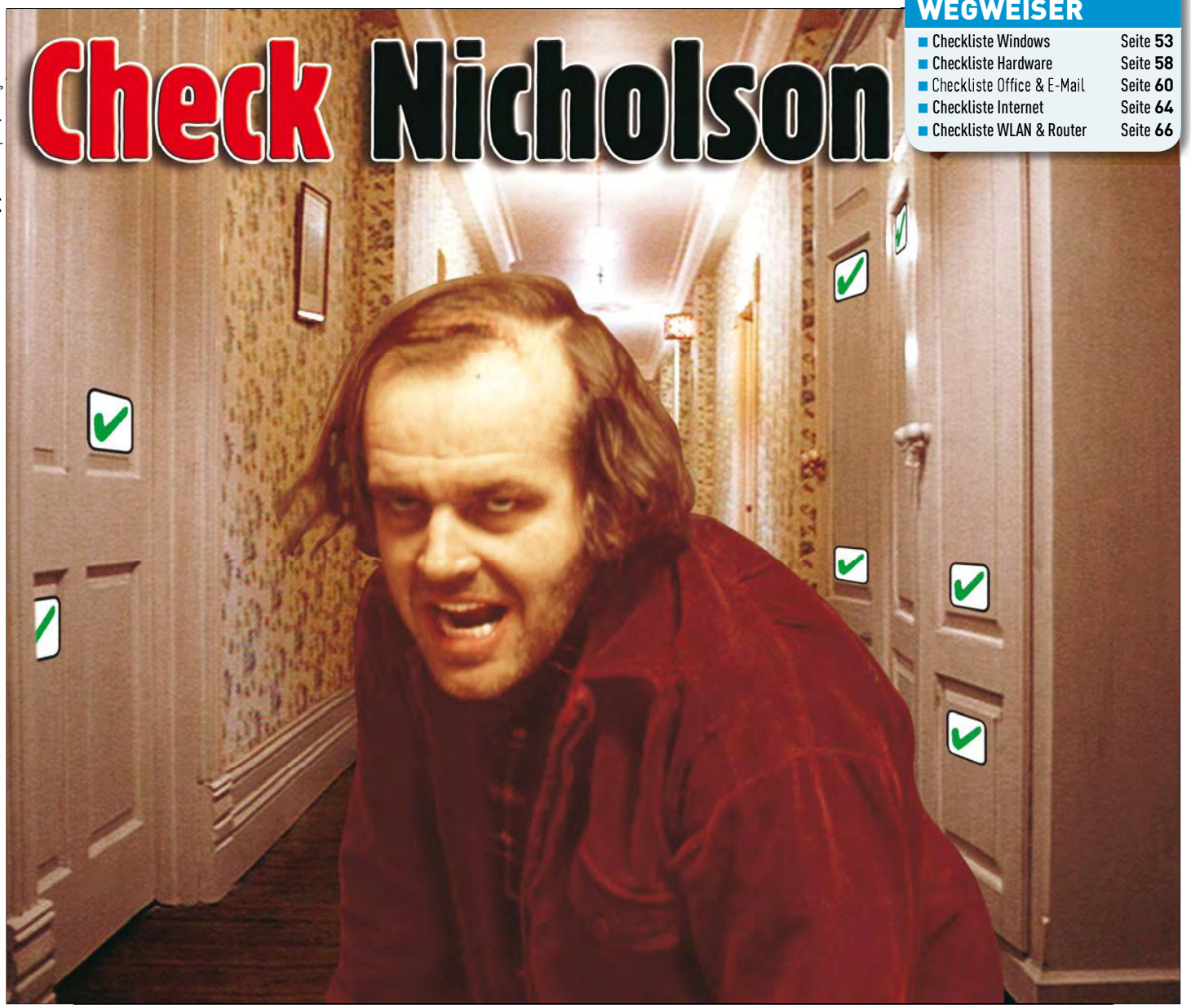
[M] Foto: Actionpress, Montage: COMPUTERBILD

Check Nicholson



ARTIKEL-WEGWEISER

Überall Viren, Datendiebe, Hacker – kommt Ihnen Ihr Computer-Alltag manchmal wie ein Horrorfilm vor? Dann müssen Sie nicht durchdrehen, sondern nur der COMPUTERBILD-Checkliste folgen. Und alles wird gut.

Sie nutzen ein Internetschutzpaket? Prima: Damit ist Ihr PC ziemlich gut geschützt. Aber vollständige Sicherheit für Ihren Computer und alle Programme kann kein Sicherheitspaket der Welt bieten. Einen kompletten Rundumschutz für Hard- und Software vor Internet-Gaunern, Spionage, Programmfehlern und Datenverlust geben Ihnen die Sicherheitstipps auf den nächsten Seiten. Folgen Sie einfach der Checkliste auf dem Umschlag dieser COMPUTERBILD-Ausgabe – und alles wird gut.

Welche Gefahren drohen?

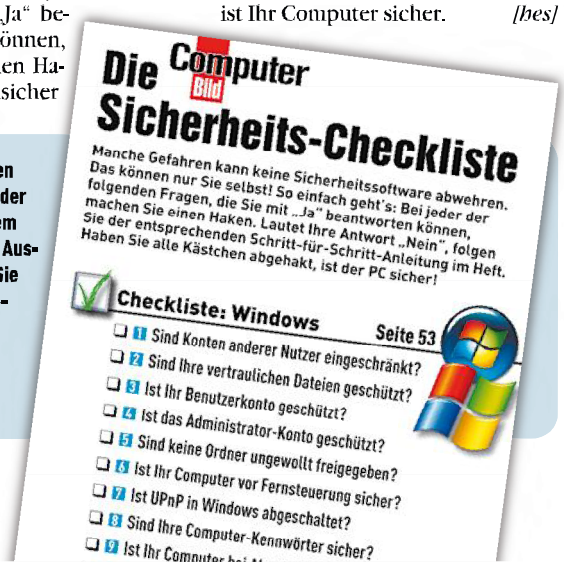
Die bekanntesten sind Computerviren und Hacker. Doch viele Risiken lauern dort, wo man Sie gar nicht vermutet. Einige Beispiele:

- **Ihr Windows**: Haben andere Personen Zugang zu Ihrem PC, können sie leicht auf Ihre Daten zugreifen. Davor schützt nicht mal Ihr Windows-Kennwort.
- **Hardware:** Selbst wenn Sie Ihr Windows per Kennwort geschützt haben, können Unbefugte mit einer Notfall-CD Ihren Computer starten und so an Ihre Daten gelangen.
- **Internet:** Der Internet Explorer speichert Ihre Kennwörter für eine schnelle Anmeldung auf Internetseiten. Fremde können das auch nutzen – und zwar in Ihrem Namen!
- **Microsoft Office:** In dem Programmpaket klaffen ständig neue Sicherheitslöcher, die Windows XP aber nicht automatisch stopft.
- **Ihr Router*:** Viele WLAN*-Router für den drahtlosen Internetzugang sind unzureichend oder gar nicht geschützt. Da kann der Nachbar gratis mitsurfen und obendrein Ihre E-Mails lesen.

Was muss ich tun?

Trennen Sie die Sicherheits-Checkliste von der Außenseite des Hefts ab, und legen Sie sie auf den Schreibtisch. Lesen Sie die Liste aufmerksam durch. Bei jeder Frage, die Sie sofort mit „Ja“ beantworten können, machen Sie einen Haken. Sind Sie unsicher oder müssen Sie mit „Nein“ antworten, folgen Sie einfach der entsprechenden Schritt-für-Schritt-Anleitung. Anschließend machen Sie wieder einen Haken in der Liste. Haben Sie alle Kästchen abgehakt, ist Ihr Computer sicher. *[hes]*

Diese Liste können Sie abhaken: Mit der Checkliste auf dem Umschlag dieser Ausgabe beseitigen Sie die 31 größten Gefahren für Ihren Computer, Ihre Daten und Ihren Geldbeutel.



*Die Erklärung dieses Fachbegriffs finden Sie auf Seite 174/175.

Checkliste: Windows

Manche Sicherheitstipps für den Computer klingen banal: Etwa der Hinweis auf ein Virenschutz-Programm oder einen Kennwortschutz für Windows. Aber hätten Sie gewusst, dass sich Ihr Computer in der Standardeinstellung von gewieften Bösewichten fernsteuern lässt? Oder dass Virenschutz-Programme oft auf eine regelmäßige Prüfung der Festplatte verzichten? Oder dass jeder Fremde mit vollen Systemrechten auf Ihre persönlichen Ordner* zugreifen kann? Die folgenden Tricks verraten Ihnen, wie sicher Ihre Daten sind.

Habe ich geprüft

1 Sind Konten anderer Nutzer eingeschränkt?

Normalerweise ist Ihr Windows-**Benutzerkonto** (S.62) 01 ein **Administrator** (S.62) 02-Konto. Nutzen auch Ihre Kinder oder Gäste den Computer, sollten Sie für diese Nutzer ein eingeschränktes Konto mit weniger Rechten erstellen. Auf diese Weise verhindern Sie, dass andere unerwünschte Änderungen an Windows vornehmen oder Ihre persönlichen Daten einsehen. Außerdem können Sie selbst ein beschränktes Konto verwenden, um sicherer im Internet zu stöbern, denn mögliche Schädlinge haben es so schwerer, sich auf Ihrem Computer einzunisten.

1 Klicken Sie auf Start, Systemsteuerung, auf Benutzerkonten und gegebenenfalls noch einmal auf den Eintrag Benutzerkonten.

2 Klicken Sie dann auf Neues Konto erstellen. Geben Sie einen Namen für das neue Konto ein, etwa Gäste, und klicken Sie auf Weiter >. Setzen Sie im nächsten Fenster per Klick einen Punkt in ● Eingeschränkt. Klicken Sie abschließend auf Konto erstellen.

3 Wenn Sie das nächste Mal Windows starten, erscheint eine Konto-Auswahl, etwa

Klicken Sie auf das neue Benutzerkonto, im Beispiel ● Gäste, um sich darauf anzumelden. *[hp]*

Habe ich geprüft

2 Sind Ihre vertraulichen Dateien geschützt?

Auf Heft-CD/DVD

Sind Ihre privaten Briefe oder wichtige Bankunterlagen vor fremden Augen sicher? Mit dem Programm TrueCrypt klappt das bestimmt: Es **verschlüsselt** (S.62) 03 Ihre Daten. Ohne die Eingabe des richtigen Kennworts ist kein Zugriff darauf möglich. So geht's:

1 Installieren Sie das Programm von der Heft-CD/-DVD in der Rubrik Titelthema. Starten Sie danach das Programm per Doppelklick auf ● TrueCrypt. Klicken Sie als Nächstes auf Nein, Volume erstellen und zweimal auf Weiter >.

2 TrueCrypt erstellt einen kennwortgeschützten Bereich auf der Festplatte* und weist ihm einen eigenen Laufwerksbuchstaben zu. Später können Sie dann Ihre sensiblen Daten auf diesem „Laufwerk" speichern. Wählen Sie einen Speicherort für die Datei aus. Klicken Sie dazu auf Datei... und etwa auf ● Eigene Dateien. Tippen Sie einen Namen für die Datei ein, hier Verschlüsselt, und klicken Sie auf Speichern und anschließend zweimal auf Weiter >.

3 Legen Sie dann fest, wie viele Megabyte* die Datei haben soll. Beispielsweise tippen Sie für 5 Gigabyte* 5000 ein. Beachten Sie dabei den freien Speicherplatz, der unter dem Eingabefeld angezeigt wird, in diesem Beispiel **Auf Laufwerk C:\ sind noch 49074.88 MB frei.** Das entspricht rund 48 Gigabyte freiem Speicherplatz. Klicken Sie anschließend einmal auf Weiter >.

