

Sie fragen – wir antworten

In dieser Rubrik finden Sie Antworten auf Ihre Fragen rund um die IT. Unsere kompetenten Partner bei dieser Serie sind die Spezialisten der Firma in4U (www.in4u.ch). Diesmal zum Thema: **Sicherheit.**

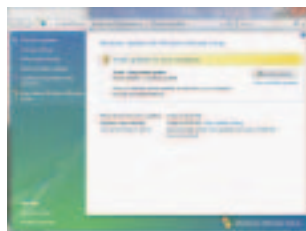
? Wie kann ich dazu beitragen, meinen Computer vor Viren zu schützen?

! Es ist nicht schwierig, den Computer vor Viren und anderen Bedrohungen zu schützen, aber Sie müssen dabei sorgfältig vorgehen.

- Installieren Sie ein Antivirenprogramm. Ein Antivirenprogramm zu installieren und immer auf dem neuesten Stand zu halten, hilft beim Schutz Ihres Computers gegen Viren. Da jeden Tag neue Viren in Umlauf gebracht werden, sollten Sie die Website des Anbieters des Antivirenprogramms regelmässig auf Aktualisierungen prüfen. Die meisten Antivirenprogramme werden im Rahmen eines Jahresabonnements verkauft, das Sie bei Bedarf verlängern können.
- Öffnen Sie keine E-Mail-Anlagen. Viele Viren sind an E-Mail-Nachrichten angehängt und verbreiten sich, sobald Sie die Anlage öffnen. Es ist ratsam, keine Anlagen zu öffnen, es sei denn, Sie erwarten eine bestimmte Anlage.
- Halten Sie Windows auf dem neuesten Stand. In regelmässigen Abständen veröffentlicht Microsoft Sicherheitsupdates, die Ihnen helfen, Ihren Computer zu schützen. Diese Updates helfen dabei, Virenattacken und



andere Computerangriffe zu verhindern, indem potenzielle Sicherheitslücken geschlossen werden. Stellen Sie sicher, dass Windows diese Updates erhält, indem Sie die automatische Aktualisierung von Windows aktivieren.



- Verwenden Sie eine Firewall. Die Windows-Firewall oder eine andere Firewall macht Sie auf verdächtige Aktivitäten aufmerksam, wenn ein Virus oder Wurm versucht, eine Verbindung mit Ihrem Computer herzustellen. Sie kann auch Viren, Würmer und Hacker davon abhalten, gefährliche Programme auf Ihren Computer herunterzuladen.



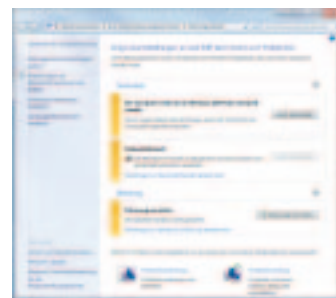
? Wie halte ich meine Antivirensoftware auf dem neuesten Stand?

! Mit veralteter Antivirensoftware ist Ihr Computer nur unzureichend geschützt. Effektiver Schutz vor aktuellen Sicherheitsrisiken ist nur durch das regelmässige Aktualisieren der Antivirensoftware möglich. Wenn Sie kein Abonnement für diese Updates besitzen, ist Ihr Computer unter Umständen anfällig für Malware-Angriffe. Im Folgenden finden Sie einige Tipps, Ihre Antivirensoftware immer auf dem neuesten Stand zu halten:

- Erwerben Sie beim Hersteller der jeweiligen Antivirensoftware ein Jahresabonnement, um die Software stets aktuell und einsatz-

bereit zu halten. Nach Erwerb eines Abonnements aktualisieren sich die meisten Antivirenprogramme selbst, sobald Sie eine Verbindung mit dem Internet herstellen.

- Um sicherzustellen, dass Ihre Software aktuell ist, öffnen Sie das entsprechende Antivirenprogramm über das Menü Start oder den Infobereich der Taskleiste, und prüfen Sie den Aktualisierungsstatus. Wenn Sie noch immer nicht sicher sind, ob Ihre Antivirensoftware auf dem neuesten Stand ist, wenden Sie sich an den Anbieter des jeweiligen Antivirenprogramms.



? Was ist Spyware?

! Spyware ist Software, die sich selbstständig auf Ihrem Computer installiert oder dort ausgeführt wird, ohne dass Sie darüber benachrichtigt oder um Zustimmung gebeten werden oder den Vorgang steuern können. Nach einer Infektion mit Spyware muss Ihr Computer nicht unbedingt Symptome zeigen, aber viele Arten von schädlicher Software oder unerwünschten Programmen können die Art und Weise beeinflussen, wie Ihr Computer arbeitet. Spyware kann z.B.

Ihr Onlineverhalten und Informationen über Sie sammeln (einschliesslich persönlicher Angaben und anderer sensibler Daten), Einstellungen auf Ihrem Computer ändern oder dazu führen, dass der Computer langsamer arbeitet.

