

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



... in Unternehmen

EINE INITIATIVE VON

MICROSOFT ÖSTERREICH, BANK AUSTRIA CREDITANSTALT, COMPUTER ASSOCIATES, EBAY AUSTRIA UND INODE.

Microsoft

Bank Austria
Creditanstalt


Computer Associates

ebay.AT

Inode

BM.I 

bm:bwk

JW
Junge Wirtschaft

WKO
WIRTSCHAFTSKAMMER ÖSTERREICH

senior**kom.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 Ratschlag 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 „Passwort 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. Ganz neu im BA-CA Sicherheitsportal ist der Bereich „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 PIN/TAN-System höchste Sicherheitsstandards.

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

Sicher im Internet



Die modernen Informations- und Kommunikationstechniken bieten enorme Möglichkeiten und Chancen und erleichtern dem Menschen in vielen Bereichen das tägliche Leben.

So angenehm diese Erscheinungen einer modernen Gesellschaft sind, so bergen sie doch auch unterschiedliche Bedrohungen in sich.

Jeder, der mit einem Computer arbeitet, weiß, dass die persönliche Sicherheit auf unterschiedlichste Weise beeinträchtigt werden kann. Das Spektrum reicht von Hacker-Angriffen bis zu Viren, die sich über das Internet verbreiten.

Diese Verletzungen der Sicherheit können enorme Kosten und immense Probleme in der Kommunikation und der Arbeit mit dem PC und dem Internet verursachen.

Verhütung und Bekämpfung der Kriminalität

Das Bundesministerium für Inneres arbeitet bei der Verhütung und Bekämpfung von Kriminalität im Bereich der Informationstechnik intensiv mit der Wirtschaft zusammen und unterstützt Projekte, die das weltweite Datennetz für den Benutzer sicherer machen. Ein sicheres und zuver-

lässiges Internet hebt die Akzeptanz der Nutzer für E-Commerce.

Computergeräte und Informationsdienste werden nur dann überzeugend sein, wenn diese so zuverlässig sind, dass wir uns über deren Sicherheit keine Gedanken mehr machen müssen.

Die Initiative „Sicher im Internet“

www.Sicher-im-Internet.AT, bei der führende Unternehmen und Institutionen zusammenarbeiten, trägt dazu bei, die modernen Informations- und Kommunikationsnetze sicherer zu machen.

Liese Prokop
Bundesministerin für Inneres

Keine Airbags, kein ESP, kein ABS.



**Und trotzdem machen
wir das Internet sicher.**

Sicherheit ist nicht nur im Straßenverkehr wichtig, sondern auch im Datenverkehr. Darum garantieren Ihnen die maßgeschneiderten Breitbandlösungen von Inode ein sorgenfreies Arbeiten: Mailversand, Downloads und Datenverkehr mit dem Höchstmaß an Sicherheit. Damit Ihre Daten nur dort hinkommen, wo sie auch wirklich hingehören.



WIR SIND DIE GUTEN

www.inode.at

Sicherheit ist wichtig für den Wachstumsmotor der heimischen Wirtschaft



Die Junge Wirtschaft vertritt die neue Generation in der Wirtschaft: Die 100.000 jungen Unternehmen Österreichs, die nachweislich der Wachstumsmotor der heimischen Wirtschaft sind.

Im digitalen Zeitalter wird ein Großteil Ihrer Geschäfte übers Netz abgewickelt – von der Unternehmenspräsentation via Homepage über die tägliche Kommunikation mit Geschäftspartnern per E-Mail bis zur elektronischen Zahlungsabwicklung.

Sicheres Arbeiten im Internet - erfolgreiches Wirtschaften

Für erfolgreiches Wirtschaften ist ein sicheres Internet unerlässlich. Deshalb unterstützt die Junge Wirtschaft Österreich die **„Sicherheit-im-Internet“-**Initiative.

Mag. Rainer Ribing
Bundesgeschäftsführer
Junge Wirtschaft Österreich

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. Wir stellen Ihnen diese mittels der vorliegenden Broschüre und im Internet unter www.Sicher-im-Internet.AT zur Verfügung. So nehmen wir uns gemeinsam der Verantwortung für das zentrale Thema Online-Sicherheit an.

Allerdings kann es im Internet ebenso wie im realen Leben keine hundertprozentige Sicherheit geben. Darum ist unsere Initiative auch **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 Internet 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, 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

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



Durch eine Firewall sind Ihre vertraulichen Daten besser geschützt.