4 Tippen Sie im nächsten Fenster zweimal ein Kennwort ein, klicken Sie auf Weiter > und gegebenenfalls auf Ja. Es folgen Klicks auf Weiter >, auf FAT, NTFS und Formatieren. Ist der Vorgang beendet , klicken Sie auf OK und auf Beenden. Wählen Sie nun die eben erstellte verschlüsselte Datei aus. Im Beispiel klicken Sie dazu auf Datei... und jeweils doppelt auf Eigene Dateien und Verschlüsselt.

5 Wählen Sie per Klick einen Laufwerksbuchstaben in der Liste aus, etwa ● V:, und klicken Sie auf Einbinden. Geben Sie im nächsten Fenster das Kennwort aus Schritt 4 ein, und klicken Sie auf OK. Das Laufwerk* wird jetzt nach Mausklicks auf Start und auf Arbeitsplatz angezeigt, in diesem Beispiel Lokaler Datenträger (V:). Sichern Sie von nun an dort Ihre vertraulichen Daten.

6 Damit das Laufwerk nach einem PC-Neustart verfügbar ist, klicken Sie auf Volumes, Momentan eingebundene Volumes als Favoriten, Ja, OK, Settings und Voreinstellungen. Setzen Sie mit Mausklicks in die Kästchen ● TrueCrypt starten und ● Alle Datenträger-Volumes einbinden Häkchen, und klicken Sie auf OK und Beenden.

Künftig erscheint beim Windows-Start das Fenster Kennwort. Geben Sie darin Ihr in Schritt 4 gewähltes Kennwort ein, und klicken Sie auf OK. Oder drücken Sie Esc, um das Einschalten des Laufwerks abzubrechen.

Achtung: Merken Sie sich das Kennwort gut. Ohne Kennwort kommen Sie nicht mehr an Ihre Daten! *[hp]*

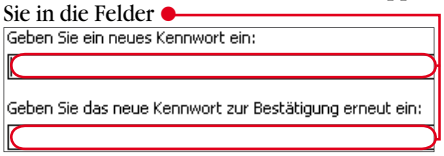
Habe ich geprüft

3 Ist Ihr Benutzerkonto geschützt?

Haben Sie Ihr Windows-Benutzerkonto mit einem Passwort geschützt? Falls nicht, kann jeder während Ihrer Abwesenheit an Ihre Daten kommen. Lesen Sie hier, wie Sie den Kennwortschutz überprüfen und gegebenenfalls einschalten.

Führen Sie den ersten Schritt von Tipp 1 aus. Wählen Sie dann per Klick Ihr Benutzerkonto aus, im Beispiel

Klicken Sie auf Kennwort erstellen, und tippen Sie in die Felder ●



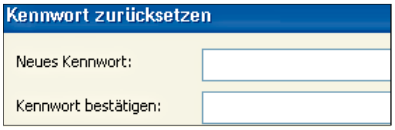
das gewünschte Passwort ein. Es folgt ein Klick auf Kennwort erstellen. Fertig! Schließen Sie das Fenster per Mausklick auf ✕. *[hp]*

Habe ich geprüft

4 Ist das Administrator-Konto geschützt?

Neben Ihrem eigenen **Administrator** (S.62) 02-Konto gibt es noch ein weiteres, verstecktes bei Windows. Es ist durch Drücken der Taste F8 während des Startvorgangs zugänglich („abgesicherter Modus"). Da das Konto über uneingeschränkte Rechte verfügt, könnten sich Fremde ohne Kennwort bei Windows anmelden, wichtige Einstellungen ändern, auf alle gespeicherten Daten zugreifen oder sogar Schadprogramme installieren. Riegeln Sie deshalb auch diesen Zugang mit einem Kennwort folgendermaßen ab:

Starten Sie Windows im normalen Modus, und melden Sie sich auf einem Administratorkonto an. In diesem Beispiel klicken Sie dazu auf ● Hubsi Computeradministrator und geben Ihr Kennwort ein. Tippen Sie dann bei gedrückter ⊞-Taste auf R. Geben Sie anschließend control userpasswords2 ein, und drücken Sie auf ↵. Klicken Sie im neuen Fenster auf den Eintrag Administrator und auf Kennwort zurücksetzen. Geben Sie im Fenster



zweimal ein Kennwort für das Konto ein, und klicken Sie anschließend auf OK. *[hp]*

Habe ich geprüft

5 Sind keine Ordner ungewollt freigegeben?

Haben Sie Ordner* auf der Festplatte* freigegeben? Dann hat jeder PC innerhalb des Netzwerks* Zugriff darauf, und bei Sicherheitslücken könnte ein Datendieb darin stöbern. So überprüfen Sie, ob Ordner offen sind:

1 Tippen Sie bei gedrückter ⊞-Taste auf R. Geben Sie dann cmd ein, und klicken Sie auf OK. Im nächsten Fenster tippen Sie `net share` ein und drücken auf ↵. Windows listet daraufhin die freigegebenen Ordner auf, etwa ●.

```
C$              C:\
ADMIN$          C:\WINDOWS
Filme           D:\Filme
Urlaubsbilder
```

Links daneben sehen Sie die Freigabe-Namen.

Wichtig: Alle Freigaben mit dem Dollarzeichen $ stammen von Windows und dürfen nicht gelöscht werden.

2 So entfernen Sie zum Beispiel die Freigabe für den Ordner `Filme`: Tippen Sie im Fenster den Befehl `net share "Filme" /d` ein. Der Freigabe-Name steht dabei in Anführungszeichen. Drücken Sie auf ↵. Fertig. Wiederholen Sie das bei Bedarf für weitere Ordner, und prüfen Sie das Ergebnis (siehe Schritt 1). Schließen Sie das Fenster per Klick auf ✕. *[hp]*

Habe ich geprüft

6 Ist Ihr Computer vor Fernsteuerung sicher?

Die „Remote-Unterstützung" von Windows ist eine Funktion zur Fernwartung des Computers. Mit Ihrer Erlaubnis kann etwa ein sachkundiger Bekannter damit über das Internet Ihren Bildschirminhalt einsehen oder sogar die Steuerung des PCs übernehmen, um Probleme aus der Ferne zu lösen. Hacker könnten diese Hintertür aber nutzen, um die Kontrolle über Ihren Computer zu erlangen. Schalten Sie die Option daher lieber ab. Das geht so:

IN WINDOWS XP:

Klicken Sie auf Start und dann mit der *rechten* Maustaste auf Arbeitsplatz. Klicken Sie anschließend auf Eigenschaften und im erscheinenden Fenster auf Remote. Entfernen Sie mit Mausklicks die Häkchen ●

☑ Ermöglicht das Senden von Remoteunterstützungsangebot

und ●.

☑ Benutzern erlauben, eine Remotedesktopverbindung herzu

Klicken Sie auf OK.

IN WINDOWS VISTA:

Tippen Sie bei gedrückter ⊞-Taste auf Pause. Klicken Sie dann auf Remoteeinstellungen und Fortsetzen. Entfernen Sie anschließend per Klick das Häkchen ●,

☑ Remoteunterstützungsverbindungen mit diesem Computer

und klicken Sie auf die Schaltfläche OK. Jetzt ist der PC sicher. *[hp]*

Habe ich geprüft

7 Ist UPnP in Windows abgeschaltet?

Mit der Funktion UPnP können Programme und Geräte wie Router* oder Medienabspieler Daten über ein Netzwerk austauschen. Sie wird zum Beispiel von Plauderprogrammen (Chat) wie dem Live Messenger verwendet. Leider könnten auch Schadprogramme diese Möglichkeit ausnutzen, um Sie auf gefährliche Internetseiten umzuleiten. Schalten Sie deshalb UPnP aus, wenn Sie gerade nicht plaudern.

1 Falls Sie Windows XP verwenden, tippen Sie bei gedrückter ⊞-Taste auf R. Geben Sie dann cmd ein, und drücken Sie auf ↵. Machen Sie dann mit Schritt 2 weiter.

Bei Windows Vista klicken Sie auf ⊞ und tippen cmd ein. Klicken Sie dann mit der *rechten* Maustaste auf cmd.exe. Es folgen Mausklicks auf Als Administrator und Fortsetzen.

2 Tippen Sie den Text `sc config upnphost start= demand` ein, und drücken Sie ↵. Daraufhin erscheint `ChangeServiceConfig SUCCESS`. Tippen Sie `sc config ssdpsrv start= demand` ein, und drücken Sie ↵. UPnP startet jetzt nicht mehr mit Windows. Falls Sie die Funktion nie wieder brauchen, ist der Tipp hier zu Ende.

UPNP BEI BEDARF EINSCHALTEN

1 Für den Fall, dass Sie UPnP noch brauchen, etwa für ein Chat-Programm, legen Sie eine Start- und eine Stopp-Datei auf der Arbeitsoberfläche* ab. Damit lässt sich UPnP jederzeit per Doppelklick starten und beenden: Geben Sie dazu `notepad` ein, und drücken Sie auf ↵. Tippen Sie im aufklappenden Fenster ●

```
Datei  Bearbeiten  Format
net start upnphost
net start ssdpsrv
```

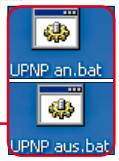
ein. Klicken Sie auf Datei und Speichern. Tippen Sie als Dateinamen upnp an.bat ein. Klicken Sie als Nächstes auf Textdateien (*.txt) und Alle Dateien. Wählen Sie per Klick als Speicherort ● Desktop aus. Falls Sie diese Schaltfläche bei Vista nicht sehen, klicken Sie zuvor auf Ordner durchsuchen. Es folgen Klicks auf Speichern und auf ✕.

Auf die gleiche Weise stellen Sie die Stopp-Datei her. Tippen Sie aber den Text ●

```
net stop upnphost
net stop ssdpsrv
```

und den Dateinamen upnp aus.bat ein.

2 Schließen Sie danach das Fenster per Klick auf ✕. Auf der Arbeitsoberfläche befinden sich jetzt die beiden neuen Dateien ●:



Mit einem Doppelklick auf UPNP an.bat schalten Sie UPnP rasch ein, mit UPNP aus.bat ebenso schnell wieder aus.

Bei Vista sehen die Schaltflächen etwas anders aus. Dort müssen Sie zum Ein- und Ausschalten von UPnP jeweils zusätzlich auf Als Administrator ausführen klicken. *[hp]*

Habe ich geprüft

8 Sind Ihre Computer-Kennwörter sicher?

Auf Heft-CD/DVD

Viele Internetaktivitäten funktionieren nur, wenn Sie ein Kennwort eingeben – zum Beispiel das Abrufen eines E-Mail-Postfachs und Bankgeschäfte. Guten Schutz bieten jedoch nur Passwörter, die Gauner nicht so schnell erraten oder mit speziellen Programme knacken können. Testen Sie einfach mal, wie gut Ihre Kennwörter sind:

1 Installieren Sie das Programm KeePass von der beiliegenden COMPUTERBILD-Heft-CD/-DVD. Starten Sie anschließend die Software mit einem Doppelklick auf ●.

Danach folgen Mausklicks auf Extras und auf den Eintrag Passwort-Generator...

2 Um ein Kennwort, beispielsweise das für Ebay, auszutesten, tippen Sie es unter Generiertes Passwort ein. Wie sicher es ist, wird dann farbig angezeigt, im Beispiel ●. Grundsätzlich gilt, je grüner, desto besser.

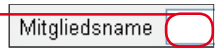
So sind etwa Passwörter, die sich aus Buchstaben, Sonderzeichen und Zahlen zusammensetzen, sehr sicher: ▮. Dagegen gelten einfache Wörter wie „Hase" oder Zahlenkombination wie „12345" als unsicher: ▮. Probieren Sie aus, ob Ihre Kennwörter durch minimale Ergänzungen sicherer werden, und passen Sie sie im Internet an. Keine Angst vor schwierigen Kombinationen: Im nächsten Schritt lesen Sie, wie Sie auch komplizierte Kennwörter niemals vergessen.

