Das Netz
Digicomp

Viren, Spam & Co

Viren, Trojaner, fiese Hacker, Datenklau, Spam-E-Mails:

Der Computer bietet ausreichend Schlupflöcher für digitale Schädlinge aller Art.

Die Missbrauchsmöglichkeiten sind vielfältig geworden – immer wieder tauchen neue Sicherheitslücken oder Schadprogramme auf.

Erfahren Sie hier, welche Risiken es gibt und wie Sie sich davor schützen können.

Wie kann ich meinen Computer schützen?

Software-Updates

Halten Sie ihr Betriebssystem und ihre installierten Programme immer auf dem neusten Stand.

Aktuelle Betriebssysteme wie Windows und MacOS spielen bereits die neuesten Updates automatisch ein.

Wie kann ich meinen Computer schützen?

Firewall

Sie verhindert gefährliche Zugriffe aus dem Internet auf Ihren Computer.

Moderne Betriebssysteme haben von Haus aus eine Firewall eingebaut, die möglicherweise aber noch aktiviert werden muss.

Anti-Viren-Programm

Moderne Betriebssysteme haben bereits ein Anti-Viren-Programm integriert.

Sie benötigen somit keine weiteren Zusatzprogramme. Achten Sie jedoch darauf, dass diese regelmäßig aktualisiert werden.

Woher bekomme ich gute Anti-Viren-Programme?

Moderne Betriebssysteme haben bereits Anti-Viren-Programme installiert.

Sie benötigen somit eigentlich keine zusätzlichen Programme mehr.

Wenn Sie trotzdem ein zusätzliches Anti-Viren-Programm installieren wollen, finden Sie eine Übersicht empfehlenswerter Anti-Viren-Programme, die Sie entweder als kostenlose Vollversion oder als zeitbegrenzte Demoversion herunterladen können, auf heise online.

Woher bekomme ich gute Anti-Viren-Programme?

Tipp

Vergessen Sie bei zeitlich begrenzten Demoversionen nach Ablauf der Testfrist nicht, die Vollversion zu erwerben und zu installieren.

Besser noch:
Installieren Sie statt der Demoversion gleich ein kostenloses Anti-Viren-Produkt – diese bieten den gleichen Schutz wie kostenpflichtige Varianten!

Brauche ich ein Anti-Viren-Programm für mein Smartphone?

Nein, für Smartphones mit dem aktuellsten Betriebssystem benötigen Sie kein eigenes Anti-Viren-Programm.

Wichtig ist jedoch immer die neueste Version des Betriebssystems aufzuspielen und die installierten Apps regelmäßig upzudaten.

Als Nutzer/in eines Android-Smartphones sind Sie prinzipiell gut geschützt, wenn Sie nur Apps aus dem offiziellen App-Shop von Google (Playstore) herunterladen. Denn so gut wie alle Android-Schädlinge fängt man sich bei unseriösen Drittanbietern an.

Brauche ich ein Anti-Viren-Programm für mein Smartphone?

Erlauben Sie Ihrem Android-Smartphone daher sicherheitshalber nicht, Apps von Drittanbietern zu installieren. Diese Option ist standardmäßig deaktiviert, kann aber in den Einstellungen geändert werden.

In Apples iOS können prinzipiell nur verifizierte Apps über den offiziellen App-Store heruntergeladen werden.

Das Risiko, das iPhone mit Malware zu infizieren, ist somit generell geringer.

Brauche ich ein Anti-Viren-Programm für mein Smartphone?

Achten Sie bei der Verbindung zu öffentlichen bzw. ungesicherten WLAN-Netzwerken, keine sensiblen Daten über das Smartphone zu senden.

Verzichten Sie hier vor allem auf Online-Banking.

Überprüfen Sie regelmäßig Ihre installierten Apps und entfernen Sie nicht mehr benötigte Anwendungen wieder vom Gerät.

Wie verschlüssele ich mein WLAN-Netzwerk?

Unverschlüsselt über ein WLAN-Netzwerk übertragene Daten sind grundsätzlich von jeder Person in der Reichweite Ihres Funknetzwerks lesbar.

So können z. B. Passwörter, Kreditkartendaten oder ähnlich sensible Informationen in die Hände von Betrügern gelangen.

Besonders problematisch ist es, wenn der unbekannte Mitbenutzer über Ihre Verbindung illegale Inhalte abruft – dann müssen Sie nämlich die rechtlichen Konsequenzen tragen! Davon abgesehen können solche „Schwarznutzer“ praktisch nicht ausfindig gemacht werden.

Wie verschlüssele ich mein WLAN-Netzwerk?

Wenn Sie heute einen neuen Internetzugang bekommen und ihr Modem anschließen, wir dieses bereits automatisch ein verschlüsseltes WLAN-Netzwerk aufbauen.

Die Zugangsdaten finden Sie in der Regel bei ihrem neuen Vertrag bzw. der Anleitung zu Ersteinrichtung ihres Zugangs.