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 nicht gewünschtem 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 persönlichen 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. In der Regel handelt es sich bei Firewalls für PCs um preiswerte Software, die im Computerfachhandel als "Personal Firewall" erhältlich ist. Im kostenlosen Windows XP Service Pack 2 ist bereits eine Firewall enthalten. Diese wird bei der Installation auch gleich automatisch aktiviert. So sind sie von Anfang an gut geschützt.

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

Aktualisieren Sie Ihre Software – das schützt Sie und Ihren PC

Heute wird in immer kürzeren Abschnitten neue oder verbesserte Software auf den Markt gebracht. Dieses Tempo ist nicht nur wichtig, um Ihnen Innovationen zu bieten, sondern auch um bisher

Tausende Programmierer arbeiten kontinuierlich daran, Ihre Software sicherer 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 entsprechende Möglichkeiten.

„Updates“ schützen Sie!

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 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



Aktualisierte Software macht Ihren PC sicherer!

unbekannte Schwachstellen so rasch als möglich zu beseitigen. Denn wo immer es Software gibt, gibt es auch Menschen, die diese Techniken missbrauchen und zur Gefährdung anderer Nutzer einsetzen.

Ungebetene Gäste: Viren und 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. Das variiert von lästigen kleineren Fehlfunktionen bis hin zu ernsthaften Problemen wie Datenverlust oder Hardwareschäden.

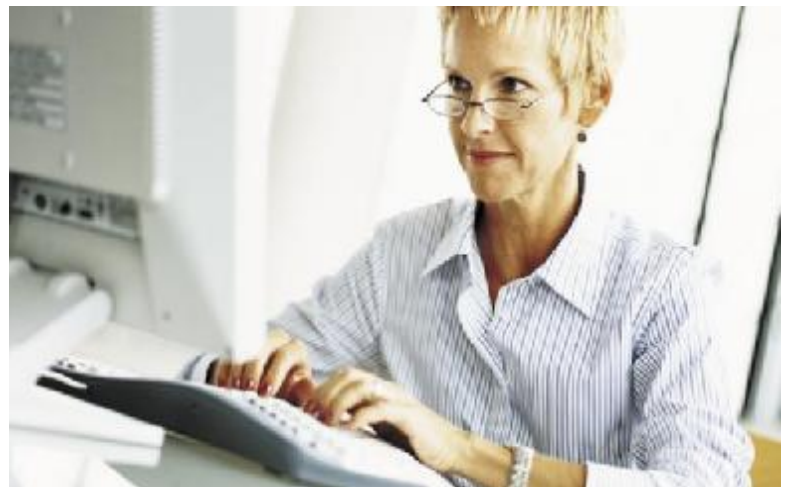
Geben Sie Viren keine Chance!

Mit speziellen Anti-Viren-Programmen können Sie die ungebetenen Gäste bekämpfen. Diese Software durchsucht Ihren PC und entfernt bekannte 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 beiliegenden Datei verleitet.

Das führt zur Infektion des PCs. Sie können durch die Aktivierung der Junk-Mail Filter in Ihrem E-Mail Programm viele dieser lästigen E-Mails beseitigen. Um nicht selbst zur Spam-Plage beizutragen, soll-



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

ten 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 unbekannten 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 unter: www.Sicher-im-Internet.AT



Ihr kostenloser eTrust™ PestScan™ jetzt online:
www.ca.com/de/products/etrust/anti-spyware.htm

Wer spioniert Sie aus?

Sie glauben, dieses Thema betrifft Sie nicht? Wir beweisen Ihnen das Gegenteil! Wenn Sie E-Mails erhalten, im Web surfen oder Dateien herunterladen, kann unbemerkt Spyware auf Ihren PC gelangen und so dessen Leistung beeinträchtigen, Ihren Internetzugang verlangsamen oder vertrauliche Informationen offen legen.

Computer Associates unterstützt Sie zuverlässig beim umfassenden Schutz Ihrer Daten. eTrust™ PestPatrol® Anti-Spyware beseitigt proaktiv Adware und Spyware sowie Trojaner, Keylogger, Hacker-Tools und andere unerwünschte Anwendungen.

Starten Sie jetzt einfach online Ihren kostenlosen eTrust™ PestScan™!

Weitere Infos über Computer Associates erhalten Sie unter www.ca.com/at



© 2005 Computer Associates International, Inc. (CA). Alle in dieser Anzeige genannten Marken, Firmennamen, Dienstleistungsmarken und Logos sind Eigentum der jeweiligen Unternehmen.