3 KeePass ist ein Passwort-Tresor. Das bedeutet, Sie können dort mehrere Kennwörter speichern und durch ein sogenanntes Master-Passwort schützen. So geht's: Falls das Fenster Passwort-Generator noch geöffnet ist, schließen Sie es per Klick auf Abbrechen. Klicken Sie dann auf Datei und Neu... Tippen Sie unter Master-Passwort: Ihr Hauptkennwort ein, und wiederholen Sie die Eingabe nach einem Klick auf OK. Danach klicken Sie wieder auf OK.

4 Speichern Sie das erste Kennwort, im Beispiel das für Ebay. Markieren* Sie dazu den Eintrag Internet, und klicken Sie auf ●

Tippen Sie neben Titel: den Namen ein, hier Ebay, und die dazugehörigen Zugangsdaten. Es folgt ein Klick auf OK. Speichern Sie auf die gleiche Weise die anderen Kennwörter, etwa die für Bankgeschäfte und das E-Mail-Postfach. Klicken Sie auf ▮ und Speichern.

5 Künftig tragen Sie Ihre Zugangsdaten so ein: Starten Sie KeePass mit dem Master-Kennwort, dann das Internet-Zugriffsprogramm*. Laden Sie die gewünschte Seite, hier http://www.ebay.de/, klicken Sie dann auf Einloggen und auf ●,



in der Startleiste auf Database und auf Ebay. Jetzt tippen Sie bei gedrückter Strg-Taste auf V. Die Zugangsdaten werden automatisch eingetragen. *[js]*

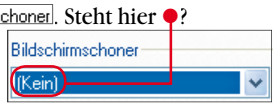
*Die Erklärung dieses Fachbegriffs finden Sie auf Seite 174/175.

Habe ich geprüft

9 Ist Ihr Computer bei Abwesenheit sicher?

Mit Virenschutz, Firewall*, **Phishing** ▸(S.62) 04 und Werbefilter ist der PC zwar prima vor Angriffen aus dem Internet geschützt – doch wie steht's um die Sicherheit auf Ihrem Schreibtisch? Ist der Computer vor unerlaubten Zugriffen sicher, während Sie in der Kantine sitzen? So finden Sie's heraus:

1 Stellen Sie zuerst sicher, dass Ihr Windows-Benutzerkonto mit einem Kennwort geschützt ist, siehe Tipp 3 auf Seite 53. Danach prüfen Sie, ob Windows automatisch per Bildschirmschoner gesperrt wird, wenn Sie längere Zeit nicht am Computer arbeiten. Auf diese Weise bleiben Fremde ausgesperrt, sollten Sie einmal die manuelle Windows-Abmeldung vergessen. Klicken Sie dazu mit der *rechten* Maustaste auf einen freien Bereich der Arbeitsoberfläche, in der nun aufklappenden Liste auf Eigenschaften und danach im neuen Fenster auf Bildschirmschoner. Steht hier ●?

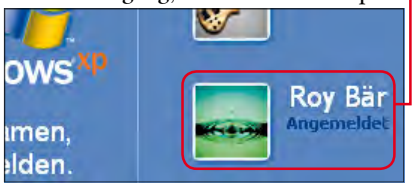


Dann wählen Sie per Klick darauf einen Bildschirmschoner in der erscheinenden Liste aus, beispielsweise Windows XP.

2 Damit Fremde den Bildschirmschoner nicht einfach per Mausbewegung beenden und danach auf Ihre Daten zugreifen können, stellen Sie sicher, dass hier ● oder vor Kennworteingabe bei Reaktivierung ein Haken zu sehen ist. Andernfalls setzen Sie ihn per Mausklick. Damit Windows bei Inaktivität nicht zu lange mit dem Starten des Bildschirmschoners wartet, tippen Sie hier ●

ein. Es folgt ein Klick auf OK.

3 Künftig wird Windows bei einer Inaktivität von fünf Minuten automatisch gesperrt. Nach dem „Aufwecken" des Computers, etwa per Mausbewegung, erscheint zum Beispiel ●.



Ohne Eingabe des richtigen Kennworts bleibt der Computer gesperrt.

Übrigens: Sie müssen nicht auf den Start des Bildschirmschoners warten oder sich mühselig abmelden, wenn Sie mal schnell weg müssen. Tippen Sie bei gedrückter ⊞-Taste auf L, um Windows manuell zu sperren. *[bes]*

Habe ich geprüft

10 Sind Ihre Programme auf dem neuesten Stand?

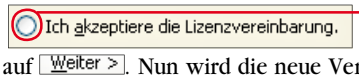
Was für Windows gilt, gilt auch für alle anderen Programme auf Ihrem Computer: Nur mit einer regelmäßigen Aktualisierung der Software stopfen Sie Sicherheitslücken und schützen Ihre Daten. Wie das übers Internet funktioniert, lesen Sie am Beispiel des Internetzugriffs-Programms* Firefox. Übrigens: Für zehn wichtige Programme finden Sie die aktuellen Versionen auf der COMPUTERBILD-Heft-CD/-DVD dieser Ausgabe. Welche das sind, erfahren Sie in der Tabelle unten.

1 Stellen Sie zuerst eine Verbindung zum Internet her, und starten Sie dann das gewünschte Programm, im Beispiel Firefox, mit Klicks auf Start und

Klicken Sie auf Hilfe und in der aufklappenden Liste auf Firefox aktualisieren... Bei vielen anderen Programmen müssen Sie statt auf Hilfe auf ? klicken und dann in der Liste zum Beispiel Nach neuer Version suchen.., Nach Updates suchen... oder Auf Online-Updates prüfen auswählen.

2 Warten Sie die Suche ab. Bei Firefox sehen Sie **Überprüfe auf verfügbare Updates**. Falls danach **Keine Updates verfügbar** erscheint, ist das Programm bereits auf dem neuesten Stand. Andernfalls haben Sie zwei Möglichkeiten:

- Installieren Sie die neue Version von der Heft-CD/-DVD von der Rubrik Titelthema.
- Aktualisieren Sie das Programm per Internet, hier mit Klicks auf **Neue Version installieren**, ●



und auf Weiter >. Nun wird die neue Version aus dem Internet überspielt und installiert. Ist der Vorgang beendet, klicken Sie im Beispiel auf **Firefox jetzt neu starten**. Nach dem Neustart ist die Software aktualisiert. *[js]*

Diese aktuellen Versionen finden Sie auf der Heft-CD/-DVD

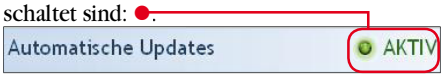
Name	Programmart	Name	Programmart
Firefox	Internet-Zugriffsprogramm	Kaspersky Security Suite CBE	Internetschutzpaket
TrueCrypt	Verschlüsselungsprogramm	Real Player	Musik-/Video-Abspielprogramm
Thunderbird	E-Mail-Programm	KeePass	Kennwort-Verwaltungsprogramm
Adobe Reader	PDF-Anzeigeprogramm	Ccleaner	Datei-Entrümpelungsprogramm
Winamp	Musik-/Video-Abspielprogramm	Flash Player	Musik-/Video-Abspielprogramm

Habe ich geprüft

11 Wird Windows automatisch aktualisiert?

Experten decken immer wieder neue Sicherheitslücken in Windows auf. Microsoft bemüht sich dann, möglichst schnell Aktualisierungen zu veröffentlichen, um diese Löcher zu stopfen. Sobald die Nachbesserungen erschienen sind, wissen aber auch Internet-Ganoven um das Sicherheitsleck und stürzen sich auf alle Computer, auf denen die Nachbesserungen noch fehlen. Um sich wirksam zu schützen, bleibt Ihnen nichts anderes übrig, als immer die neuesten Sicherheits-Updates zu installieren. So stellen Sie fest, ob das automatisch geschieht:

Tippen Sie bei gedrückter ⊞-Taste auf R, und geben Sie wscui.cpl ein. Drücken Sie dann auf ↵. Im neuen Fenster sehen Sie, ob die sogenannten „Automatischen Updates" eingeschaltet sind: ●



Sind sie jedoch INAKTIV, schalten Sie sie jetzt ein. Klicken Sie dazu bei Windows XP auf Automatische Updates aktivieren, bei Windows Vista auf Einstellungen ändern...,

und auf Fortsetzen. Schließen Sie das Fenster per Klick auf ✕. *[hp]*

Computer Bild TIPP

Auf Heft-CD/DVD

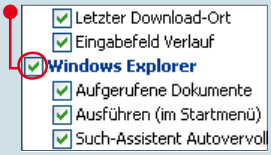
DATEIPROTOKOLLE LÖSCHEN

Windows merkt sich alle Dateien, die Sie zuletzt geöffnet haben, und zeigt sie in der Liste

an – leider auch jedem Fremden. Ihre Computernutzung geht niemanden etwas an. Um sich vor neugierigen Blicken zu schützen, entfernen Sie regelmäßig die Listeneinträge. Das erledigt das Programm Ccleaner automatisch für Sie beim Windows-Start. Sie finden die Software auf der Heft-CD/-DVD dieser Ausgabe in der Rubrik Titelthema. Der Clou: Ccleaner beseitigt auch die Protokolle anderer Programme, etwa des Internet Explorers. So geht's:

Starten Sie Ccleaner nach der Installation per Doppelklick auf ●.

Die zu löschenden Protokolle kennzeichnet Ccleaner mit Häkchen. Stellen Sie sicher, dass der Haken ●



zu sehen ist. Denn er sorgt dafür, dass der Dateiverlauf im Startmenü beseitigt wird.

Passen Sie die Voreinstellungen des Programms Ihrem Bedarf an: Entfernen Sie etwa den Haken Papierkorb leeren, wenn Ccleaner den Papierkorb nicht automatisch leeren soll. Beachten Sie auch die Protokolle weiterer Programme, die nach einem Klick auf Anwendungen zu sehen sind.

Im Anschluss klicken Sie auf Einstellungen, auf Einstellungen und setzen mit einem Mausklick in das Kästchen ● Automatisches Reinigen einen Haken. Schließen Sie das Programm dann mit einem Klick auf ✕. Künftig werden Ihre gewählten Nutzungsprotokolle bei jedem Windows-Start automatisch geleert. *[bes]*

Habe ich geprüft

12 Ist ein Virenschutz eingerichtet?

Erscheint unten rechts am Bildschirm das Symbol ? Dann kann der Virenschutz veraltet sein oder sogar fehlen. Zur Prüfung klicken Sie doppelt darauf. Erscheint neben Virenschutz der Hinweis NICHT AKTUELL, aktualisieren Sie die Software. Geht das nicht, oder steht dort NICHT GEFUNDEN, installieren Sie ein neues Schutzprogramm, etwa die Kaspersky Security Suite CBE, zu finden auf der Heft-CD/-DVD unter Sicherheits-Center. *[bes]*

Habe ich geprüft

13 Ist der Computer vor Hackern geschützt?

Gute Schutzpakete wie die Kaspersky Security Suite CBE beinhalten eine Firewall*. Haben Sie nur ein Virenschutz-Programm, etwa Avira Antivir, muss zumindest die eingebaute Firewall von Windows aktiviert sein. Überprüfen Sie das: Tippen Sie bei gedrückter ⊞-Taste auf R, und geben Sie wscui.cpl ein. Drücken Sie dann auf ↵. Im neuen Fenster sehen Sie den Status der Firewall. Im Beispiel ist sie aktiv: ●.

