Achtung, Betrüger!

Die Antiviren-Software allein genügt nicht: Wer das Internet nutzt, muss Regeln beachten, um sich vor Viren und Hackern zu schützen.

Die meisten PC-Besitzer, die häufig oder auch nur gelegentlich im Internet surfen, haben ein Antiviren-Programm und eine Firewall installiert. Diese zwei Sicherheits-Tools bieten einen guten Schutz gegen allerlei Viren, Würmer und Trojaner, sodass man sich im Normalfall keine Sorgen um die Sicherheit machen muss.

Trotzdem kann es vorkommen, dass ein virtueller Schädling auf den Computer gelangt und sich auf dem Rechner installiert. Dies passiert einerseits, weil die Sicherheits-Softwares nicht 100 Prozent der sogenannten Malware erkennen können. Doch sind es andererseits in vielen Fällen die Nutzer selbst, die es mit ihrem unvorsichtigen Verhalten den Viren, Hackern und Online-Betrügern ermöglichen, auf dem Computer Schaden anzurichten oder gar mit gestohlenen Kreditkartenangaben das Konto zu plündern.

Hacker wollen Geld

War es in den Anfangszeiten des Internets noch einfacher zu erkennen, dass ein Computer von einem Virus befallen war, machen sich die Schädlinge heute kaum noch bemerkbar. Der Grund dafür: Früher waren die Hacker eher aus sportlichem Ehrgeiz daran interessiert, in ein gut gesichertes System einzudringen oder ihren selbst gebastelten Virus an möglichst viele PCs auf der ganzen Welt zu senden. So wurden einzelne Viren gar zu Berühmtheiten wie der «I love You»-Virus. Einzelne Hacker blamierten manche Bank, ohne den Geldinstituten wesentlich Schaden zuzufügen.

Heutzutage hingegen sind die Interessen der Hacker immer öfter finanzieller Natur. Cyberkriminelle versuchen beispielsweise durch Phishing an die Kennwörter fürs Online-Banking zu gelangen oder übernehmen die Identität eines Nutzers, um in dessen Namen Dritten Schaden zuzufügen. Diese Entwicklung beschreibt der halbjährlich erscheinende «Symantec Internet Security Threat Report», der eine regelrechte Professionalisierung und Kommerzialisierung der Internetkriminalität in den letzten zwei Jahren ausmacht.

Vorsicht bei Bankgeschäften

Was nützt es, wenn man zwar die beste Antiviren- und Firewall-Software hat, jedoch unbekannten Mail-Absendern ohne mit der Wimper zu zucken Kreditkarteninformationen preisgibt? Es gilt die eiserne Regel: Zahlungs- und Bankinformationen nie an einem anderen Ort eintippen, als auf der gesicherten Website der Bank oder des Online-Shops.

Mittels des sogenannten Phishings haben schon manche Betrüger nichts ahnende Bankkunden dazu gebracht, vertrau-

Begriffe, die Sie kennen müssen

- **Firewall:** Eine Firewall ist eine Schranke zwischen Computer und Internet mit der Aufgabe, nur bekannte, ungefährliche Inhalte auf den Computer zu lassen. Sie bietet Schutz vor Bedrohungen. Eine Firewall kann eine Software sein oder auch Hardware, also ein zusätzliches Gerät.
- **Trojaner:** Als Trojaner oder Trojanisches Pferd werden kleine Programme bezeichnet, die meist per E-Mail als harmlose Anlagen getarnt auf den Computer gelangen und dort Schaden anrichten können. Der Name lehnt an die Sage um Troja an, wonach griechische Soldaten versteckt in einem hölzernen Pferd in die gesicherte Stadt Troja gelangten.
- **Malware:** Malware ist ein Überbegriff für alle unerwünschten oder schädlichen Programme und Codes, die den Computer bedrohen. Dazu gehören etwa Viren, Würmer, Trojaner und mehr.

Gut zu wissen

- **Hier finden Sie Tipps und Infos zu IT-Sicherheit:** www.swisssecurityday.ch; www.infosurance.ch; www.goout.ch
- **Hier können Sie Passwörter auf ihre Sicherheit überprüfen:** https://passwortcheck.datenschutz.ch
- **Kurse in IT-Sicherheit bei der Klubschule Migros:** www.klubschule.ch

Unsichtbar im Hintergrund und ständig auf der Lauer: Internet-Betrüger erfinden laufend neue Tricks.

Handy-Viren sind halb so schlimm

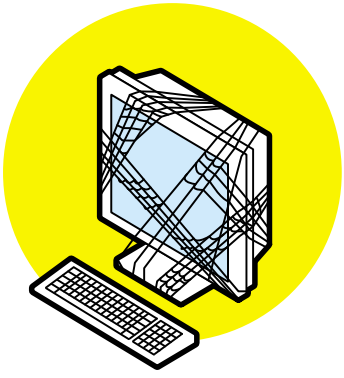
Angst vor Handy-Viren braucht man zumindest heute noch keine zu haben. Zwar existieren **Schädlinge für gewisse Handytypen,** doch sind grosse Angriffswellen wie im Internet auf den Mobiltelefonen bisher ausgeblieben.