Wichtig!!!

Ändern Sie dieses Standard-Passwort nachdem eine Verbindung hergestellt wurde. So können Sie sicherstellen, dass nur Sie Zugang haben!

Wie kann ich den Browser sicher einstellen?

Moderne Internetbrowser sind bereits mit einer Reihe an Sicherheitsmechanismen ausgestattet, welche auch von Haus aus aktiviert sind.

Sie müssen also keine weiteren Einstellungen mehr vornehmen. Wenn Sie zusätzliche Plug-ins installieren ist es wichtig, darauf zu achten, dass diese nur aus offiziellen Quellen stammen.

Lesen Sie auch die entsprechenden Bewertungen in den Foren durch um sich zu vergewissern, dass keine Sicherheitseinstellungen des Browsers umgangen werden.

Was ist „Spam“?

Spam ist für viele Internetnutzer/innen eine echte Plage.

Fast jede E-Mail-Adresse, die länger als ein paar Monate verwendet wird, erhält täglich Dutzende unerwünschte Massenzusendungen, in denen von Potenzmitteln bis zu Gartenliegen so ziemlich alles beworben wird.

Auch die Zusendung von Schadprogrammen sowie Phishing-E-Mails und andere E-Mail-Betrügereien sind ein Problem.

Was ist „Spam“?

Spam ist in Österreich nach § 107 Telekommunikationsgesetz verboten.

Eine Zusendung von Werbe-E-Mails ist ohne vorherige Einwilligung des Adressaten nicht erlaubt, ebenso Massensendungen (auch ohne Werbung) an mehr als 50 Personen, deren Einwilligung nicht vorliegt.

Dasselbe gilt übrigens für SMS.

Was ist „Spam“?

Auch wenn die österreichische Rechtslage eindeutig ist, so ist das Spam-Problem damit keineswegs gelöst.

Die Spammer verwenden ausgeklügelte Methoden, sodass sich sowohl die Abwehr der unerwünschten E-Mails wie auch die gesetzliche Verfolgung schwierig gestalten.

Experten gehen davon aus, dass rund 70% der weltweit verschickten E-Mails Spam-Nachrichten sind. Die gute Nachricht allerdings: Tendenz sinkend!

Erlaubt ist eine Zusendung von Werbe-E-Mails nur in folgenden Fällen

- Wenn der Adressat vorher zustimmt, wobei jede Form der Zustimmung möglich ist: schriftlich oder mündlich, ausdrücklich oder stillschweigend, sogar durch Akzeptieren von AGB (z. B. bei einer Online-Bestellung).

Erlaubt ist eine Zusendung von Werbe-E-Mails nur in folgenden Fällen

- Wenn der Versender die Kontaktinformation im Zusammenhang mit einem Verkauf oder einer Dienstleistung erhalten hat und die Werbung ähnliche Produkte betrifft.

  Dabei muss der Empfänger über die Möglichkeit der Ablehnung aufgeklärt werden.

  Die Nutzung der Kontaktdaten für Werbung ist außerdem nur zulässig, wenn der Adressat nicht in die ECG-Liste eingetragen ist. (Quelle: Franz Schmidbauer, Internet4Jurists)

Was kann ich gegen Spam tun?

Gehen Sie sorgsam mit Ihrer E-Mail-Adresse um und geben Sie sie nur an Personen weiter, denen Sie vertrauen. Geben Sie Ihre E-Mail-Adresse nicht leichtfertig überall im Internet bekannt.

Verwenden Sie mindestens zwei E-Mail-Adressen: eine, um mit Familie, Freunden und beruflich zu kommunizieren, und eine andere, um sich damit für Online-Services, in Sozialen Netzwerken oder Foren zu registrieren, an Gewinnspielen teilzunehmen etc.

Die Zweitadresse können Sie z. B. bei einem der großen Webmail-Anbieter (z. B. Yahoo!, Hotmail oder Google Mail) einrichten.

Was kann ich gegen Spam tun?

Antworten Sie niemals auf Spam-E-Mails, auch nicht, um sich zu beschweren. Denn damit bestätigen Sie dem Spammer nur, dass Ihre E-Mail-Adresse aktiv ist. Oft bekommt man dann noch mehr Spam. Auch beim Öffnen können bereits versteckte Programme aktiviert werden, die Ihre E-Mail-Adresse verifizieren – öffnen Sie Spam-E-Mails daher besser nicht und klicken Sie in keinem Fall auf irgendwelche Links in der E-Mail.

Verwenden Sie den Spamfilter Ihres E-Mail-Programmes und Ihres E-Mail-Anbieters.

Was kann ich gegen Spam tun?

Öffnen Sie keine mitgeschickten Dateianhänge! Diese könnten Schadprogramme enthalten, die beim Öffnen der Datei aktiviert werden.

