigen. Denn wo immer es Software gibt, gibt es auch Menschen, die diese Techniken missbrauchen und zur Gefährdung anderer Nutzer einsetzen.

Tausende Programmierer arbeiten kontinuierlich daran, Ihre Software sicher zu machen. Der Einsatz aktueller Software schließt jene Tore, die etwa Viren und Würmer zum Betreten Ihres PCs benutzen. Sie müssen nur darauf achten, dass Ihr PC immer über die neueste Software verfügt. Nahezu alle Softwarehersteller bieten Ihnen dazu die entsprechenden Möglichkeiten.

Es gibt zwei Wege, wie Sie Ihre Software auf dem neuesten Stand halten können: Besuchen Sie die Webseiten der Softwarehersteller und laden Sie die entsprechenden Aktualisierungen, so genannte „Updates“, auf Ihren PC.

Einfacher und komfortabler geht es mit der Funktion „automatische Aktualisierungen“, die meist in der Menüleiste der einzelnen Anwendungen zu finden ist. Wenn Sie diese Option aktivieren, müssen Sie nicht selbst nach Aktualisierungen suchen oder fürchten, dass Ihnen wichtige



Der Einsatz aktueller Software schließt jene Tore, die etwa Viren zum Betreten Ihres PCs benutzen.

Neuerungen entgehen. Ihr PC lädt die aktuelle Software herunter und installiert sie automatisch. Bei seriösen Unternehmen wie Microsoft werden dabei keine zusätzlichen Daten abgefragt.

Mehr Informationen zum Thema „aktuelle Software“ finden Sie im Internet unter:
www.Sicher-im-Internet.at

Ungebetene Gäste: Viren & Spam

Viren und Spam verbreiten sich im Internet oft rasant. Viren sind Computercodes, die sich an Programme oder Dateien heften und PCs bei Benützung dieser Dateien sofort infizieren. Das kann für Ihren PC und Ihre Daten sehr unangenehme Folgen haben. Die möglichen Auswirkungen der einzelnen Viren sind sehr unterschiedlich und variieren von lästigen kleineren Fehlfunktionen bis hin zu ernsthaften Problemen wie Datenverlust oder Hardwareschäden.

Geben Sie Viren keine Chance!

Mit speziellen Anti-Viren Programmen können Sie die ungebetenen Gäste bekämpfen. Diese Software durchsucht Ihren PC und befreit ihn von bekannten Computerviren. Um auch gegen neueste Viren einen vollständigen Schutz zu gewährleisten, muss das Anti-Virus-Programm regelmäßig aktualisiert werden: Sie sollten wöchentlich, zumindest aber einmal im Monat Ihren Virenschutz auf den letzten Stand bringen.

Gefahr durch Spam Mails

E-Mails mit kommerziellen oder illegalen Inhalten, die gleichzeitig an tausende Adressen geschickt werden, heißen Spam. Häufig enthalten Spam-Mails auch virenverseuchte Dateien. Mittels raffinierter Tricks werden die Empfänger zum Öffnen der verseuchten Datei verleitet.



Mit speziellen Anti-Viren-Programmen können Sie ungebetene Gäste auf Ihrem PC bekämpfen.

Dieses führt zur Infektion des PCs. Durch die Aktivierung der Junk-Mail Filter in Ihrem E-Mail Programm können Sie viele dieser lästigen E-Mails beseitigen. Um nicht selbst zur Spam-Plage beizutragen, sollten Sie außerdem keine Mails versenden, die dazu aufrufen, „an alle Bekannten weitergeschickt zu werden“.

Grundsätzlich gilt: Wenn Sie eine E-Mail mit einer Anlage von einem unbekanntem Absender erhalten, löschen Sie diese Mail sofort. Auch bei mitgeschickten Dateien von bekannten Absendern ist Vorsicht geboten: Der PC Ihres Geschäftspartners könnte infiziert sein. Fragen Sie hier besser nach, bevor Sie unbekannte und ungewollte Dateien öffnen.

