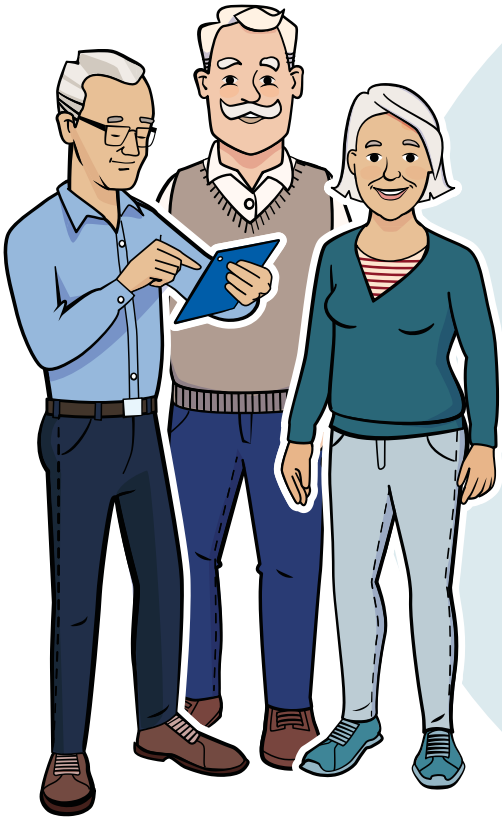
Kapitel 3
Sicherheit geht vor



Endlich!
Der Schalttermin für den
Internet-Zugang ist da! Herr
Meister hilft Frau und Herrn Neumann
beim Einrichten des Routers und des WLANs.

„Bevor ihr aber ins Netz geht, möchte ich euch noch ein paar Tipps geben. Wie im realen Leben gibt es auch im Internet ein gewisses Maß an Kriminalität. Und wenn ihr mit dem Computer, Tablet oder Smartphone im Internet stöbert, können das – zumindest technisch – andere auch bei euch. Mit Schutzprogrammen werden die Geräte vor sogenannten Viren, Trojanern, Bot-Netzen und Spam abgeschirmt. Das Gute ist, dass heute schon umfangreiche Sicherungsmechanismen integriert sind. Wichtig ist aber, dass ihr darauf achtet, dass ihr diese Programme auf dem aktuellen Stand haltet. Wer alle Sicherheitsmaßnahmen beachtet und – wie in der realen Welt – mit gesundem Menschenverstand handelt, dem kann im Netz eigentlich nichts passieren.“

Grundsicherung am Computer

Alle Betriebssysteme bieten Ihnen mit ihren *Schutzprogrammen*[48] eine gute Grundsicherung für Ihren Computer (übrigens auch für das Tablet und das Smartphone). Über die Systemsteuerung Ihres Rechners gelangen Sie zum Sicherheitscenter. Dort können Sie die Einstellungen verwalten und automatische Aktualisierungen festlegen. Zur wichtigen Grundausstattung eines Rechners gehört die *Firewall*[49], die stets eingeschaltet sein sollte und die Ihren Datenverkehr überwacht. Sie arbeitet wie ein Türsteher an Ihrer

48 Schutzprogramme sind Programme, die die Betriebsbereitschaft eines Computers sicherstellen.

49 Firewall, gesprochen: Feierwol, engl., Brand(schutz)mauer.

Haustür und verhindert im übertragenen Sinn, dass ungebetene Gäste in Ihr Haus eindringen, sich umschauen, Sachen mitnehmen oder mutwillig zerstören. Kostenlose Programme zusätzlich zu der mit Ihrem Betriebssystem ausgelieferten Firewall sind z. B. Comodo Internet Security, ZoneAlarm Free oder Free Firewall. Diese Gratisversionen bieten einen grundlegenden Schutz, werben aber in der Regel auch für weitere kostenpflichtige Varianten.

Schadprogramme

Die Firewall schützt vor *Spyware*[50], die ausspioniert, welche Seiten Sie im Internet besuchen und welche Daten Sie dort angeben. Wertvolle Informationen werden auch von Anbietern legaler Software gesammelt, sofern Sie bei der Einrichtung nicht der Übermittlung persönlicher Daten widersprochen haben. Diese sind für die Werbewirtschaft von hohem Wert. So kann es Ihnen passieren, dass Sie plötzlich während des Surfens oder über E-Mail zielgerichtete Werbeangebote erhalten.