Ein PC könnte infiziert sein, wenn eines oder mehrere der folgenden Symptome auftreten:

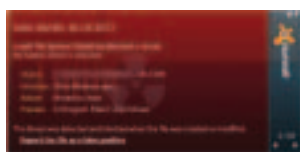
- Der PC funktioniert aussergewöhnlich langsam, besonders beim Surfen im Internet.
- Der Internet-Explorer öffnet Werbefenster, die in keinem erkennbaren Zusammenhang zu den besuchten Websites stehen.
- Die Browser-Startseite wurde geändert.
- Im Favoritenordner stehen Links, die nicht vom Benutzer gespeichert wurden.
- Der PC verbindet sich selbständig mit dem Internet.
- Die Firewall meldet laufend Versuche von Programmen, die eine Verbindung zum Internet herstellen wollen.
- Selbständiges Löschen
- Es befindet sich eine Spyware-Warnung am Desktop als Hintergrund, die zum Beispiel den Erwerb eines angeblichen Anti-Spyware-Programms bewirbt.

Software zum Erkennen und Entfernen von Spyware:



Wie funktioniert ein Virens Scanner?

Der Hersteller der Antiviren-Software liefert regelmässig Informationen über neue Viren und Schädlingsprogramme. Dies findet mindestens einmal pro Tag statt und geschieht, vom Benutzer unbemerkt im Hintergrund.



Virusmeldung bei Avast Internet Security

Ein signaturbasierter Virens Scanner, der im Hintergrund scannt prüft neu heruntergeladene Dateien oder eingelegte Datenträger

schon beim ersten Einsatz. Man kann daher eine Infektion mit bekannten Computer-Viren grundsätzlich vermeiden. Die bekannten Viren sind durch Spezialisten analysiert und als schädlich eingestuft. Der Hersteller von Anti-Viren-Software muss daher nicht nur in der Lage sein, viele Viren zu finden, sondern sie auch möglichst exakt und schnell identifizieren, von Schädlingen verursachte Aktionen rückgängig machen können und sollte möglichst keine Fehlerkennung liefern, denn das kann ebenfalls schlimme Folgen haben.



Wenn ein schädliches Programm noch nicht dem Antiviren-Programm bekannt ist, kann es vor diesem unbekanntem Schädling nicht schützen. Erst wenn der Hersteller per Update der Software diesen neuen Schädling bekannt macht, bietet die Software Schutz vor diesem Schädling – leider oft zu spät. Denn wenn ein Schädling erst einmal aktiv ist, ist er nicht einfach zu entfernen, häufig kommt man dann um eine Neuinstallation von Betriebssystem und Programmen nicht herum.

Kann ich mich von Spammails austragen?

Oft enthalten Spammails kleine Links wie «no more», «unsubscribe» usw., die zum Austragen auffordern. Klicken Sie nie auf diese Links! Sobald Sie versuchen, sich von einer Spammail abzumelden, geben Sie den Spammern zur Kenntnis, dass Ihre E-Mail-Adresse nicht nur existiert, sondern dass Sie deren Werbemails auch lesen. Das Ergebnis ist, dass Ihre E-Mail-Adresse zu einem höheren Kurs gehandelt werden kann und sie bald darauf noch weit mehr Spam erhalten.

Eine einfache Regel lautet: haben Sie sich nicht selber eingetragen, sollten Sie sich auch nicht selber austragen (und umgekehrt – haben Sie einen Newsletter oder eine Mailingliste einst bestellt, sollten Sie sich auch selber austragen, wenn Sie keine weiteren E-Mails davon erhalten möchten).

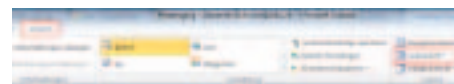
Wichtiger Hinweis, wenn Sie nicht noch mehr Spam erhalten wollen:



Öffnen Sie keine Spammails und deaktivieren Sie die Vorschau in Ihrem E-Mail-Programm, so dass nur erwünschte E-Mails angezeigt werden. In Spammails enthaltene Bilder sind typischerweise so konstruiert, dass die Spammer ihren Abruf registrieren und so die Gültigkeit der empfangenden E-Mail-Adresse verifizieren können. Dadurch erhalten Sie in Zukunft noch weit mehr Spammails.

Um die Vorschau in Outlook zu deaktivieren gehen sie wie folgt vor:

1. Klicken Sie auf die Registerkarte «Ansicht» weiter klicken Sie auf «Lesebereich»



2. Wählen Sie hier «Aus»



Was versteht man unter Phishing?

Phishing ist eine spezielle Form der Internetkriminalität und bezeichnet eine Methode des Diebstahls vertraulicher Daten von Internet-Nutzern. Diese werden durch Phishing-eMails überlistet, vertrauliche Daten, z.B. ihre Zugangsdaten zu Online-Diensten oder Kontonummer, PIN und TAN für ihren Onlinebanking-Zugang, preiszugeben. Ist der Betrüger im Besitz dieser Daten, kann er im Namen seines Opfers Aktionen ausführen und so z.B. von dessen Bankkonto Überweisungen tätigen.