Mehr Informationen zum Thema „Schutz vor Viren und Spam“ finden Sie im Internet auf: www.Sicher-im-Internet.at

Schützen Sie sich vor „Spionen“ auf Ihrem Rechner

Spyware nennt sich Software, die ohne Ihr Wissen Daten auf Ihrem Rechner sammelt und an Dritte weitergibt. Hat sich solch ein Programm auf Ihrem PC eingestellt, beginnt es mit dem Sammeln von Passwörtern, E-Mail-Adressen oder auch Daten über Ihr Surfverhalten im Internet. Diese Daten werden dann weitergeleitet und der befallene Rechner wird gezielt mit Werbung beschickt. Sie erkennen den Befall von Spyware z.B. daran, dass plötzlich gezielt Werbebanner (siehe: <http://de.wikipedia.org/wiki/Werbepbanner>) oder Popups (siehe: <http://de.wikipedia.org/wiki/Popup>) erscheinen - auch, wenn Sie nicht im Internet surfen.



Laden Sie niemals Software von einer nicht vertrauten Quelle herunter!

So genannte „Trojanische Pferde“ nisten sich ebenfalls auf Ihrem PC ein. Diese Programme tarnen sich als nützliche Soft-

ware, sie schädigen jedoch den befallenen Computer. Beispiele sind vermeintliche Sicherheitsupdates, die in Wahrheit die Firewall und den Virenschutz deaktivieren oder Bildschirmschoner, die hübsche Bilder anzeigen, im Hintergrund aber Programme zerstören.

Sicher vor Trojanischen Pferden mit Anti-Spyware-Programmen

Meist gelangen Trojanische Pferde beim Herunterladen von Programmen aus scheinbar legitimen Quellen auf Ihren PC. Laden Sie daher niemals Software von einer nicht vertrauenswürdigen Quelle herunter und installieren Sie keine Software, die Ihnen per E-Mail geschickt wird. Seriöse Unternehmen verschicken ihre Software niemals per E-Mail.

Spyware und Trojanische Pferde können Sie mit guten Anti-Spyware-Programmen von Ihrem PC entfernen. Teilweise sind diese auch gratis im Internet erhältlich. Nutzen Sie dazu offizielle, bekannte Unternehmens-Websites, wie z.B. von Computer Associates oder Microsoft. Mittels periodischer Aktualisierungen der Programme können Sie ihren PC vor Neubefall schützen. Diese Programme überprüfen Ihren PC auch regelmäßig auf Neubefall.

Mehr Informationen zum Schutz vor „Spyware“ und „Trojanischen Pferden“ finden Sie unter: www.Sicher-im-Internet.at

Über das Passwort Fischen

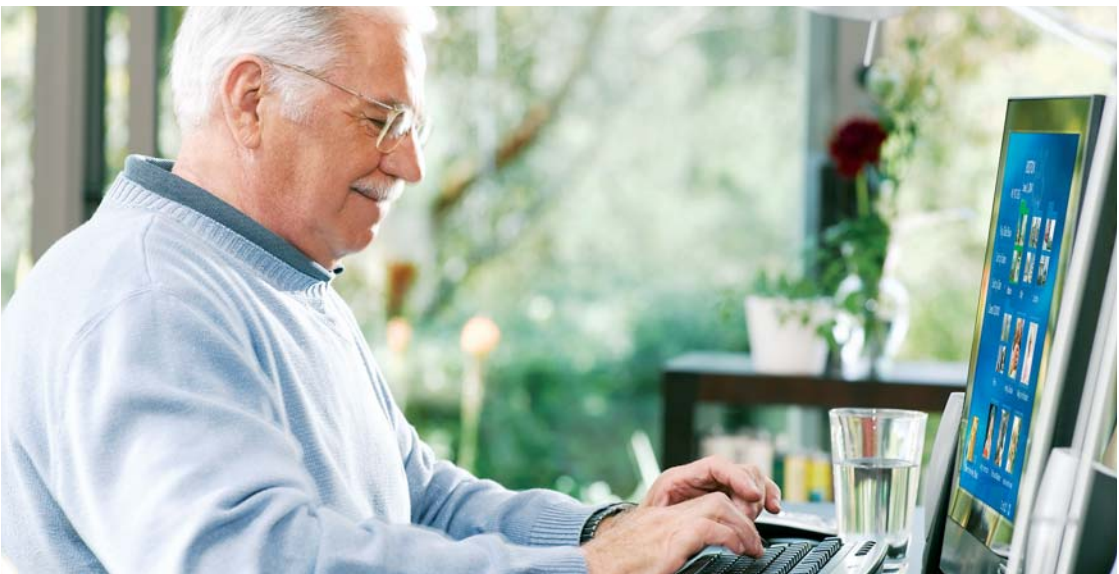
Hinter Phishing (Kunstwort aus „password“ und „fishing“) verbirgt sich eine Art des Betrugs im Internet. Meist wird versucht, über Spam-Mails (Massen-E-Mails) persönliche Informationen zu bekommen. Getarnt als seriöse Nachrichten beispielsweise eines Kreditinstituts fordern solche E-Mails den Empfänger zur Aktualisierung persönlicher Daten auf. Der Benutzer wird mittels Link auf eine scheinbar seriöse Website gelockt, die jener des jeweiligen Unternehmens täuschend ähnlich ist. Eine weitere gängige Methode ist es, bekannte Websites täuschend ähnlich nachzubauen und dort Kundendaten zu sammeln. Mit den ge-