Ist sie dagegen 

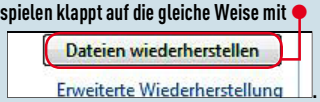
, schalten Sie sie jetzt ein. Klicken Sie dazu bei Windows XP auf

und Jetzt aktivieren. Bei Windows Vista klicken Sie auf Jetzt einschalten und Fortsetzen. *[hp]*

Computer TIPP

REGELMÄSSIGE DATENSICHERUNG

Hundertprozentige Sicherheit am PC? Die gibt's leider nicht. Beugen Sie für den Ernstfall – zum Beispiel einen Virenbefall – vor, und sichern Sie regelmäßig Ihre wichtigen Dateien. Die nötige Software ist in Windows bereits eingebaut: Unter Vista drücken Sie die Taste ⊞, tippen Sichern ein und klicken dann in der Liste auf Sichern und Wiederherstellen. Per Klick auf Dateien sichern starten Sie dann die Software. Das Zurückspielen klappt auf die gleiche Weise mit ●



Falls Sie Windows XP Professional oder die Media Center Edition verwenden, finden Sie das Sicherungsprogramm nach Mausklicks auf Start, Alle Programme, Zubehör, auf Systemprogramme und dann auf Sicherung. Folgen Sie dann einfach den Anweisungen auf dem Bildschirm. In XP Home müssen Sie die Software erst nachinstallieren. Und das geht so:

1 Legen Sie Ihre Windows-CD ins Laufwerk, und warten Sie einen Moment, bis das Fenster

auf dem Bildschirm zu sehen ist. Klicken Sie dann auf

und auf

2 Klicken Sie nun jeweils doppelt auf die Einträge VALUEADD, MSFT, NTBACKUP und NTBACKUP. Sobald Fertig stellen erscheint, klicken Sie darauf und schließen die beiden Fenster mit Klicks auf ✕. Jetzt können Sie das Programm wie oben beschrieben starten und Ihre wichtigen Dateien sichern. *[js]*

Habe ich geprüft

14 Ist Ihr Computer frei von Rootkits?

Immer häufiger bedrohen Rootkits (Tarnviren) Ihren PC (siehe „Sicherheitscenter" auf Seite 20). Rootkits sind Schadprogramme, die sich selbst und meist noch weitere eingeschleuste Viren* auf der Festplatte* verstecken. Das gelingt Ihnen oft so gut, dass selbst Virenschutz-Programme die Infektion im Nachhinein nicht erkennen. Rootkits könnten nämlich unbemerkt auf Ihren PC gelangt sein, etwa wenn der Schutz einmal veraltet war. Um sicherzugehen, dass Ihr PC nicht verseucht ist, müssen Sie eine spezielle Rootkit-Suche durchführen. Das kann jedes bessere Virenschutz-Programm. So geht's zum Beispiel mit der Kaspersky Security Suite CBE (auf Heft-CD/-DVD):

1 Bringen Sie Kaspersky bei bestehender Internetverbindung auf den neuesten Stand: Klicken Sie dazu mit der *rechten* Maustaste auf das Symbol ●,

und dann auf Update. Warten Sie, bis im nächsten Fenster **erfolgreich abgeschlossen** zu sehen ist. Dann klicken Sie auf Schließen.

2 Klicken Sie jetzt doppelt auf ✕, im nächsten Fenster auf Virensuche und danach auf Rootkit-Suche. Das Programm sollte, wie in diesem Beispiel Kaspersky, den gesamten Computer mit allen Laufwerken* („Arbeitsplatz") nach Tarnviren durchsuchen: ●. Wählen Sie diese Option andernfalls aus.

3 Nach einem Klick auf Untersuchung starten wird der Computer überprüft. Es gibt nun folgende Möglichkeiten:

- Das Programm findet keine Tarnviren und meldet im Beispiel abgeschlossen: Beenden Sie die Software dann per Klick auf ✕. Wiederholen Sie die Prüfung, falls der Computer einmal längere Zeit ohne ausreichenden Schutz ist.
- Das Programm meldet einen Fund. In diesem Fall folgen Sie den Anweisungen der Software, um den Schädling zu entfernen. Da nach dem Löschen eines Rootkits häufig weitere Viren auf der Festplatte enttarnt werden, sollten Sie den Computer anschließend einer Komplettprüfung unterziehen (siehe Tipp 15).

Übrigens: Falls Ihr Schutzprogramm keine Rootkit-Suche bietet und Sie Kaspersky nutzen möchten, entfernen Sie Ihr bisheriges Programm vor der Kaspersky-Installation. *[bes]*

Habe ich geprüft

15 Wird der PC regelmäßig auf Viren geprüft?

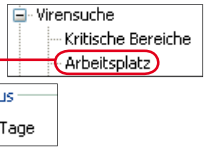
Gute Virenschutz-Programme bieten einen sogenannten Hintergrunddienst, auch Wächter genannt, der automatisch neue und stichprobenartig bereits vorhandene Dateien auf der Festplatte kontrolliert. Dabei untersucht der Dienst aber in der Regel nicht alle Dateien, sondern nur Programmdateien. Aus diesem Grund sollten Sie den Computer zwar nicht täglich, aber doch regelmäßig einer Komplettprüfung unterziehen. Lesen Sie hier am Beispiel der Kaspersky Security Suite CBE (auf der Heft-CD/-DVD dieser Ausgabe), wie Sie sicherstellen, dass Ihr Virenschutz-Programm diesen Job automatisch erledigt.

1 Aktualisieren Sie Kaspersky wie im Tipp 12 beschrieben. Danach starten Sie die Komplettprüfung von Hand. Klicken Sie dazu mit der *rechten* Maustaste auf ●

und dann in der aufklappenden Liste auf Arbeitsplatz untersuchen. Ihr Computer wird daraufhin gründlich auf Schadsoftware überprüft, denn es werden alle Dateien berücksichtigt. Der Vorgang dauert einige Minuten, im Beispiel ist die Restzeit hier

ablesbar. Falls das Programm im Anschluss **keine gefährlichen Objekte gefunden** meldet, ist der PC sauber, und Sie können das Fenster per Klick auf Schließen schließen. Andernfalls folgen Sie den Anweisungen der Schutzsoftware, um gefundene Viren unschädlich zu machen.

2 Da sich die Hersteller der Virenschutz-Programme gern auf die Wirkung des Hintergrund-Wächters verlassen, ist die automatische Komplettprüfung des Computers häufig nicht im Programm voreingestellt. Schauen Sie deshalb nach: Klicken Sie dazu bei Kaspersky mit der *rechten* Maustaste auf das Symbol ✕ und in der aufklappenden Liste auf Einstellungen... Im nächsten Fenster folgen Klicks auf ● und auf ●,



damit dort ein Haken erscheint.

3 Eine tägliche Komplettprüfung ist übertrieben, es reicht auch eine wöchentliche, bei seltener PC-Nutzung eine monatliche. Um das einzustellen, klicken Sie auf Ändern..., dann im nächsten Fenster auf ● und in der Liste auf Wochen oder Monate. Setzen Sie per Mausklick hier ● Übersprungene Aufgabe starten einen Haken, und klicken Sie danach zweimal auf OK sowie auf ✕, um alle noch geöffneten Fenster zu schließen. Künftig wird der Computer an jedem Monatsersten untersucht. Wird er an diesem Tag nicht eingeschaltet, holt das Programm die Aufgabe beim nächsten Windows-Start selbstständig nach. *[bes]*

*Die Erklärung dieses Fachbegriffs finden Sie auf Seite 174/175.

Checkliste: Hardware

Mit der Checkliste auf den Seiten 53 bis 56 haben Sie Windows und installierte Programme vor Hackern, Viren* und vielen anderen Risiken sicher gemacht. Doch manche Gefahren lauern schon vor dem Start von Windows. Wenn etwa Fremde mit einfachen Rettungs-CDs das installierte Betriebssystem* aushebeln, bietet auch das beste Windows-Kennwort keinen Schutz vor unberechtigten Zugriffen. Lesen Sie hier die wichtigsten Hardware-Tricks, wie Sie Ihren PC vor Datenklau bewahren.

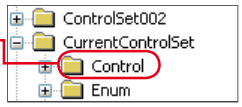
Habe ich geprüft

16 Ist Ihr Computer vor Datendiebstahl per USB-Stift geschützt?

Die beste Sicherung gegen Hacker-Angriffe und Spähprogramme hilft nichts, wenn ein Datendieb private Dateien oder Zugangsdaten für Ihr Bankkonto und Internet-Shops einfach direkt von Ihrem Computer kopieren kann. Um Ihren PC auch gegen solche Angriffe zu schützen, führen Sie diesen Tipp durch. Damit verhindern Sie, dass andere Personen Daten auf USB*-Stifte und auf Geräte wie MP3*-Spieler oder USB-Festplatten* kopieren können.

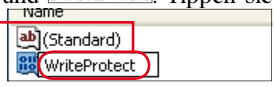
1 Klicken Sie unter Windows XP auf Start und danach auf Ausführen. Im nächsten Fenster tippen Sie regedit in das Eingabefeld ein und klicken auf OK. Unter Windows Vista klicken Sie auf , geben in das Eingabefeld regedit ein und drücken auf die ↵-Taste. Bestätigen Sie die folgende Sicherheitsabfrage mit einem Mausklick auf Fortsetzen.

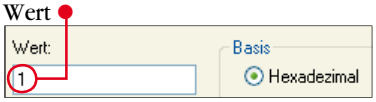
2 Klicken Sie im nächsten Fenster jeweils doppelt auf HKEY_LOCAL_MACHINE, SYSTEM und CurrentControlSet. Klicken Sie danach mit der *rechten* Maustaste auf und dann in der aufklappenden Liste auf



Neu und Schlüssel. Tippen Sie anschließend den Namen ein, und drücken Sie auf die ↵-Taste. Achten Sie dabei auf die Groß- und Kleinschreibung.

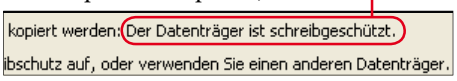
3 Klicken Sie mit der *rechten* Maustaste auf StorageDevicePolicies und in der aufklappenden Liste auf Neu und DWORD-Wert. Tippen Sie danach ein, und drücken Sie zweimal auf die ↵-Taste. Im nächsten Fenster geben Sie den Wert





ein und klicken auf OK. Schließen Sie das Fenster Registrierungs-Editor per Klick auf .

4 Starten Sie den PC neu. Wenn Sie künftig versuchen, Daten auf einen USB-Stift oder eine USB-Festplatte zu kopieren, erscheint



und der Vorgang wird abgebrochen. Schließen Sie das Fenster per Klick auf OK. Ab jetzt wird es für einen unbefugten Dritten also nicht mehr möglich sein, ohne Ihr Wissen Daten auf seinen USB-Stift zu kopieren.

USB-SCHREIBSCHUTZ ENTFERNEN

Um das Schreibverbot für angeschlossene USB-Laufwerke* wieder aufzuheben, gehen Sie folgendermaßen vor:

1 Führen Sie Schritt 1 des vorigen Abschnitts aus. Klicken Sie doppelt auf Control und einmal auf StorageDevicePolicies. Klicken Sie dann doppelt auf WriteProtect.