Computer Associates®

Schützen Sie sich vor „Spionen“ auf Ihrem Rechner

Spyware nennt sich jene Software, die ohne Ihr Wissen Daten auf Ihrem Rechner erhebt und an Dritte weitergibt. Hat sich solch ein Programm auf Ihrem PC eingenistet, beginnt es mit dem Sam-



Laden Sie niemals Software von einer nicht vertrauten Quelle herunter!

meln 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 oder Pop-ups erscheinen - auch, wenn Sie nicht im Internet surfen.

Schützen Sie sich vor Trojanischen Pferden

So genannte „Trojanische Pferde“ nisten sich ebenfalls auf Ihrem PC ein.

Diese Programme tarnen sich als nützliche Software, 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.

Meist gelangen Trojanische Pferde beim Herunterladen von Programmen aus scheinbar legitimen Quellen auf Ihren PC. Laden Sie daher niemals Software von einer nicht vertrauten 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 vor Trojanischen Pferden“ finden Sie unter: www.Sicher-im-Internet.AT

Passwort Fischen (Phishing) und Spam-Mails

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. Eine weitere gängige Methode ist es, bekannte Websites täuschend ähnlich nachzubauen. Mit den gestohlenen 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 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 ein 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?

Übermitteln Sie keine vertraulichen Daten, wenn Sie per E-Mail dazu aufgefordert werden. Setzen Sie sich persönlich oder telefonisch mit dem Absender-Unternehmen in Verbindung. Fragen Sie nach, ob das E-Mail tatsächlich seriös ist, bevor Sie Daten übermitteln. Auf diese Weise lassen sich Phishing-Mails rasch entlarven. Besonders wichtig: Geben Sie Ihre persönlichen Daten niemals auf Internet-seiten ein, deren Link Sie per E-Mail erhalten haben. Dasselbe gilt für Websites, die Sie nicht kennen. Besondere Vorsicht ist bei Ihnen bekannten Websites geboten, die plötzlich anders aussehen oder neue Elemente aufweisen. Diese könnten gefälscht sein.

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

Computer mit Original-Software sparen Zeit und Geld

So mancher Unternehmer meint, mit dem Kauf von PCs ohne Software könne er sparen. Doch die Hoffnung auf Kostenersparnis durch den Bezug der dazugehörigen Software über diver-

Support und Garantieleistungen - ganz zu schweigen von den drohenden rechtlichen Konsequenzen. Denn der Einsatz von illegaler Software im Unternehmen kann zu empfindlichen Strafen führen.



Bei diversen „Gelegenheitskäufen“ handelt es sich oft um Raubkopien: Probleme sind hier nahezu vorprogrammiert.

se Downloads oder im Bekanntenkreis trägt. Durch dieses meist unkoordinierte Beschaffen von Software entsteht ein wahrer „IT-Fleckerlteppich“, der zu enormen Kosten führen kann: Zum Beispiel auf Grund von Effizienzverlusten, Systemproblemen und Arbeitsausfällen.

Originale für mehr Effizienz!

Zudem handelt es sich bei diversen „Gelegenheitskäufen“ oft um Raubkopien: Probleme mit Viren, Treibern und Rechnerabstürzen sind hier geradezu vorprogrammiert. Noch dazu bieten diese Raubkopien keine Möglichkeit auf Updates,

Der Kauf von originalen und ordentlich lizenzierten Softwarepaketen, zum Beispiel als Komplettlösung vom Fachhandel, zahlt sich daher für Unternehmen sicherlich aus. Dabei können sich Unternehmen – auch Klein- und Mittelbetriebe – nicht nur Nerven, Zeit und Geld sparen, sie gewinnen auch an Effizienz im Arbeitsalltag und können ihre modernen Informationstechnologien optimal nutzen.

Mehr Informationen zum „Einsatz von Original-Software“ finden Sie im Internet unter: www.Sicher-im-Internet.AT

Einfach 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 einige Tipps für Sie zusammengestellt:

1. Sichere Verbindung: Kontrollieren Sie, noch bevor Sie Ihre Kontonummer und den Zugriffscode eingeben, ob eine sichere Verbindung hergestellt wurde. Ein kleines, abgesperktes Schloss  in der unteren Statuszeile des Internet-Browsers zeigt Ihnen, dass eine sichere Kommunikation gewährleistet ist. Falls kein Schloss erscheint, werden Ihre Daten nicht verschlüsselt übertragen.