Vermeiden Sie, dass Ihre E-Mail-Adresse öffentlich im Internet aufscheint. „Tarnen“ Sie Ihre E-Mail-Adresse, damit diese für Programme, die das Web durchsuchen, nicht erkennbar ist. Verwenden Sie z. B. eine Grafik mit Ihrer E-Mail-Adresse anstelle eines Texts oder schreiben Sie „max dot mustermann at xy dot at” anstelle von „max.mustermann@xy.at”. Lassen Sie sich von Ihrem Website-Administrator beraten!

Wie nutze ich Spamfilter richtig?

Alle modernen E-Mail-Programme bieten sehr gute, selbstlernende Spamfilter an.

Die meisten funktionieren so, dass als Spam identifizierte E-Mails automatisch in einen eigenen „Junk“- oder „Spam“-Ordner verschoben werden.

Dort können Sie die Nachrichten nochmals kontrollieren, ob nicht irrtümlicherweise auch erwünschte E-Mails aussortiert wurden.

Das kann passieren, wenn der Filter besonders streng eingestellt ist.

Wie nutze ich Spamfilter richtig?

Hinweis:

Wichtig ist, dass Sie nach Installation eines neuen E-Mail-Programms ein paar Wochen lang den Spamfilter „anlernen“, damit sich dieser Ihren Bedürfnissen anpassen kann.

Andernfalls wird er nicht zu Ihrer Zufriedenheit funktionieren. Das Anlernen funktioniert!

HOAX – was ist das?

Ein Hoax ist eine Falschnachricht im Internet, die absichtlich als solche in Umlauf gebracht wurde.

Angefangen bei harmlosen Scherzmeldungen und Kettenbriefen bis hin zu weniger witzigen „Horrormeldungen“ oder gefakten Fotos (z. B. von schwer misshandelten Tieren oder Kindern).

Kennen Sie vielleicht ...?
Achtung! Hiermit widerspreche ich den neuen Facebook-Nutzungsrichtlinien …

HOAX – was ist das?

Oder:
Achtung! Ein Virus breitet sich auf Facebook aus. Nehmt auf keinen Fall die Freundschaftsanfrage von XX an! …

So ähnlich – und noch in vielen anderen Varianten – kommen Hoaxes daher. Kaum ein Thema, das von den „kreativen Urheber/innen“ nicht ausgelassen wird. Meistens werden die Falschmeldungen auf Facebook oder auf WhatsApp verbreitet. Früher wurden auch viele Hoaxes via E-Mail versandt.

Der einzige Zweck eines Hoaxes ist es, möglichst viele Leute zu narren.

HOAX – was ist das?

Auch Kettenbriefe sind oft Hoaxes. Sofern keine betrügerischen Machenschaften dahinter stecken, sondern nur unverfängliche Zahlenspielchen oder Liebesorakel, ist das nicht weiter tragisch. Mitunter gibt es aber auch Kettenbriefe, die sehr bedrohlich formuliert sind und den Empfänger/innen Angst machen.

Ein Beispiel: In einer Audionachricht auf WhatsApp wird dazu aufgefordert, die Nachricht an Freund/innen zu verbreiten oder der/die Zuhörer/in stirbt. Diese sind vor allem für die Kleinsten angsteinflößend. Nehmen Sie diese Angst ernst und reden Sie mit ihren Kindern darüber.

HOAX – was ist das?

Doch wie erkennen Sie einen Hoax?

Gute Tipps und Tricks dazu gibt es von der TU Berlin. Ist man dennoch unsicher, ob eine Nachricht echt ist oder nicht, hilft es auch, Auszüge aus der Nachricht in Suchmaschinen einzugeben – meist lässt sich ein Schwindel so sehr schnell entlarven.

HOAX – was ist das?

Sind Hoaxes gefährlich?

Tatsächlich sind die meisten Hoaxes harmlos und der Aspekt des Scherzes steht im Vordergrund, wenngleich die Abgrenzung von betrügerischen Phishing-Mails oder Scams nicht immer ganz einfach ist. Unlustig wird es auch dann, wenn wahllos Fotos von Internetnutzer/innen mit Zusätzen wie „Gesuchter Kinderschänder“ o.ä. im Netz verbreitet werden. Und auch die Zusendung von Schadprogrammen in sog. „Malware-Mails“ ist ein Problem.
Deshalb: Nachrichten löschen bzw. ignorieren, keine Anhänge öffnen und vor allem nicht weiterverbreiten!

Datenschutz

Sich völlig anonym durch den Alltag zu bewegen, ist heutzutage unmöglich.

Auch im Internet gilt: Einen hundertprozentigen Datenschutz gibt es nicht! Jeder Einstieg ins Web hinterlässt – beabsichtigt oder unbeabsichtigt – Spuren. Leider gibt es viele Versuche, diese Spuren zu lesen und auch illegal zu nutzen.

Für einen großen Teil der verfügbaren Daten über uns sind wir aber selbst verantwortlich, weil wir oft sehr leichtfertig mit Angaben zur eigenen Person umgehen.