2 Im nächsten Fenster tippen Sie den Wert

ein und klicken auf OK. Schließen Sie das Fenster Registrierungs-Editor mit einem Klick auf . Danach können Sie wieder wie gewohnt Daten auf USB-Laufwerke kopieren. Starten Sie den PC gegebenenfalls neu, damit die Änderung wirksam wird. *[mk]*

Habe ich geprüft

17 Ist Ihr Computer kennwortgeschützt?

Mit dem Sicherheitstipp 3 auf Seite 53 haben Sie zwar Windows vor Eindringlingen geschützt, aber nicht den Computer. Denn Fremde können ihn immer noch mithilfe einer CD oder DVD starten und so an Ihre Daten gelangen. Verhindern lässt sich das nur mit einem BIOS▸[S.62] 05-Kennwort:

1 Schalten Sie den Computer ein, und drücken Sie mehrmals auf Entf. Erscheint das BIOS nicht, versuchen Sie es mit F2, F10 oder Strg und Esc. Markieren* Sie mit den Pfeiltasten den Eintrag ▸ Advanced BIOS Features. Ist diese Zeile auf Ihrem Bildschirm nicht zu sehen, wählen Sie stattdessen Boot und danach Security aus. In beiden Fällen drücken Sie anschließend auf die ↵-Taste. Steht neben Security Option oder Password Check das Wort [System], machen Sie gleich mit Schritt 2 weiter. Falls nicht, markieren Sie diese Zeile und drücken nacheinander auf ↵ und ↓, um die Einstellung System auszuwählen. Bestätigen Sie die Änderung mit einem Druck auf die ↵-Taste.

2 Markieren Sie den Eintrag Supervisor Password beziehungsweise Set Supervisor Password, und drücken Sie auf ↵. Ist die Zeile nicht zu sehen, drücken Sie vorher einmal auf Esc.

Tippen Sie danach ein beliebiges Kennwort ein. Statt der Zeichen werden Sternchen angezeigt, hier

. Achtung: Wählen Sie ein Kennwort, das Sie sich gut merken können. Sollten Sie es vergessen, kommen Sie nicht mehr an Ihre Daten! Drücken Sie auf ↵, und wiederholen Sie die Kennworteingabe im Fenster Enter Password: beziehungsweise neben Confirm Password. Drücken Sie anschließend noch einmal auf ↵.

3 Wählen Sie dann mit den Pfeiltasten den Menüpunkt Save & Exit Setup aus. Sehen Sie ihn nicht, drücken Sie einmal auf Esc. Wählen Sie Exit und Exit & Save Changes aus, und drücken Sie auf die Taste ↵. Im nächsten Fenster, etwa SAVE to CMOS and EXIT (Y/N)?, drücken Sie erneut auf ↵. Der PC startet daraufhin neu. Bevor Windows erscheint, tippen Sie das Kennwort ein. Das sieht hier so aus:

Drücken Sie abschließend auf die ↵-Taste, um Windows zu starten. *[js/mk]*

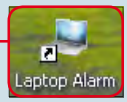
Computer Bild TIPP

Auf Heft-CD/DVD

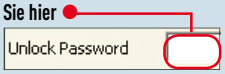
DIEBSTAHLSCHUTZ FÜRS NOTEBOOK

Schützen Sie Ihren tragbaren Computer vor Diebstahl etwa in Cafés, Zügen oder Wartezimmern. Das geht mit dem Programm Laptop-Alarm von der Heft-CD/-DVD. Es lässt eine laute Sirene ertönen, wenn sich jemand unberechtigt am Computer zu schaffen macht. Stellen Sie zuvor sicher, dass die Tonausgabe des Notebooks nicht zu leise ist.

1 Zuerst installieren Sie das Programm aus der Rubrik Titelthema und starten es mit einem Doppelklick auf



. Die folgende Meldung weist darauf hin, dass keine Kopfhörer getragen werden dürfen, während Laptop-Alarm aktiviert ist. Klicken Sie auf OK, Accept, Options, und tippen Sie hier ein Passwort ein. Damit können Sie später den Alarm wieder ausschalten. Es folgt ein Klick auf OK.



2 Klicken Sie im Fenster Syfer.nl - Laptop Alarm auf Lock Computer. Auf diese Weise wird das Notebook für jegliche Bedienung gesperrt und der Alarm eingeschaltet. Jede Mausbewegung, das Abziehen des Strom- oder des Mauskabels lösen einen Sirenenton aus. Ein ahnungsloser Dieb kann das Notebook nicht klauen, ohne Aufmerksamkeit zu erregen. Um den Alarm zu beenden, tippen Sie das Passwort ein und drücken auf ↵. *[mk]*

*Die Erklärung dieses Fachbegriffs finden Sie auf Seite 174/175.

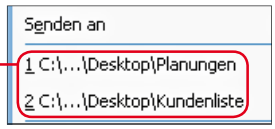
Checkliste: Office & E-Mail

Auch E-Mail-Programme wie Outlook Express und Microsoft Office sind mögliche Gefahrenquellen für Ihren Computer und Ihren Geldbeutel: Schadprogramme und Phishing ▸(S.62) 04-Nachrichten können darüber auf die Festplatte gelangen. Auf den folgenden Seiten erfahren Sie unter anderem, wie sich Sicherheitslücken in Office automatisch stopfen lassen. Zudem können Sie gefährliche Funktionen in der Software abschalten und Ihre Dokumente so als E-Mail-Anhänge verschicken, dass Fremde sie nicht öffnen und heimlich lesen können.

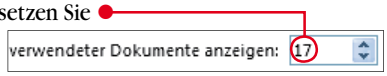
Habe ich geprüft

18 Lässt sich Ihre Arbeit nicht nachverfolgen?

Word, Excel & Co. zeigen nach einem Klick auf Datei an, welche Dokumente Sie zuletzt geöffnet haben, zum Beispiel ●.



Wenn Sie diese verräterischen Spuren entfernen möchten, starten Sie Word und klicken auf Extras sowie Optionen.... Im nächsten Fenster klicken Sie auf Allgemein und entfernen anschließend den grünen Haken vor Liste zuletzt geöffneter. Falls Sie Word 2007 verwenden, klicken Sie stattdessen nacheinander auf ●, Optionen und auf Erweitert. Ersetzen Sie ●



durch die Zahl 0. Bestätigen Sie die Änderung mit einem Mausklick auf OK. Die Dateiliste wird gelöscht und die Funktion ausgeschaltet. Wiederholen Sie diesen Tipp bei Bedarf in Excel und Powerpoint. *[js]*

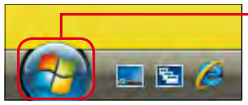
Habe ich geprüft

20 Werden Sicherheitslücken in Office geschlossen?

Wenn Sie den Tipp 11 auf Seite 55 abgehakt haben, ist Windows einigermaßen vor neuen Sicherheitslücken geschützt, da Aktualisierungen automatisch installiert werden. Doch wie sieht's mit den Office-Programmen aus? Gibt es in Outlook & Co. denn keine Sicherheitslücken? Und ob! Aber glücklicherweise lassen sich diese ebenfalls mit regelmäßigen Updates beseitigen.

SO GEHT'S BEI WINDOWS VISTA

Normalerweise sollte Vista bereits so eingestellt sein, dass Office-Updates automatisch aus dem Internet überspielt werden. Überprüfen Sie es sicherheitshalber: Klicken Sie auf ●,



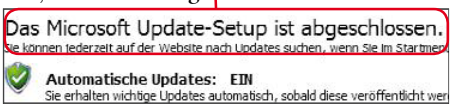
Alle Programme und Windows Update. In der linken Fensterhälfte folgt danach ein Mausklick auf Einstellungen ändern.

Sehen Sie dann hier ●

einen Haken, ist alles in Ordnung, und Sie können das Fenster per Klick auf ✕ schließen. Andernfalls setzen Sie den Haken vorher mit einem Mausklick.

SO GEHT'S BEI WINDOWS XP

Stellen Sie eine Internetverbindung her, und klicken Sie auf Start, Alle Programme und Windows Update. Erscheint das Fenster Microsoft Update, ist alles in Ordnung, und Sie können das Fenster per Klick auf ✕ schließen. Erscheint Microsoft Windows Update, klicken Sie auf Microsoft Update, auf Jetzt beginnen und auf Weiter. Warten Sie ein paar Sekunden, bis die Meldung ●



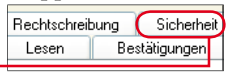
erscheint. Dann folgt ein Klick auf ✕. *[js]*

Habe ich geprüft

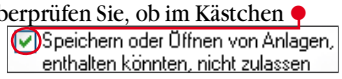
19 Blockiert die E-Mail-Software schädliche Anhänge?

Die meisten Schädlinge gelangen in E-Mail-Anhängen auf den Computer. Normalerweise werden Sie vom Virenschutz-Programm unschädlich gemacht. Wenn Sie ganz sicher gehen wollen, sorgen Sie dafür, dass Ihr E-Mail-Programm Dateiformate*, die Schädlinge enthalten könnten, gar nicht erst auf die Festplatte lässt. Bei Outlook ist das bereits der Fall. Outlook Express und Windows Mail können das normalerweise auch. Schauen Sie nach, ob die Funktion dort wirklich eingeschaltet ist:

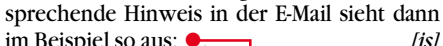
1 Falls noch nicht geschehen, starten Sie Ihr E-Mail-Programm. Klicken Sie dann auf Extras und in der aufklappenden Liste auf Optionen.... Im nächsten Fenster folgt ein Klick auf ●.



2 Überprüfen Sie, ob im Kästchen ●



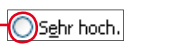
ein Häkchen steht. Ist das bei Ihnen nicht der Fall, setzen Sie es per Mausklick. Schließen Sie dann die Einstellungen per Klick auf OK ab. Outlook Express oder Windows Mail blockieren nun auch verdächtige Dateien. Der entsprechende Hinweis in der E-Mail sieht dann im Beispiel so aus: ●. *[js]*



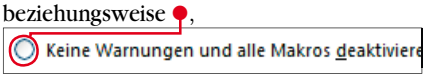
Habe ich geprüft

21 Können Office-Dateien keinen Schaden anrichten?

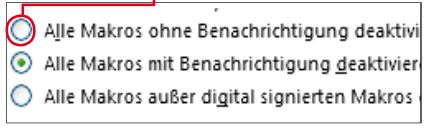
Makros sind kleine Programme mit Befehlszeilen, die die Arbeit mit Word, Excel, Powerpoint und Outlook vereinfachen. Leider gibt's neben vielen nützlichen auch schädliche Makros, die zum Beispiel Dateien löschen können. Schalten Sie die Funktion deshalb lieber ab: Bei Office 2002, 2003 und Outlook 2007 klicken Sie dazu auf Extras, Makro und Sicherheit. Klicken Sie anschließend auf ●



beziehungsweise ●,



sodass dort ein Punkt erscheint. Schließen Sie das Fenster danach mit einem Klick auf OK. Bei Word, Excel und Powerpoint 2007 klicken Sie zum Deaktivieren auf ●, anschließend auf Optionen und danach auf Vertrauensstellungscenter. Nach einem Mausklick auf Einstellungen für das Vertrauensstellungscenter... setzen Sie hier ●



einen Punkt und schließen die beiden offenen Fenster jeweils per Klick auf OK. *[js]*

Computer Bild TIPP

DATEIEN SICHER MAILEN

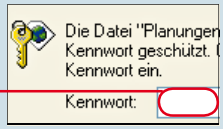
E-Mails sind wie Postkarten. Denn sie jagen schließlich im Klartext durchs weltweite Datennetz. Schützen Sie wenigstens Ihre Word-Dokumente, Excel-Tabellen oder Bilder, bevor Sie sie per E-Mail verschicken. Dazu brauchen Sie die Dokumente nur in eine ZIP ▸(S.62) 04-Datei zu packen und mit einem Kennwort zu sperren. Die entsprechende Funktion ist in Windows XP bereits eingebaut:

1 Klicken Sie mit der *rechten* Maustaste auf die gewünschte Datei, im Beispiel ●,

und wählen Sie dann in der Liste die Einträge Senden an und ZIP-komprimierten Ordner per Mausklick aus. Übrigens: Falls Sie mehrere Dateien zusammenfassen möchten, markieren Sie sie zuvor bei gedrückter Strg-Taste.

2 Öffnen Sie nun mit einem Doppelklick die Zip-Datei, hier ●.