Auf dem ersten Platz der potenziellen Angreifer stehen **Computerviren und Würmer**. Beides sind Programme, die die Software und das Betriebssystem manipulieren und unbrauchbar machen können. Würmer haben die unangenehme Eigenschaft, die Infrastruktur Ihres Computers zu nutzen, um sich selbst zu vervielfältigen, nachdem sie – von Ihnen ungewünscht und unbemerkt – installiert wurden. Beispielsweise lesen Würmer, die in Ihrem E-Mail-Programm gespeicherten Adressen aus, um die Empfänger anzuschreiben und sich so weiter zu verbreiten.

Trojaner[51] tarnen sich besonders perfide: Korrekterweise eigentlich als „Trojanische Pferde" bezeichnet, verstecken sie sich in nützlichen Programmen, installieren aber oft im Hintergrund Software, die es nicht immer gut mit Ihrem Rechner meint. Das können z. B. Spionageprogramme sein, die Ihre Tastatureingaben aufzeichnen oder Ihren Computer unbemerkt fernsteuern.

Bot-Netz[52] ist eine Gruppe automatisierter Schadprogramme. Hier werden mehrere Tausend Computer oder noch mehr zusammengeschlossen und von einem *Server*[53] missbräuchlich ferngesteuert. Bot-Netze werden für den Versand von Massen-E-Mails, für die großflächige Verbreitung von Schadprogrammen oder für weitere *Hacker*[54]-Angriffe ausgenutzt.

50 Spyware, gesprochen: Speiwehr, engl. Kunstform aus spy, Spion, und Software.

51 Trojaner, gesprochen: Trojaner.

52 Bot-Netz, gesprochen wie geschrieben.

53 Server, gesprochen: Sörwer, engl., Diener. Hier: Bezeichnung für einen Netzwerkrechner.

54 Hacker, gesprochen: Häcker, von engl. to hack, hacken. Alltagssprachlich für Personen, die widerrechtlich in Computersysteme eindringen.

Spam-Mails

Als Spam oder *Junk-Mails*[55] werden unerwünschte E-Mail-Nachrichten benannt, die über das Internet übermittelt werden.

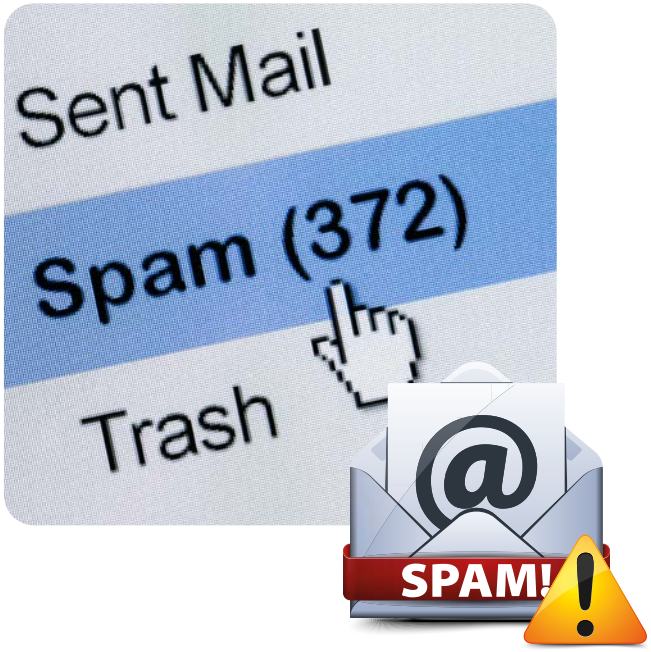
Daran können Sie Spam-Mails erkennen

- unbekannte oder merkwürdige Absender-Adressen
- fehlende persönliche Anrede
- reißerische Betreffs
- komischer Inhalt, wie z. B. eine dringende Aufforderung, man solle eine Datei öffnen oder Daten eingeben
- *Links*[56] oder eingefügte Formulare
- seltsame Anhänge
- Rechtschreib- und Grammatikfehler und ungewöhnliche Formulierungen
- fremdsprachige E-Mails

Sollten Sie sich unsicher sein, hilft Ihnen oft auch eine Internet-Recherche.

Der richtige Umgang mit Spam-Mails

- Niemals auf Spam antworten oder weiterleiten.
- Niemals auf Anhänge oder Links in den Spam-Mails klicken.



Um Spam-Mails vorzubeugen...

- installieren Sie ein Spam-Filterprogramm.
- verwenden Sie immer die aktuellste Version des Browsers.
- versuchen Sie Ihre E-Mail-Adresse. so geheim wie möglich zu halten.