stohlenen Daten verkaufen/kaufen die Datendiebe Ware oder sie bestellen mit Ihren Kreditkarteninformationen Waren über das Internet.

So schützen Sie sich vor Spam-Mails:

Seien Sie vorsichtig bei der Weitergabe Ihrer E-Mail-Adresse oder der Eintragung in Internet-Formulare. Gehen Sie davon aus, dass Ihre Angaben unter Umständen weitergegeben oder für andere Zwecke missbraucht werden.

Nutzen Sie Spam-Filter: Aktuelle E-Mail Programme haben eine Filter-Funktion



Nutzen Sie ein zweites Postfach für Online-Bestellungen, die Registrierung auf Internet-Seiten und die Bestellung von Newslettern.

(Phishing) und Spam-Mails

zum Schutz vor unerwünschten Mails. Aktivieren Sie diesen Filter für Ihr Postfach und testen Sie, welche Schutz-Einstellung zum besten Ergebnis führt. Fragen Sie auch den Internet-Anbieter, ob er einen Service zum Schutz vor Spam-Nachrichten anbietet.

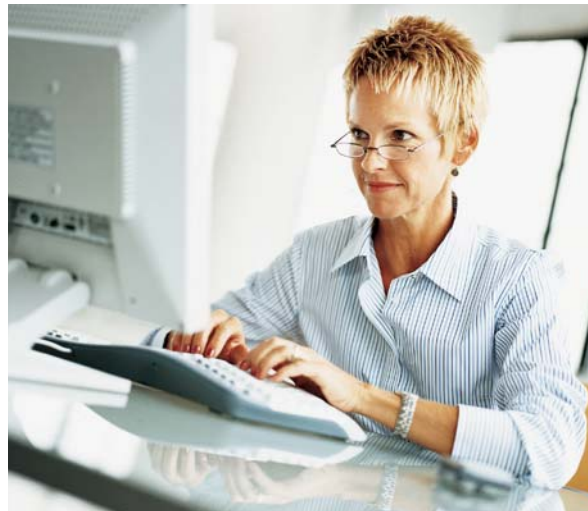
Nutzen Sie ein zweites Postfach für Online-Bestellungen, die Registrierung auf Internet-Seiten und die Bestellung von Newslettern. Solche zusätzlichen Postfächer können Sie bei vielen Internet-Anbietern kostenlos einrichten.

Antworten Sie nicht auf Spam-Mails. Auch der Versuch, die oft in Spam-Mails angebotene Funktion zum Austragen aus einer Verteilerliste zu nutzen, bewirkt keine Eindämmung der Spam-Flut. Diese Dinge helfen nur dem Spammer dabei, Ihre Mail-Adresse zu verifizieren.

Was tun gegen Phishing?