Im nächsten Fenster klicken Sie auf Datei und auf Ein Kennwort hinzufügen.... Tippen Sie neben Kennwort: ein beliebiges Passwort ein, und wiederholen Sie es neben Kennwort bestätigen:. Klicken Sie auf OK, und schließen Sie das Fenster per Klick auf ✕. Jetzt können Sie die Zip-Datei wie gewohnt per E-Mail verschicken. Der Empfänger wird beim Öffnen aufgefordert, das Kennwort einzugeben: ●.



Natürlich müssen Sie es ihm zuvor noch mitteilen, am besten telefonisch. *[js]*

*Die Erklärung dieses Fachbegriffs finden Sie auf Seite 174/175.

Habe ich geprüft

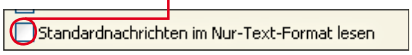
22 Werden E-Mails automatisch im Textmodus angezeigt?

Bunte, farbenfrohe E-Mails sind zwar schön anzusehen, bergen aber auch Risiken. Denn immer mehr Schädlinge verstecken sich in scheinbar harmlosen Bildchen. Gehen Sie auf Nummer sicher, und öffnen Sie alle neuen E-Mails als Textnachricht. Sie können dann immer noch von Fall zu Fall entscheiden, ob Sie die jeweilige E-Mail in ganzer Pracht genießen möchten. So funktioniert's:

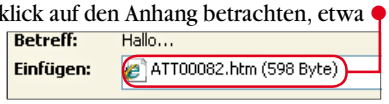
1 Starten Sie Ihr E-Mail-Programm. Klicken Sie auf Extras und in der Liste auf Optionen... Bei Outlook 2007 klicken Sie stattdessen auf den Eintrag Vertrauensstellungscenter...

Im nächsten Fenster klicken Sie auf Lesen, dann bei Outlook 2002/2003 auf E-Mail-Optionen... und bei Outlook 2007 auf E-Mail-Sicherheit.

2 In allen Outlook-Versionen setzen Sie anschließend hier



mit einem Mausklick einen Haken. In Outlook Express und Windows Mail heißt der Eintrag Alle Nachrichten als Nur-Text lesen. Schließen Sie alle Einstellungsfenster per Klick auf OK. Künftig werden alle E-Mails als Text ohne Bilder angezeigt. Wenn Sie einem Absender vertrauen, können Sie die komplette Nachricht per Doppelklick auf den Anhang betrachten, etwa



oder Sie klicken mit der Maus auf den Eintrag Diese Nachricht wurde zum Nur-Text-Format und anschließend auf Als HTML anzeigen. *[js]*

Habe ich geprüft

23 Sind Sie vor Phishing-E-Mails sicher?

Regelmäßig ist Ihr elektronisches Postfach mit Werbung überfüllt? Dann haben Sie offenbar keinen Spamfilter installiert. An bunte Werbeversprechen kann man sich zwar zähneknirschend gewöhnen, doch Vorsicht: Unter den Angeboten für Pillen, Partnerschaften und Pokerrunden lauern auch Gefahren für Ihren Geldbeutel: fiese **Phishing** (S.62) 04-Nachrichten! Spamfilter schützen daher nicht nur vor unerwünschter, sondern auch vor gefährlicher Post. Deshalb sollten Sie diese Schutzmaßnahmen in jedem Fall anwenden:

FILTER DES ANBIETERS NUTZEN

Am besten ist die Werbung, die gar nicht erst auf Ihre Festplatte gelangt. Fragen Sie daher Ihren E-Mail-Anbieter, ob er einen eingebauten Werbefilter für Ihr Postfach anbietet. Bietet der Dienst keinen (wirksamen) Schutz, empfiehlt sich der Wechsel des Anbieters. Die besten Werbefilter bei den Gratis-Postfächern boten im Test von COMPUTERBILD 15/2008 GMX Freemail, Jubii und Google Mail.

Bietet Ihr Dienst diesen Filter, prüfen Sie auf der Internetseite des Anbieters, ob diese Schutzfunktion auch aktiv ist. Das ist nämlich nicht immer automatisch der Fall. Bei GMX Freemail beispielsweise klicken Sie nach der Anmeldung auf

Erscheint dann GMX Spamschutz aktiv können Sie sich wieder abmelden. Ist dagegen Ihr GMX Spamschutz ist nicht aktiv! zu sehen, klicken Sie zuvor noch auf den Eintrag GMX Spam-Schutz aktivieren!. Jetzt können Sie den Filter nach einem Mausklick auf persönliche Einstellungen vornehmen, noch „schärfer" einstellen. Danach folgt ein Klick auf übernehmen.

FILTER AUF DEM PC NUTZEN

Auch durch den besten Werbefilter der E-Mail-Anbieter rutschen mitunter lästige oder gar gefährliche Nachrichten. Die E-Mail-Programme Outlook, Windows Mail und Thunderbird verfügen daher über eingebaute Filter, die solche Post herausfischen. Leider gilt das nicht für das in Windows XP enthaltene Outlook Express. Dort sollten Sie einen zusätzlichen Filter installieren, etwa Spampal, den Sie unter dem Webcode 10345[1]) aus dem Internet laden können. Falls Sie ohnehin die Kaspersky Security Suite CBE von der COMPUTERBILD-Heft-CD/-DVD installiert haben, werden Sie bereits wirksam durch den Filter „Anti-Spam" geschützt: *[hes]*

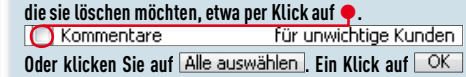
Computer Bild TIPP

DATEI-INFOS LÖSCHEN

Wenn Sie Word- oder Excel-Dateien per E-Mail verschicken, kann der Empfänger nicht nur den Inhalt des Dokuments einsehen. Er erfährt zum Beispiel auch, wann und von wem die Datei bearbeitet wurde, oder er bekommt sogar peinliche Kommentare zu lesen. So entfernen Sie diese Daten:

SO GEHT'S BEI WINDOWS VISTA

In Windows Vista haben Sie die Möglichkeit, die Dateiinfos in einem Rutsch aus mehreren Dokumenten zu entfernen. Markieren Sie dazu die gewünschten Dateien, zum Beispiel bei gedrückter Strg-Taste, und klicken Sie mit der *rechten* Maustaste auf die Markierung. In der Liste klicken Sie auf Eigenschaften und auf Details. Klicken Sie auf Eigenschaften und persönliche Informationen entfernen und Folgende Eigenschaften aus dieser Datei, sodass dort ein Punkt erscheint. Markieren Sie nun die Infos, die sie löschen möchten, etwa per Klick auf

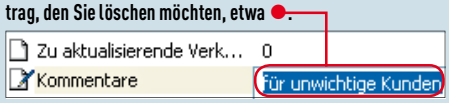


Oder klicken Sie auf Alle auswählen. Ein Klick auf OK löscht die gewählten Angaben. Klicken Sie auf OK.

SO GEHT'S BEI WINDOWS XP

Bei Windows XP müssen Sie die Dateien einzeln auswählen und auch die Infos einzeln daraus löschen. Klicken Sie dazu mit der *rechten* Maustaste auf die gewünschte Datei, in diesem Beispiel

und dann in der Liste auf Eigenschaften. Es folgt ein Mausklick auf Dateiinfo. Als Nächstes klicken Sie auf den ersten Eintrag, den Sie löschen möchten, etwa



Mit der Taste ← entfernen Sie ihn. Wiederholen Sie das bei Bedarf für weitere Infos. Nach einem Klick auf OK können Sie die Datei ruhigen Gewissens verschicken. *[js]*

WAS IST EIGENTLICH?

01 Benutzerkonto
Windows lässt sich auf einem PC für verschiedene Personen einrichten. Vorteil: Jeder Computernutzer kann seine Arbeitsoberfläche nach eigenen Wünschen gestalten. Außerdem bleiben die persönlichen Dateien auf diese Weise geschützt.

02 Administrator
Unter Windows gibt es verschiedene Arten von Benutzerkonten: Konten mit eingeschränkten Rechten und Administratorkonten. Ein Administrator darf zum Beispiel neue Programme installieren und weitere Benutzerkonten anlegen.

03 Verschlüsselung
Daten können nach einer komplizierten Regel, dem sogenannten Schlüssel, in scheinbar wirre Zeichenfolgen umgewandelt („verschlüsselt") werden. Nur wer im Besitz des festgelegten Kennworts ist, kann verschlüsselte Daten wieder nutzbar machen.

04 Phishing
Das Wort Phishing setzt sich aus den englischen Begriffen Password (Passwort) sowie Fishing (Fischen) zusammen. Dabei versuchen Betrüger mithilfe gefälschter E-Mails und Internetseiten Kennwörter von Bank- und Auktionshaus-Kunden auszuspähen.

05 BIOS
BIOS steht für „Basic Input Output System" (Basis-Eingabe-Ausgabe-Programm). Es prüft nach dem Einschalten die Computer-Bauteile und lädt das Betriebsprogramm.

06 ZIP
Das ist ein Verfahren zum Schrumpfen von Dateien. Eine ZIP-Datei kann mehrere komprimierte Dateien enthalten und per Kennwort geschützt werden.

*Weitere Fachbegriffs-Erklärungen auf Seite 174/175

[1]) Wie die Webcodes funktionieren, steht auf Seite 18.

Checkliste: Internet

Zwar geht vom Internet die größte Gefahr für Computer und Geldbörse aus. Dennoch reichen wenige Maßnahmen, um sich wirksam zu schützen. Auf dieser Seite lesen Sie, wie Sie Ihr Internet-Zugriffsprogramm vor Schadsoftware und Betrugsversuchen abschotten, wie Sie einen riskanten Netzwerkdienst abschalten und welche Regeln den Umgang mit Geld sicherer machen. Achten Sie auch auf einen sicheren Arbeitsplatz: Verhindern Sie, dass Fremde in Ihrem Namen Internetseiten besuchen und so an Ihr Geld kommen können.

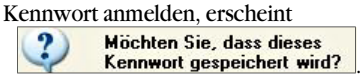
Habe ich geprüft

24 Sind Sie sicher vor Identitätsklau?

Die Kennwortspeicherung des Internet-Zugriffsprogramms ist ja so bequem: Automatisch trägt sie Ihre Kennwörter auf Internetseiten ein. Aber Vorsicht: Haben andere Personen Zugriff auf den PC, oder verwenden Sie ein Notebook (Verlustgefahr!) können Fremde einfach Ihr Bankkonto ausspähen oder auf Ihre Kosten einkaufen. Verwenden Sie als Ausfüllhilfe besser Kee Pass (Tipp 8), und entfernen Sie die Daten aus dem Zugriffsprogramm.

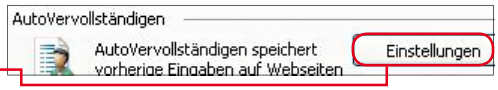
SO GEHT'S BEIM INTERNET EXPLORER

Klicken Sie auf Extras und in der Liste auf Browserverlauf löschen... Nach Mausklicks auf Kennwörter löschen... und auf Ja sind Ihre Daten entfernt. Es folgt ein Klick auf Schließen. Wenn Sie sich das nächste Mal bei einer Internetseite per Kennwort anmelden, erscheint

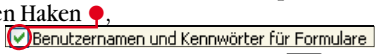


Klicken Sie künftig bei Internetseiten von Banken, Postfächern, Ebay und Co. auf Nein.

Am sichersten ist es, die Kennwort-Speicherung ganz auszuschalten. Klicken Sie dazu auf Extras und dann auf Internetoptionen. Nach einem Klick auf Inhalte klicken Sie auf ●.



Entfernen Sie im nächsten Fenster per Mausklick den Haken ●, und

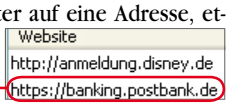


klicken Sie anschließend zweimal auf OK.