Betroffen von Mobiltelefon-Schädlingen können theoretisch so genannte **Smartphones** sein, die über ein Betriebssystem verfügen, für das Zusatzsoftwares – und somit auch Viren – entwickelt werden können. Seit einiger Zeit bieten die Hersteller von Sicherheitssoftware auch Programme zur Abwehr von Handy-Viren an. Malware kann theoretisch über das mobile Internet oder über den PC, an dem das Handy angeschlossen wird, eingefangen werden. Ein anderer Weg sind Bluetooth- und WLAN-Verbindungen. Der Handy-Wurm «Cabir» sorgte als Handy-Ungeziefer, das sich via Bluetooth von einem Handy auf ein anderes kopieren kann, vor ein paar Jahren für Schlagzeilen. Obwohl er keine weite Verbreitung fand und keinen grossen Schaden anrichtete, möchte man solches Ungeziefer trotzdem nicht auf seinem Mobiltelefon wissen. Deshalb: Erhält man Daten via Bluetooth, sollte man diese nur akzeptieren, wenn der Absender und der Inhalt bekannt sind.

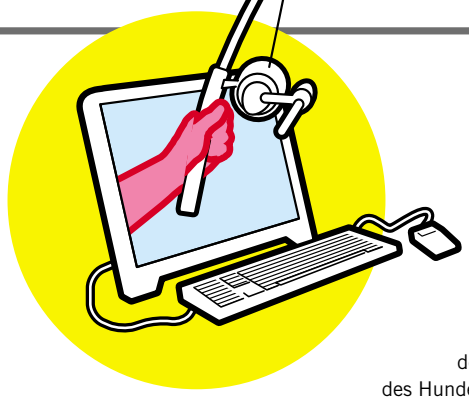
Und vor allem: Bei Nichtgebrauch sollte man die **Bluetooth- und WLAN-Funktion abschalten.** Das ist nicht nur sicherer, sondern schont zudem den Akku, denn aktiviertes Bluetooth braucht ständig Strom.

Die besten Tipps für sicheres Surfen

1. Sicherheitssoftwares benutzen
Jeder PC, der mit dem Internet verbunden ist, sollte über eine aktuelle Version eines Antiviren-Programms und einer Firewall verfügen. Bei diesen sollte die automatische Aktualisierungsfunktion aktiviert sein, damit Updates des Herstellers regelmässig installiert werden können. So ist die Chance grösser, dass neu in Umlauf gebrachte Schädlinge erkannt werden.



2. Keine dubiosen Links öffnen
Auch ohne angehängte Datei kann ein Mail eines unbekannten Absenders gefährlich sein. Beispielsweise dann, wenn es einen Link beinhaltet mit der Bitte, diesen zu öffnen. Dahinter kann sich ein ausführbares Programm verstecken, das sich durch Anklicken auf dem PC einnistet. Deshalb: Mauszeiger weg von solchen Links.



3. Sichere Passwörter verwenden
Ein sicheres Passwort sollte aus zehn oder besser mehr Zeichen bestehen und neben Buchstaben auch Zahlen und Sonderzeichen beinhalten. Es sollten keine Wörter verwendet werden, die man im Lexikon findet, da ein Computer innert Sekunden sämtliche bekannten Wörter als Passwort ausprobieren kann. Benützen Sie keine persönlichen Angaben wie den Namen des Partners, des Hundes oder Ähnliches.

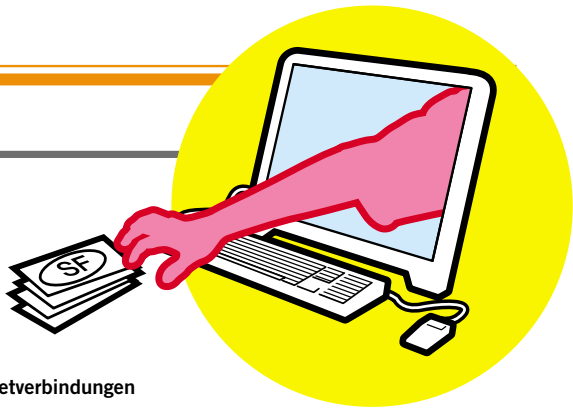
4. Regelmässige Datensicherungen vornehmen
Es kann vorkommen, dass der Computer abstürzt, ein virtueller Schädling Daten vernichtet oder der Datenzugriff aus anderen Gründen

Fortsetzung auf Seite 78

liche Informationen bekannt zu geben. Oft läuft dies so ab: Die Betrüger senden ein Mail, das so aussieht, als käme es direkt von der Bank. Im Mail oder auf einer gefälschten Website wird der Bankkunde «aus Sicherheitsgründen» gebeten, die geheimen Daten in ein Formular einzufüllen – und schon landen die Daten in den falschen Händen. Deshalb gilt: Wachsam bleiben, wenn man übers Web mit Finanzdaten zu tun hat. Um die Bank im Internet zu besuchen, sollte nie ein (per Mail zugesandter) Link verwendet werden. Besser, man tippt die Webadresse von Hand im Browser ein. Text Felix Raymann, Illustrationen Esjottes von Rotwein/Caepsele

Ist Ihnen Internet- und PC-Sicherheit wichtig? Das Quiz und die Umfrage auf www.migrosmagazin.ch

Die besten Tipps für sicheres Surfen



verhindert wird. Speichert man seine wichtigen Daten regelmässig auf eine CD, eine DVD, ein externes Laufwerk oder einen USB-Stick, ist man vor Datenverlusten weitgehend gefeit.