Das einfachste und effektivste Rezept, um Betrug durch Phishing zu vermeiden ist Wachsamkeit. Kein seriöses Unternehmen fragt Passwörter, Kreditkartennummern und ähnliches per E-Mail ab. Wenn ein solches Mail im Postfach aufscheint, ist es ein Trickbetrug – unabhängig davon wie überzeugend es aussieht. Übermitteln Sie daher keine vertraulichen Daten, wenn Sie per E-Mail dazu aufgefordert werden und setzen Sie sich zuerst

persönlich oder telefonisch mit dem angeblichen Absender-Unternehmen in Verbindung. Fragen Sie nach, ob das E-Mail tatsächlich seriös ist, bevor Sie Daten übermitteln. Besonders wichtig: Geben Sie Ihre persönlichen Daten niemals auf Internetseiten ein, deren Link Sie per E-Mail erhalten haben.



Antworten Sie auf keinen Fall auf Spam-Mails.

Mehr Informationen zu den Themen „Spam-Mails und Phishing“ finden Sie unter: www.Sicher-im-Internet.at

Sicherheit im Internet beginnt beim eigenen Namen



Die Zeiten der auf blumenladen_lisi@hotmail.com oder ähnlich lautenden geschäftlichen E-Mailadressen sind vorbei. Unternehmer setzen heute auf ihren Namen, der – auch und gerade im Internet – für sie selbst, ihr Produkt, ihre Geschäftsidee steht. Unternehmer haben erkannt, dass ein professioneller und seriöser Internetauftritt ein wichtiger Erfolgsfaktor ist. Der eigene Name wird zur Visitenkarte, zu einem Link zwischen virtueller und realer (Geschäft-)Welt. Eines steht fest: Es gehört auch für Privatpersonen, zum „guten Ton“, auf seine eigene Namens-Website zu verweisen. Der starke Trend hin zu virtuellen Networking-Plattformen wie Xing, Myspace oder Facebook macht deutlich: Es geht um Inszenierung und Präsentation der „Marke Ich“. Und der eigene Name ist Kern dieser Marke.

Namen sichern – bevor es jemand anders tut

Das Bewusstsein, dass man als Privatperson kein persönliches Recht auf seine Namensdomain hat, ist kaum vorhanden. Anders gesagt: Ist mein www.nachname.at einmal vergeben, habe ich schlichtweg Pech gehabt. Daher der Rat an alle User: Sicherheit hört nicht bei Firewall, Software Update und Antiviren-Software auf, sondern beginnt bei der Absicherung der eigenen Domain(s). Spitzname, Kosename, Event-Homepage, die Namen der Kinder,... Der Vielfalt sind im Internet keine Grenzen gesetzt. Unbedingt den eigenen Namen absichern, bevor es jemand anderer tut. Alle Informationen rund um Namensdomains sowie die Kontaktdaten von Registraren in Ihrer Nähe finden Sie auf www.at-partner.at

Bleiben Sie auf der sicheren Seite – schützen Sie sich vor illegaler Software

Lange hat Herr Müller für einen neuen PC gespart. Um nicht über den Tisch gezogen zu werden, hat er bei verschiedenen Händlern nach dem günstigsten Angebot gesucht. Ein Händler überzeugt ihn schlussendlich mit einem besonders reizvollen Angebot: Zum PC gibt es kostenlos eine Microsoft Windows Vista und Office 2007 Edition, die gleich auf den Rechner gespielt werden. Wer würde da schon „Nein, danke!“ sagen? Das Schnäppchen hat aber einen Haken: Die Lizenzierung für die beiden Softwareprodukte bekommt Herr Müller nicht. Nichts ahnend macht er sich damit strafbar. Tatbestand: Keine Lizenzierung.

Damit Sie sich optimal vor illegaler Software schützen können, hier einige Tipps:

Erkundigen Sie sich vor dem Kauf über die üblichen Preise der Produkte (z.B. in Katalogen und Fachzeitschriften).

Achten Sie beim Kauf – auch im Internet – auf die Originalverpackung, den kompletten Lieferumfang, alle Dokumentationen und die Art der Lizenz- und Upgrade-Möglichkeiten.