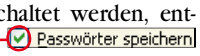
SO GEHT'S BEI FIREFOX

Im Firefox lassen sich Kennwörter einzeln löschen: Klicken Sie auf Extras, auf Einstellungen... und auf ●.

Danach klicken Sie auf Gespeicherte Passwörter... und im nächsten Fenster auf eine Adresse, etwa auf ●.



Nach einem Klick auf Entfernen ist das dazugehörige Passwort von der Platte gelöscht. Wiederholen Sie das gegebenenfalls für weitere Passwörter, oder klicken Sie auf Alle entfernen und Ja, um alle Kennwörter zu löschen. Es folgt ein Klick auf Schließen. Soll die Kennwortspeicherung ganz ausgeschaltet werden, entfernen Sie den Haken ●.



Es folgt ein Klick auf OK. Wurde die Speicherung nicht ausgeschaltet, erscheint nach einer Kennworteingabe künftig gegebenenfalls die Leiste

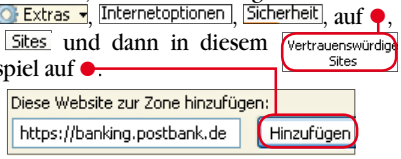
Bei riskanten Seiten klicken Sie dann besser auf Nie für diese Website. *[bes]*

Habe ich geprüft

27 Ist der Computer sicher vor schädlichen Internetseiten?

Viele Internetseiten enthalten Programme, die ohne Ihr Wissen auf dem Computer gestartet werden. Meist sind das nützliche Funktionen, oft aber auch Schädlinge. Leider kann der Internet Explorer nicht zwischen guter und böser Software unterscheiden. Am sichersten ist es daher, wenn Sie alle Programme verbieten: Klicken Sie dazu auf Extras, Internetoptionen und Sicherheit. Stellen Sie dann mit dem Regler unter Sicherheitsstufe dieser Zone die Stufe Hoch ein. Nach einem Klick auf OK ist der PC sicher.

Eventuell funktionieren jetzt manche Internetseiten nicht mehr. Handelt es sich um wichtige Seiten (etwa Bankseiten), die ungefährlich sind, klicken Sie bei geladener Seite auf Extras, Internetoptionen, Sicherheit, auf ●, auf Sites und dann in diesem Beispiel auf ●.



Erscheint Sites müssen das "https://"-Präfix, klicken Sie auf OK, entfernen den Haken Für Sites und klicken erneut auf Hinzufügen. Nach Klicks auf Schließen und auf OK sind Programmfunktionen auf dieser Internetseite erlaubt. *[bes]*

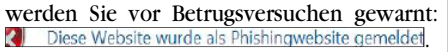
Habe ich geprüft

25 Sind Sie vor gefälschten Seiten sicher?

Betrüger haben es auf Ihre Zugangsdaten abgesehen, zum Beispiel für Banken und Internet-Shops. Internet Explorer und Firefox bieten Schutz vor solchen Phishing ▸(S.62) 04-Fallen. Prüfen Sie, ob dieser Schutz aktiv ist:

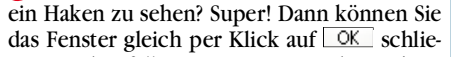
SO GEHT'S IM INTERNET EXPLORER

Klicken Sie auf Extras und Phishingfilter. Steht dort Automatische Websiteprüfung ausschalten, ist alles in Ordnung. Andernfalls folgen Klicks auf Websiteprüfung einschalten und OK. Künftig werden Sie vor Betrugsversuchen gewarnt:



SO GEHT'S IM FIREFOX

Klicken Sie auf Extras, auf Einstellungen... und auf Sicherheit. Ist hier ●



ein Haken zu sehen? Super! Dann können Sie das Fenster gleich per Klick auf OK schließen. Andernfalls setzen Sie zuvor den Haken. Firefox warnt künftig mit der Meldung

vor gefährlichen Seiten. *[js]*

Habe ich geprüft

26 Ist der Bonjour-Dienst von iTunes abgeschaltet?

Bonjour? Das ist eine Netzwerktechnologie des Computer- und iPod-Herstellers Apple, die irgendwie richtig freundlich klingt. Weniger nett: Wer das Apple-Programm iTunes auf dem PC installiert, der bekommt zwangsweise Bonjour auf den Computer. Mit Bonjour lassen sich in Netzwerken gemeinsam Musikstücke nutzen, spezielle Netzwerk-Drucker, -Lautsprecher und -Videogeräte anschließen. Haben Sie nicht? Dann sagen Sie dem Dienst „Adieu", und deinstallieren sie ihn. So schließen Sie ein Einfallstor für Angriffe aus dem Internet.

Ist Bonjour auf Ihrem PC installiert? Um es herauszufinden, klicken Sie nacheinander auf Start, Systemsteuerung und ●.

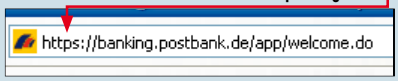
Schauen Sie in der folgenden Liste nach, ob dort Bonjour auftaucht. Ist das nicht der Fall, können Sie die offenen Fenster per Klick auf schließen. Andernfalls klicken Sie zuvor auf Bonjour, auf Entfernen und Ja. Beim nächsten iTunes-Start bestätigen Sie das Fehlen von Bonjour per Klick auf OK. *[bes]*

Computer Bild TIPP

DREI GOLDENE REGELN ZUM SCHUTZ VOR GAUNERN IM INTERNET

Phishing ist die größte Gefahr für Ihr Geld: Internetgauner fälschen dazu E-Mails, die zu (ebenfalls gefälschen) Internetseiten von Banken oder Internet-Auktionshäusern wie Ebay führen. Dort werden Kreditkarten-, Konto- oder Zugangsdaten erfragt, um an Ihr Erspartes zu kommen oder um auf Ihre Kosten einzukaufen. Mit diesen drei goldenen Regeln schützen Sie sich:

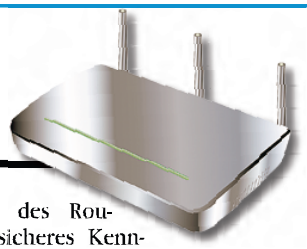
- **Antworten Sie niemals auf E-Mails einer Bank oder eines Online-Auktionshauses. Klicken Sie in solchen E-Mails niemals auf Links*, die angeblich zur Internetseite des Anbieters führen.**
- **Geben Sie in Internetformularen nie Kontonummer, Persönliche Indentifikationsnummer (PIN) und Transaktionsnummer (TAN) zusammen ein. Echte Banken erfragen die TAN erst zum Abschluss der Überweisung.**
- **Vertrauen Sie Internetformularen nur dann, wenn die Adresse der Seite mit den Buchstaben „https" beginnt: ●.**



Außerdem muss neben der Adresse (Internet Explorer) oder am unteren Fensterrand (Firefox) ein kleines Schlosssymbol zu sehen sein. Nur dann werden Ihre Daten verschlüsselt ▸(S.62) 03 übertragen. *[bes]*

*Die Erklärung dieses Fachbegriffs finden Sie auf Seite 174/175.

Checkliste: WLAN & Router



Für Hacker ist ein ungesichertes WLAN* ein gefundenes Fressen. Denn das Funknetz ist meist auch auf der Straße oder im Nachbarhaus zu empfangen. Effektiven Schutz bietet nur das WLAN-Verschlüsselungsverfahren „WPA“, am besten in der neuesten Variante „WPA2“. Zwar beherrschen alle modernen Router diese Technik. Doch noch immer werden viele Geräte verkauft, in denen dieser wichtige Schutz ausgeschaltet ist. Wie Sie herausbekommen, ob und wie Ihr Funknetzwerk gesichert ist, lesen Sie auf diesen Seiten. Zudem erfahren Sie, wie Sie sowohl für den WLAN-Zugang als auch für das Einstellmenü des Routers ein sicheres Kennwort festlegen. So können sich Eindringlinge das WLAN-Kennwort nicht einfach über das Internet-Zugriffsprogramm anzeigen lassen.

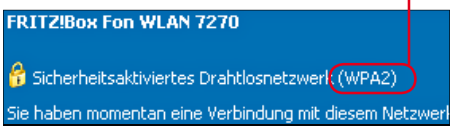
Habe ich geprüft

28 Ist Ihre WLAN-Verbindung mit WPA-Verschlüsselung gesichert?

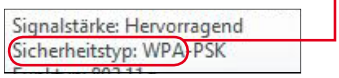
Sie nutzen einen WLAN-Router? Dann müssen Sie die Funkverbindung per WPA-Verschlüsselung absichern. Bei vielen WLAN-Routern wird aber noch das veraltete Verschlüsselungsverfahren WEP oder gar keine Verschlüsselung eingesetzt. Im Folgenden überprüfen Sie, ob Ihr WLAN sicher ist, und aktivieren bei Bedarf die WPA-Verschlüsselung:

WLAN-VERBINDUNG ÜBERPRÜFEN

Klicken Sie bei bestehender WLAN-Verbindung unter XP mit der *rechten* Maustaste auf und dann auf **Verfügbare Drahtlosnetzwerke anzeigen**. Bei Windows Vista klicken Sie aufs WLAN-Symbol und auf Verbindung herstellen oder trennen. Anschließend erscheint eine Liste der verfügbaren Funknetze. Achtung: Nicht jedes WLAN, das Windows als „sicherheitsaktiviert“ bezeichnet, ist auch wirklich sicher. Das ist die Verschlüsselung nur, wenn hinter dem Netzwerknamen das Kürzel WPA oder WPA2 steht:



Hinweis: Bei Vista müssen Sie den Mauszeiger über den WLAN-Netzwerknamen führen. Erst dann wird die Verschlüsselung angezeigt:



Ist Ihr WLAN nicht WPA- oder WPA2-verschlüsselt, lesen Sie in den nächsten Schritten, wie Sie die Verfahren aktivieren.

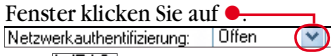
AKTUALISIERUNG VON WINDOWS XP

Windows Vista ist bereits für Funkverbindungen mit WPA2-Verschlüsselung ausgestattet. Bei Windows XP wird die Funktion erst mit der Software-Aktualisierung Service Pack 3 nachgerüstet. Führen Sie daher zuerst Tipp 11 durch, um Windows gegebenenfalls auf den neuesten Stand zu bringen.

WLAN-KARTE AUF WPA PRÜFEN

Viele ältere WLAN-Karten sind nicht WPA-fähig. So prüfen Sie die Ihres PCs: Klicken Sie mit der *rechten* Maustaste auf

und dann auf Erweiterte Einstellungen ändern. Klicken Sie danach auf Drahtlosnetzwerke und auf Hinzufügen... Im nächsten Fenster klicken Sie auf



Ist WPA oder WPA2 in der aufklappenden Liste aufgeführt, ist Ihre WLAN-Karte bereits WPA-fähig. Schließen Sie das Fenster per Klick auf . Ist WPA nicht aufgelistet, prüfen Sie auf der Internetseite des WLAN-Karten- oder PC-Herstellers, ob eine Treiberaktualisierung für WPA verfügbar ist. Oder kaufen Sie einen neuen WPA-fähigen WLAN-USB-Adapter, zum Beispiel den AVM Fritz WLAN USB (rund 30 Euro).

ÄLTERE ROUTER AKTUALISIEREN

Bei Routern, die älter als etwa zwei Jahre sind, müssen Sie zum Einrichten der WPA-Verschlüsselung meist die Router-Software („Firmware“) aktualisieren. Lesen Sie am Beispiel des Speedport W501, wie die Aktualisierung funktioniert. Bei anderen Routern geht's ähnlich.