2. Passwörter, PIN und TAN sicher verwalten: Mitarbeiter von Banken werden Sie nie nach Ihren Zugangsdaten wie Kontonummer 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 Sperre 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.



Mitarbeiter von Banken werden Sie per E-Mail nie nach Ihren Zugangsdaten fragen.

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 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.

Nur am „eigenen Computer“ sind Sie sicher!

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

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 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.



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

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** besonders wichtig: Die Mitarbeiter müssen über die Gefahren und die möglichen rechtlichen Konsequenzen, die durch das Herunterladen von Software entstehen können, informiert sein. So können zum Beispiel in Bildschirmschonern Trojanische Pferde eingearbeitet sein,



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

die das Netzwerk zerstören. Von einzelnen Mitarbeitern installierte Programme können lizenzpflichtig sein und somit unwissentlich illegal eingesetzt werden. Das kann schwerwiegende rechtliche Conse-

im Unternehmen – einige weitere Tipps

quenzen für das Unternehmen zur Folge haben.

- **Vertraulichkeit im Internet:** Online-Tagebücher, Chats und Foren erfreuen sich großer Beliebtheit. Diese Anwendungen sind allerdings keine Privatbereiche, die nur von einigen wenigen Internet-Benutzern besucht werden, 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** müssen besonders sorgsam verwaltet werden, um eine Spamflut und Überlastung der Mail-Server zu vermeiden. Mitarbeiter sollten daher ihre Unternehmens-E-Mail Adresse nur für berufliche Belange verwenden. Auch die Auflistung von E-Mail 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 Anti-Virus-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 Anti-Virus-Programm und die Firewall wichtig.

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.

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

2. Prüfen Sie alle Dateien mit einem aktuellen Anti-Virus-Programm: Lassen Sie Ihr Anti-

Virus-Programm regelmäßig nach Computerviren und Würmern suchen. Bei den



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

meisten Anti-Viren-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

Das Sicherheitskonzept von eBay



Über 1,5 Millionen Menschen aus Österreich besuchen eBay.at jeden Monat. Weltweit zählt der Online-Marktplatz bereits 147 Millionen registrierte Mitglieder, die im Jahr 2004 1,4 Milliarden Artikel mit einem Gesamthandelswert von 34,2 Milliarden Dollar kauften und verkauften.

Echte Betrugsfälle geschehen nur sehr selten. Doch auch wenn der Anteil an Problemfällen sehr gering ist, muss jeder Internet-Nutzer Maßnahmen treffen, um sich vor schwarzen Schafen zu schützen. Denn: Wo viele Menschen zusammenkommen, um Handel zu treiben, wird es immer Einzelne geben, die versuchen, Vertrauen zu missbrauchen. Der Schutz fängt zunächst bei jedem einzelnen Marktplatz-Teilnehmer selbst an. Genauso wie in der Offline-Welt muss man auch im Internet den gesunden Menschenverstand nutzen und Vorsicht walten lassen, wenn man kauft oder verkauft.

Dreistufiges Sicherheitssystem

Um den Mitgliedern maximale Sicherheit beim Handeln auf dem Online-Marktplatz zu ermöglichen, hat eBay ein dreistufiges Sicherheitssystem aufgebaut: Es beginnt mit der **Vorbeugung** durch gezielte Aufklärung der eBay-Nutzer und der Bereitstellung von Sicherheitsangeboten, durch deren conse-

quente Nutzung die Marktplatz-Teilnehmer größtmögliche Sicherheit beim Handel über eBay erreichen können.

Im Rahmen der zweiten Stufe, der **Nachverfolgung**, kümmert sich eBay um den unbürokratischen Schadensausgleich bei Problemfällen und unterstützt die Strafverfolgungsbehörden im Rahmen der gesetzlichen Möglichkeiten bestmöglich bei ihren Ermittlungen.

Auf der dritten Stufe stehen die **Früherkennung** von Problemfällen und das aktive Eingreifen durch eBay im Fokus.



Das Sicherheitsportal von eBay

- ◀ Jeder eBay-Nutzer sollte sich vor seinem ersten Handel bei eBay ausführlich auf dem Sicherheitsportal von eBay Österreich informieren. Die Erfahrung zeigt, dass sich nahezu alle Fälle von Missbrauch vermeiden ließen, hätten sich die Nutzer dort ausreichend informiert.

Information macht sicher:
www.ebay.at/sicherheitsportal



Microsoft®

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?

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.**

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

Microsoft Infoservice

E-Mail: austria@microsoft.com

☎ 08000 123-345 (gebührenfrei)