Vorsicht bei Einzelkomponenten wie z.B. Echtheitszertifikat: Die meisten Unternehmen vertreiben in der Regel keine derartigen Einzelkomponenten.

Achtung bei Compilation CDs, die mehrere Produkte von verschiedenen Herstellern umfassen: Die gängigen Hersteller vertreiben ihre Produkte nicht auf solchen Compilation CDs.

Achten Sie beim Kauf auf das Verpackungsdesign: Schlampige Verpackung, schlechte Farbqualität sowie nachgemachte Hologramme können ein Indiz für Fälschungen sein.

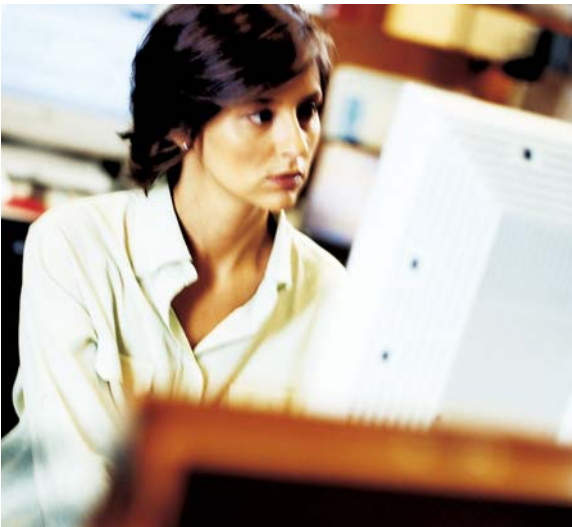


Informieren Sie sich schon vor dem Kauf um später viel Freude mit Ihrer neuen Software zu haben.


Mehr Informationen zum Thema „Schutz vor illegaler Software“ finden Sie im Internet unter: www.Sicher-im-Internet.at

Sicher Online Banking verwenden

Bankgeschäfte lassen sich über das Internet einfach und bequem abwickeln. Das spart den Anwendern Zeit und Geld. Besonders wichtig ist dabei aber das richtige Verhalten, um Ihre Sicherheit beim Online-Banking zu gewährleisten. Wir haben für Sie einige Tipps zusammengestellt:



Viele österreichische Banken bieten bereits die Möglichkeit der digitalen Signatur.

1. Sichere Verbindung: Ein kleines, abgesperrtes Schloss  zeigt Ihnen, dass eine sichere Kommunikation gewährleistet ist. Sie finden dieses Schloss entweder in der unteren Statuszeile des Browsers oder neben der Adresszeile. Ein Doppelklick auf das Icon verrät Ihnen Details zur Verschlüsselung und Schlüssellänge.

2. Passwörter, PIN und TAN sicher verwalten:

Mitarbeiter von Banken werden Sie nie nach Ihren Zugangsdaten wie Kontonummer, Verfügernummer oder Passwort fragen. Sollten Sie entsprechende Anfragen per Mail oder Telefon erhalten, handelt es sich höchstwahrscheinlich um Betrüger. Speichern Sie Ihre Passwörter, PIN und TAN nicht auf Ihrem PC, um diese Nummern vor unbefugtem Zugriff zu schützen. Für den Notfall haben alle großen Bankinstitute Telefonhotlines eingerichtet, an die Sie sich vertrauensvoll zwecks Sperrung Ihrer Zugangsdaten wenden können.

3. Ändern Sie Ihre PIN regelmäßig, um sich zu schützen:

Ihre neue PIN sollte nicht auf Tastenkombinationen wie z.B. „1111“, das eigene Geburtsdatum oder die letzten Ziffern Ihrer Handynummer lauten, denn solche Kombinationen sind leicht zu erraten und vermindern Ihre Sicherheit.

4. Benutzen Sie beim Online Banking den Logout-Button:

Beenden Sie Ihre Bankgeschäfte ausschließlich durch die Betätigung des Logout-Buttons. Damit nehmen Sie einem Angreifer alle Chancen, Einblicke in Ihre Daten zu nehmen.