5. Verdächtige E-Mail-Anhänge nicht öffnen
Auch wenn sie auf den ersten Blick recht harmlos aussehen: E-Mail-Anhänge können Viren, Würmer und andere Schädlinge enthalten, die sich automatisch auf dem PC installieren, sobald man sie öffnet.

Kennt man den Absender nicht, sollte man Anhänge nicht öffnen.

6. Gesicherte Internetverbindungen verwenden
Wenn man in einem Online-Shop einkauft und seine Kreditkartenangaben in ein Online-Formular eintippt, sollte man darauf achten, dass die verwendete Website die Daten verschlüsselt transferiert. Solche Webseiten werden mit dem Adress-Zusatz «https» (statt nur «http») und einem kleinen Schloss-Symbol gekennzeichnet. Erscheint eine Fehlermeldung, die beispielsweise auf ein ungültiges Zertifikat aufmerksam macht, sollte man nicht einfach auf «Weiter» klicken.

7. Updates der verwendeten Programme vornehmen
Nicht nur die Sicherheitsprogramme sollten ständig aktualisiert werden, auch der Browser oder das Betriebssystem sind sicherer, wenn sie auf dem aktuellsten Stand gehalten werden. Dabei muss es sich nicht zwingend um das allerneuste Betriebssystem handeln. Wichtig ist, dass der Hersteller für die verwendete Version regelmässig Updates liefert, in denen auftretende Sicherheitslücken geschlossen werden. Beim Browser sollte man immer die neuste Version verwenden, welche die aktuellen Sicherheitsfunktionen enthält. Die Browser werden üblicherweise kostenlos zur Verfügung gestellt.

Das sagt der Experte

Hacker machen heutzutage mehr Geld als Drogendealer

BILD ANNE MORGENSTERN

Andreas Wisler, IT-Sicherheitsexperte, gibt bei der Klubschule Migros Kurse für IT-Sicherheit

Andreas Wisler, welches sind die grössten Gefahren im Internet?
Das organisierte Verbrechen findet auch im Internet statt. Studien besagen, dass heute mehr Geld mit Hacking gemacht wird als mit Drogen. Firmen werden gezielt angegriffen, wobei Heimanwender oft ahnungslos als Mittel zum Zweck missbraucht werden.

Wie ist es möglich, dass ein normaler PC-Benutzer ohne sein Wissen bei kriminellen Handlungen mithilft?
Den Hackern gelingt es, Computer, die am Internet angeschlossen sind, in ein sogenanntes Botnet zu integrieren. So können über diese Computer aus der Ferne beispielsweise Angriffe gestartet, Daten ausgetauscht und Spam- oder Phishing-Mails versendet werden.

Wie wird ein PC Teil eines Botnets?
Durch eine Sicherheitslücke, beispielsweise nicht aktualisierte Firewall-Software. Oder über manipulierte Webseiten, die man besucht. Bei einer Zählung durch Google wurden kürzlich eine halbe Million Websites gefunden, die versuchen, beim Besucher eine schädliche Software zu installieren.

Und wie merkt man, ob man Teil eines solchen Botnets ist?
Das ist das Problem: Man kann nicht erkennen, ob der eigene PC ein sogenannter Zombie-PC ist und von anderen kontrolliert wird. Auch das Antivirenprogramm bemerkt dies nicht.

Sind davon nur Windows-PCs betroffen oder auch Macs?
Ein Mac ist tatsächlich weit weniger gefährdet als ein Windows-PC, doch gibt es mittlerweile auch Schädlinge für Apple-Computer. Auch die Mac-Besitzer sollten sich vorsehen und sich nicht unbedacht im Internet bewegen.

Ist das neue Windows Vista sicherer als XP?
Man fährt wahrscheinlich besser mit Vista. Beispielsweise lässt sich die in Windows XP integrierte Firewall von einem Hacker problemlos abschalten.

Setzt man sich auch einer Gefahr aus, wenn man unterwegs mit seinem Laptop über WLAN im Internet surft?
Theoretisch schon. Es können zum Beispiel Passwörter abgefangen werden. Die Gefahr bei WLAN besteht aber auch zu Hause, wenn man den WLAN-Router nicht absichert. Dann können Nachbarn oder jemand in einem Auto vor dem Haus über den betreffenden Internetanschluss illegale Handlungen begehen. Am sichersten ist die sogenannte WPA-Verschlüsselung, die beim WLAN-Router einfach aktiviert werden kann.

Hatten Sie selbst schon einmal einen Virus auf Ihrem Computer?
Nein, zum Glück noch nie. Mit einem aktuellen System und Vorsicht beim Surfen konnte ich das bisher verhindern.