1 Rufen Sie den „Download“-Bereich auf der Internetseite des Routerherstellers auf (die wichtigsten Internetadressen finden Sie bei www.computerbild.de unter dem Webcode 10265[1]). Wählen Sie Ihren Router, etwa den Telekom Speedport W501V mit Klicks auf DSL-Hardware, Speedport Serie, auf Speedport W 5xx-Se und auf Speedport W 501 V.

2 Nun wird die Firmware angezeigt, etwa Firmware Version 28.04.38 des Speedport W 501V. Im Beispiel laden Sie die Firmware per Klick auf Download herunter. Speichern Sie die Datei auf der Festplatte Ihres Computers, beispielsweise auf der Arbeitsoberfläche* (Desktop).

3 Rufen Sie das Routermenü auf. Tippen Sie dazu in Ihrem Internet-Zugriffsprogramm die im Handbuch angegebene Adresse des Routermenüs ein. Für Speedport-Router ist das etwa http://speedport.ip, für die Fritz Box http://fritz.box. Rufen Sie das Menü zum Firmware-Update auf. Beim Speedport klicken Sie dazu einmal auf **Konfiguration starten** und auf **Laden & Sichern**. Bei der Fritz Box klicken Sie auf **Einstellungen** (teils auch „Erweiterte Einstellungen“), auf **System** und auf Firmware-Update. Wählen Sie dann die in Schritt 2 gespeicherte Firmware-Datei. Die Aktualisierung dauert einige Minuten. Danach ist der Router wieder einsatzbereit.

WPA-VERSCHLÜSSELUNG AKTIVIEREN

1 Rufen Sie das Routermenü auf, wie zuvor in Schritt 3 beschrieben. Starten Sie das Konfigurationsmenü: bei Speedport-Routern etwa per Klick auf **Konfiguration starten**, bei der Fritz Box auf **Einstellungen**. Bei neueren Fritz-Box-Modellen klicken Sie dann auf „Erweiterte Einstellungen“.

2 Klicken Sie bei der Fritz Box im Menü WLAN auf **> Sicherheit** (bei anderen Routern auf „WLAN“ oder „Verschlüsselung“), und aktivieren Sie die WPA- oder WPA2-Verschlüsselung. Die Einstellungen sehen je nach Router anders aus. Bei neueren Fritz Boxen etwa lassen sich per Klick auf WPA / WPA2 mit Pre-shared key sowohl Verbindungen mit WPA- als auch mit WPA2-Verschlüsselung nutzen. Bei anderen Routern wählen Sie entweder WPA oder WPA2. Beide Verfahren gelten derzeit als sicher.

Wichtig: Sind für WPA oder WPA2 mehrere Einträge aufgelistet, wählen Sie stets die Variante mit dem Zusatz „Pre-Shared Key“ oder „PSK“.

3 Tippen Sie ein selbst ausgedachtes sicheres Kennwort in das Feld

ein. Klicken Sie bei der Fritz Box einmal auf Übernehmen, andernfalls auf **Speichern <<**. Beachten Sie zur Kennwort-Wahl den Tipp 29. Der Router startet danach automatisch neu. Warten Sie mehrere Minuten, bis keine Leuchtanzeige am Gerät mehr blinkt.

4 Ihr WLAN ist nun sicher verschlüsselt. Es sind aber noch die alten Einstellungen gespeichert. Um sie zu löschen, klicken Sie unter XP mit der *rechten* Maustaste auf . Dann klicken Sie auf **Verfügbare Drahtlosnetzwerke anzeigen** und danach auf .

Unter Vista klicken Sie auf , dann auf Netzwerk- und Freigabecenter und im Anschluss auf Drahtlosnetzwerke verwalten. Die im Computer gespeicherten Funknetzwerke werden daraufhin angezeigt. Klicken Sie auf den Namen Ihres WLANs, und löschen Sie die Einstellung mit einem Klick auf Entfernen.

5 Anschließend müssen Sie die Verbindung zum WLAN neu herstellen. Klicken Sie mit der *rechten* Maustaste auf . Bei XP klicken Sie dann auf **Verfügbare Drahtlosnetzwerke anzeigen**, bei Vista auf Verbindung herstellen oder trennen. Klicken Sie danach auf den Namen Ihres WLANs, zum Beispiel .

Unter Windows XP stellen Sie die Verbindung mit einem Mausklick auf Verbinden her, unter Vista per Klick auf Verbindung herstellen. Ihr Computer erkennt automatisch, welches WLAN-Verschlüsselungsverfahren im Router eingestellt ist. Tippen Sie das in Schritt 3 festgelegte Kennwort in das erscheinende Abfragefenster ein, und klicken Sie auf Verbinden. Das Kennwort wird daraufhin vom Computer gespeichert. Künftig stellt er die Verbindung zum Netzwerk automatisch her. Wiederholen Sie Schritt 4 und 5 mit allen Computern in Ihrem WLAN. *[cj]*

*Die Erklärung dieses Fachbegriffs finden Sie auf Seite 174/175.

[1]Wie die Webcodes funktionieren, lesen Sie auf Seite 18.

Habe ich geprüft

29 Ist Ihr WLAN-Kennwort sicher?

Das in Tipp 28 eingestellte WPA-Verfahren gilt derzeit als sicher. Dennoch bleibt eine prinzipielle Schwachstelle bestehen: das WLAN-Kennwort selbst. Wer hier aus Bequemlichkeit einen allzu trivialen Begriff wie Vorname („Volker2“) oder Kosename („Schatzi“), Begriffe aus dem Wörterbuch oder ein Geburtsdatum eintippt, öffnet ungebetenen Gästen Tür und Tor. Denn längst gibt's Programme, die automatisch umfangreiche Wortlisten abarbeiten, um ein WLAN zu knacken. Diese sogenannte „Lexikon-Attacke“ ist bei Hackern sehr beliebt. An einem sicheren Kennwort führt daher kein Weg vorbei. Der Nachteil: Es lässt sich schlecht merken. Mit einem Trick geht's doch:

1 Wählen Sie einen Ihnen geläufigen Satz mit mindestens fünf Wörtern oder mehr. Notieren Sie sich die Anfangsbuchstaben, bei Bedarf inklusive Satzzeichen: für den Satz „**Es gibt kein Bier auf Hawaii**“ etwa „**EgkBaH**“.

2 Setzen Sie in die Mitte des Satzes eine beliebige Zahl, etwa „423“. Der Beispielsatz könnte somit lauten: „Es gibt kein Bier 423 auf Hawaii.“ Merken Sie sich diesen Satz.

3 Das dazugehörige Kennwort zur Absicherung von WLAN und Routermenü lautet nun „EgkB423aH“. Wichtig: Beachten Sie die Unterschiede in der Groß- und Kleinschreibung. Wenn Sie den Kennwortsatz nun nicht am Kneipentisch ausplaudern, ist der Passwortschutz Ihres WLANs sicher. *[cj]*

Computer Bild TIPP

WPA2-PROBLEME BEHEBEN

Scheitert die WPA-Verbindung in Tipp 28, hilft Folgendes:

- **Wählen Sie in Schritt 2 des Abschnitts „WPA-Verschlüsselung aktivieren“ nur WPA oder nur WPA2 anstelle von WPA/WPA2.**
- **Manche Router bieten bei WPA noch die Wahl zwischen dem TKIP- und AES-Verfahren. Probieren Sie beide aus.**
- **Stellen Sie Ihren Router von WPA2 auf WPA um.**
- **Löschen Sie alte WLAN-Einstellungen, wie in Schritt 4 des Abschnitts „WPA-Verschlüsselung aktivieren“ erklärt.** *[cj]*

Habe ich geprüft

30 Ist Ihr Router kennwortgeschützt?

Mit der Vergabe eines WLAN-Kennworts in Tipp 28 ist Ihr Funknetz sicher. Aber was ist mit dem Routermenü? Falls Sie das nicht mit einem eigenen Kennwort geschützt haben, ist es ohne oder mit einem vorab eingestellten Standardkennwort wie „0000“ auch anderen zugänglich. Ihre Kinder etwa könnten die Einstellungen des Routers verändern. In bestimmten Fällen sind sogar Zugriffe aus dem Internet möglich. Stoppen Sie das:

1 Rufen Sie das Routermenü auf. Dazu tippen Sie statt einer Internetadresse die Menü-Adresse des Geräts im Internet-Zugriffsprogramm ein. Bei der Fritz Box ist das http://fritz.box und beim Speedport http://speedport.ip. Werden Sie zur Eingabe eines Kennworts aufgefordert, geben Sie es ein. Sie finden es auf der Geräteunterseite oder im Handbuch. Wählen Sie im Menü „Einstellungen“ oder „Konfiguration“, danach gegebenenfalls „Erweiterte Einstellungen“. Wählen Sie danach das Menü für das System- oder Router-Kennwort:

- Bei Speedport-Geräten befindet es sich unter **Sicherheit** und System Passwort.
- Bei Fritz-Box-Modellen finden Sie das Kennwort in den Einstellungen unter System und FRITZ!Box-Kennwort.
- Bei Siemens-Routern wählen Sie Verwaltung und dann „Passwort“ oder „Systemkennwort“.

2 Tippen Sie ein schwer zu erratendes Passwort Ihrer Wahl ein (siehe Tipp 29). Merken Sie es sich, und klicken Sie auf **Speichern <<** oder auf Übernehmen.

Künftig müssen Sie dieses Kennwort vor jedem Zugriff auf das Routermenü eintippen. Auch ein eventueller Fernzugriff über das Internet ist dann nur noch nach Eingabe dieses Kennworts möglich. *[cj]*

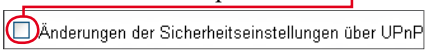
Habe ich geprüft

31 Ist UPnP im Router ausgeschaltet?

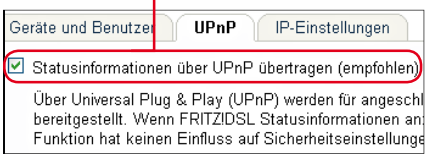
Sie spielen gerne übers Internet mit anderen am Computer oder an der Spielekonsole? Oder Sie nutzen Internet-Plauderprogramme? Dann bremst häufig die im Router eingebaute Kontrolle der Datenübertragung per Firewall* das Tempo – und den Spaß. Viele Nutzer heben deshalb die Sicherheitsfunktionen für diese Anwendungen über eine sogenannte „Port-Freigabe“ auf. Erfolgt diese Freigabe automatisch, drohen Sicherheitsrisiken. Solange Sie etwa für Internetspiele nicht auf eine Port-Freigabe angewiesen sind (siehe COMPUTERBILD 14/2008, Seite 94 und 96), sollten Sie sie per UPnP in Ihrem Router ausschalten. So funktioniert's bei der Fritz Box 7270 (bei anderen Routern geht's ähnlich):

1 Rufen Sie das Routermenü auf, wie in Schritt 1 in Tipp 30 beschrieben. Klicken Sie auf Einstellungen und Erweiterte Einstellungen, bei anderen Routern auch auf „Konfiguration“.

2 Suchen Sie den Menüpunkt für die Sicherheitseinstellungen per UPnP. Diesen finden Sie bei der Fritz Box unter den Einträgen System und Netzwerk. Bei anderen Routern finden Sie den Menüpunkt auch unter „Sicherheit“, „Firewall“ oder „Port-Freigabe“ („Port-Forwarding“). Prüfen Sie als Nächstes, ob die Änderung der Sicherheitseinstellungen (Port-Freigabe) per UPnP deaktiviert ist. Bei der Fritz Box zum Beispiel darf hier



kein Haken gesetzt sein. Andernfalls entfernen Sie ihn per Klick. Achtung: Die Änderung der Sicherheitseinstellungen per UPnP ist nicht zu verwechseln mit der Statusanzeige oder Musikverwaltung per UPnP. Diese Funktionen sind unbedenklich:



Speichern Sie die Einstellungen, bei der Fritz Box etwa per Klick auf Übernehmen. *[cj]*