Mehr Informationen zum Thema „Sicheres Online Banking“ finden Sie unter: www.Sicher-im-Internet.at

Kaufen Sie sicher im Internet ein - Online Shopping Sicherheitstipps

Das Internet ist der größte Marktplatz der Welt: Es bietet vielfältige Möglichkeiten zum bequemen Online-Shopping auf Kaufportalen und Versteigerungs-Plattformen. Allerdings ist Vorsicht geboten, denn auch im Internet gibt es Betrüger. Mit einigen grundlegenden Vorsichtsmaßnahmen können Sie sich aber wirkungsvoll schützen: Der beste Schutz vor Online-Betrügern ist eine ausgeprägte

Speziell bei Online-Auktionen gilt: Seriöse Verkäufer werden Ihre per E-Mail zum Produkt geäußerten Fragen bestimmt beantworten. Lesen Sie vor dem Kauf die Bewertungen des Verkäufers und benutzen Sie ein Treuhandkonto, wenn der Kaufpreis 200,- Euro übersteigt. Diese Treuhandkonten bieten Ihnen Sicherheit, da sie eine neutrale Position zwischen Verkäufer und Käufer einnehmen und



Bei Online-Auktionen gilt: Seriöse Verkäufer werden Ihre per E-Mail zum Produkt geäußerten Fragen bestimmt beantworten.

Skepsis. Senden Sie daher niemals E-Mails, in denen Ihre Kreditkartennummern oder andere wertvolle Daten enthalten sind. Unverschlüsselte E-Mails können von jedermann gelesen werden.

Nutzen Sie für Online-Einkäufe keine öffentlichen Internetzugänge wie etwa Internet-Cafés. Kleine Spionageprogramme sind in der Lage Ihre Tastatureingaben bzw. Daten aufzuzeichnen und an unbefugte Personen weiterzugeben.

eine Zahlung nur dann weiterleiten, wenn die Ware in einem ordnungsgemäßen Zustand beim Empfänger angekommen ist. Sollte doch einmal etwas schief gehen: Melden Sie den Vorfall dem Online-Auktionshaus, damit entsprechende Schritte von Seiten des Auktionshauses gesetzt werden können.

Mehr Informationen zum Thema „Online Shopping“ finden Sie unter: www.Sicher-im-Internet.at

Sicheres Verhalten rund um das Internet

Die IT in Unternehmen ist unterschiedlichen Gefahren ausgesetzt. Neben externen Bedrohungen wie Viren und Spam bestehen auch interne Gefahren. Oft sind dabei – meist unwissentlich – Mitarbeiter mitverantwortlich. Hier einige Tipps, die den Umgang mit dem Internet im Unternehmen sicherer machen:

- **Passwörter für PC, E-Mail** oder andere Programme im Unternehmen sind vertrauliche Daten. Einfach zu erratende Wörter wie der eigene Vorname oder Zeichenfolgen wie „1234“ scheiden da-

Klebezettel, mit dem das Passwort am Monitor fest gehalten wird. In diesem Fall ist ein Passwort so sinnvoll wie ein teures Schloss, an dem der Schlüssel stecken gelassen wird.

- **Information** ist **bei Sicherheitsfragen** wichtig: Mitarbeiter müssen über die Gefahren und möglichen rechtlichen Konsequenzen, die durch das Herunterladen von Software entstehen können, informiert sein. So können zum Beispiel in Bildschirmschonern Trojanische Pferde eingearbeitet sein, die das Netzwerk zerstören. Von einzelnen



Mitarbeiter müssen über die Gefahren, die durch das Herunterladen von Software entstehen können, informiert sein.

her als Passwörter aus. Auch einheitliche Passwort-Systeme für Abteilungen sind problematisch, da sie ebenfalls leicht zu erraten sind. Allerdings führen zu komplexe Zeichenfolgen oft zum berüchtigten

Mitarbeitern installierte Programme können lizenzpflichtig sein und somit unwissentlich illegal eingesetzt werden. Das kann schwerwiegende rechtliche Konsequenzen für das Unternehmen zur Folge haben.

im Unternehmen – einige weitere Tipps

- **Vertraulichkeit im Internet:** Online-Tagebücher, Chats und Foren erfreuen sich großer Beliebtheit. Diese Anwendungen sind allerdings kein Privatbereich, der nur von einigen wenigen Internet-Benutzern besucht wird, sondern öffentlich und meist frei zugänglich. Jede Information, die ein Mitarbeiter über die aktuelle Situation seines Unternehmens im Internet schreibt, steht für viele Personen zur Verfügung und kann zu schwierigen Situationen für das Unternehmen und den Mitarbeiter führen.

- **Firmen-E-Mail Adressen** sollten besonders sorgsam verwaltet werden, um eine Spamflut und Überlastung der Mail-Server zu vermeiden. Mitarbeiter sollten daher ihre Unternehmens Email-Adresse nur für berufliche Belange verwenden. Auch die Auflistung von Email-Adressen auf Unternehmens-Websites sollte mit Bedacht durchgeführt werden: Damit diese Adressen nicht in automatischen Spam-Mail Verzeichnissen landen, ist eine Darstellung als Grafik zu empfehlen.

Klare IT-Sicherheitsrichtlinien für Unternehmen

Unternehmen sollten in schriftlicher Form dokumentieren, welche Sicherheitsmaßnahmen in der jeweiligen Organisation von allen Mitarbeitern zu beachten sind. Bestandteil einer guten Sicherheitsrichtlinie sind umfangreiche Information sowie

klare Handlungsempfehlungen.



Sicherheit im Unternehmen beginnt beim Mitarbeiter.

Zu einem erfolgreichen Sicherheitskonzept gehören auch Schulungen und Informationen für Mitarbeiter. Diese müssen regelmäßig wiederholt und aktualisiert werden, um einen gleichmäßig hohen Sicherheitsstand zu gewährleisten. Dadurch kann sichergestellt werden, dass alle Anwender die für sie relevanten Sicherheitstipps kennen und auch befolgen.

Mehr Informationen zum Thema „Sicheres Surfen im Internet“ finden Sie unter: www.Sicher-im-Internet.at

Sicherheits-Check: Tipps zur Wartung des Computers

Ihr PC und Ihr Auto haben etwas gemeinsam: Beide müssen regelmäßig gewartet werden. Ihr Computer braucht zwar keinen Ölwechsel, Sie sollten aber Ihre Software aktualisieren, das Abonnement für das Antivirus Programm regelmäßig erneuern und den Computer auf Spyware prüfen. Folgende Aufgaben sollten zu Ihrem Pflichtprogramm gehören:

1. Melden Sie sich für E-Mail-Benachrichtigungen über Software-Updates an: Die meisten Software Hersteller informieren Sie per E-Mail, sobald ein Software Update verfügbar ist. Das ist besonders für das Betriebssystem, das Antivirusprogramm und die Firewall wichtig.



PC und Auto haben etwas gemeinsam: Beide müssen regelmäßig gewartet werden.

2. Installieren Sie Software Updates sofort: Wenn Sie eine Benachrichtigung für ein Update bekommen, laden Sie es herunter und installieren Sie das Update.

Zusätzlich zu diesen Schritten empfehlen sich regelmäßige Wartungsarbeiten. Nehmen Sie sich jede Woche etwas Zeit für Ihren PC – es lohnt sich.



Regelmäßige Wartungsarbeiten für den PC lohnen sich!

1. Sichern Sie Ihre Dateien: Beim Sichern Ihrer Dateien erstellen Sie eine Kopie der Computerdateien. Diese können Sie im Falle des Verlustes der Originale verwenden.

2. Prüfen Sie alle Dateien mit einem aktuellen Anti-Virus-Programm: Lassen Sie Ihr Antivirus Programm regelmäßig nach Computerviren und Würmern suchen. Bei den meisten Antivirus-Programmen lassen sich diese Prüfungen automatisch einstellen.

3. Ändern Sie Ihre Passwörter: Wenn Sie immer das gleiche Passwort verwenden, lässt es sich leichter ausspionieren. Ändern Sie regelmäßig alle Ihre Kennwörter, um Ihre Sicherheit zu verbessern.

Mehr Informationen zum Thema „Sicherheits-Check“ finden Sie unter: www.Sicher-im-Internet.at

DIE 3 FRAGEN FÜR SICHERES ONLINE SHOPPING

Wie im Alltagsleben, so sollten auch Internetnutzer beim Handel über eBay ihrem gesunden Menschenverstand vertrauen. Kaufen Sie niemals, ohne sich vorher ausreichend zu informieren, so wie Sie es sonst auch machen. Die folgenden 3 einfachen Fragen sollen Ihnen dabei helfen:

1) WER ist der Verkäufer?

Informieren Sie sich ausführlich über den Verkäufer bevor Sie ein Gebot abgeben oder einen Artikel kaufen:

eBay bietet Ihnen eine Transparenz, die es sonst nicht gibt: das Bewertungsprofil. Jedes eBay-Mitglied hat ein Bewertungsprofil, in dem Käufer und Verkäufer die Transaktionen gegenseitig beurteilen. Sehen Sie sich das Bewertungsprofil Ihres potentiellen Verkäufers an, es gibt Aufschluss über die Qualität des bisherigen Verhaltens des Verkäufers bei eBay.

2) WAS kaufe ich?

Informieren Sie sich ausführlich über den Artikel bevor Sie ein Gebot abgeben oder einen Artikel kaufen:

Lesen Sie sich die Artikelbeschreibung genau durch. Beachten Sie auch Informationen zu Zahlung und Versand des Artikels und vergleichen Sie den Artikel mit anderen, gleichartigen Artikeln. Nehmen Sie Kontakt mit dem Verkäufer auf (z.B. bezüglich Gebrauchsspuren, Höhe der Versandkosten, Rückgabebedingungen).

Stellen Sie dem Verkäufer Fragen zum Angebot, indem Sie einfach auf den Link „Frage an den Verkäufer“ oben rechts auf jeder Artikelseite klicken. Ein verantwortungsvoller Verkäufer wird Ihnen gerne und ausführlich antworten.

Seien Sie besonders kritisch, wenn Neuware zu einem Festpreis eingestellt ist, der deutlich unter der Preisempfehlung des Herstellers liegt.

3) WIE bezahle und bekomme ich den Artikel?

Informieren Sie sich ausführlich über Versandkosten und Versanddauer sowie die akzeptierten Zahlungsmethoden des Verkäufers bevor Sie ein Gebot abgeben oder einen Artikel kaufen:

Sollten Sie versicherten Versand bevorzugen, damit die Sendung nachverfolgt werden kann, klären Sie dies mit dem Verkäufer vorab ab. Für hochpreisige Artikel empfiehlt eBay die Verwendung von Treuhandservices.

Wählen Sie ein sicheres Bezahlungssystem wie z.B. Überweisung, Kreditkarte, PayPal, Nachnahme oder Barzahlung bei Übergabe. Bargeldtransfers wie z.B. Western Union dürfen von Verkäufern bei eBay nicht angeboten werden.

Mehr zum sicheren Online-Shopping finden Sie auf dem Sicherheitsportal von eBay.at:
www.ebay.at/sicherheitsportal

Bist du dir sicher – mit uns Dreien?

Und wie! Mit uns beiden auf den ersten Blick, mit meinem PC auf den ersten Klick.

Dank der Programme von Microsoft. Die sind einfach, aktuell, schnell und automatisch sicher, vom Start weg. Klar gehört meine Software gepflegt – wie meine Beziehung auch.

Das ist aber einfach und geht sehr schnell. Wie?

Hilf auch Du Deinem PC sicherer zu sein.

Mit nur drei einfachen Schritten schützt Du ihn vor den Gefahren des Internets.

www.microsoft.com/austria/PC-Schutz

Mit regelmäßigen Aktualisierungen bin ich auf dem sichersten Stand – und damit voll entspannt. Für noch mehr Sicherheit: Zuerst Augen auf, dann erst E-Mail auf. Egal ob beim Surfen oder Mailen, beim Shoppen oder Banken:

Mit den Programmen von Microsoft bin ich mir ganz sicher.