Und, lassen Sie sich nicht ärgern! Markieren Sie die unerwünschte Mail und verschieben Sie sie einfach in Ihren Spam- oder Junk-Ordner. Diesen Ordner sollten Sie aber nicht sofort leeren, sonst landet eine ähnliche Mail des gleichen Absenders beim nächsten Mal wieder in Ihrem Posteingang.

55 Spam, gesprochen: Spemm, engl., Kunstwort. Junk, gesprochen: Dschank, engl., Abfall, Plunder.

56 Link, engl., Verbindung. Wenn Sie auf Internet-Seiten farbig hervorgehobene und unterstrichene Stellen anklicken, öffnet sich ein neues Bildschirmfenster mit neuem Inhalt. Sie werden „verlinkt“.

Schutzprogramme

Gegen all diese Schadprogramme können Sie sich wirkungsvoll absichern, z. B. mit kostenpflichtigen Programmen wie Kaspersky Internet Security, Bitdefender Internet Security, ESET Internet Security, G Data Internet Security sowie Avira Internet Security. Auch in dieser Sparte gibt es kostenfreie Programme, dazu zählen Avira Free Antivirus, Avast Free Antivirus oder AVG Antivirus Free. Neben vielen Computerzeitschriften prüft auch die Stiftung Warentest (www.test.de) regelmäßig Aktualität und Leistungsumfang von Schutzprogrammen.

Nachteil von kostenfreien Programmen

Viele Software-Firmen bieten Programme mit einem verminderten Leistungsumfang kostenlos an. Auf Ihrem Rechner eingesetzt, entfalten die Programme dann ihre Werbewirkung: Sie preisen Ihnen durch automatische Reklameeinblendungen umfangreichere, dafür aber kostenpflichtige Programmteile an oder werben für ein weiteres Partnerprogramm. Lassen Sie sich nicht nerven und gehen Sie nicht auf jede Kaufempfehlung der Firmen ein!

TIPP

Werbung blocken

Werbung blocken

Ein *Adblocker*[57] blockiert Werbung auf Internet-Seiten. Mit einem solchen Filterprogramm haben Sie die Möglichkeit, einen Großteil der Werbebanner auszublenden und unsichtbar zu machen. Ein weiterer Vorteil ist, dass sich dadurch Internet-Seiten schneller öffnen. Viele Unternehmen sehen diese Programme kritisch, da sie ihre Webseiten über Werbung finanzieren und irgendwann keine kostenlosen Angebote mehr machen können. So kann man z. B. manchmal Zeitungsartikel im Internet nicht lesen, wenn man einen Adblocker eingeschaltet hat.

57 *Adblocker, gesprochen: Äddblocker, Kurzform für Advertisement Blocking, engl., Anzeigenunterdrückung.*

Updates *58*

Bei allen (Schutz-)Programmen ist besonders wichtig, dass Sie sie immer auf dem neuesten Stand halten. Da die Hersteller bemüht sind, bekannt gewordene Sicherheitslücken sofort zu schließen, bieten sie regelmäßig kostenlose Updates der Programme an.

Weitere Hinweise, wie man seinen Computer gut schützt, zeigt das Bundesamt für Sicherheit in der Informationstechnik auf seiner Internet-Seite: www.bsi-fuer-buerger.de.

Abo-Fallen

Der Bundesverband Informationswirtschaft, Telekommunikation und neue Medien (www.bitkom.de) gibt Ratschläge, wie Sie sich gegen Abo-Fallen schützen können. Dazu hier die folgenden drei Tipps:

1. Geben Sie für angeblich kostenlose Internet-Inhalte oder Dienstleistungen keine persönlichen Informationen weiter. Programme können Sie ohne Angabe Ihrer Telefonnummer, Adresse oder gar Bankverbindung herunterladen.

2. Wenn Sie mit Geldforderungen konfrontiert werden, lassen Sie sich nachweisen, wie der angebliche Vertrag zustande kam.

3. Bleiben Sie unaufgeregt, wenn Ihnen mit rechtlichen Schritten und Inkasso gedroht wird; meist handelt es sich um leere Drohungen. Lassen Sie jedoch keine juristischen Fristen verstreichen. Widersprechen Sie dem vermeintlichen Vertrag und nutzen Sie die Musterbriefe, die Ihnen die Verbraucherzentralen und die Stiftung Warentest bereitstellen.

TIPP

Datenschutz

- Laden Sie keine Dateien von unbekannten oder zweifelhaften Internet-Seiten herunter.
- Installieren Sie nur seriöse Software.
- Öffnen Sie keine E-Mails und E-Mail-Anhänge von Ihnen unbekannten Absendern.
- Gehen Sie mit Bedacht vor, wie Sie es auch im realen Leben tun.

Datenschutz

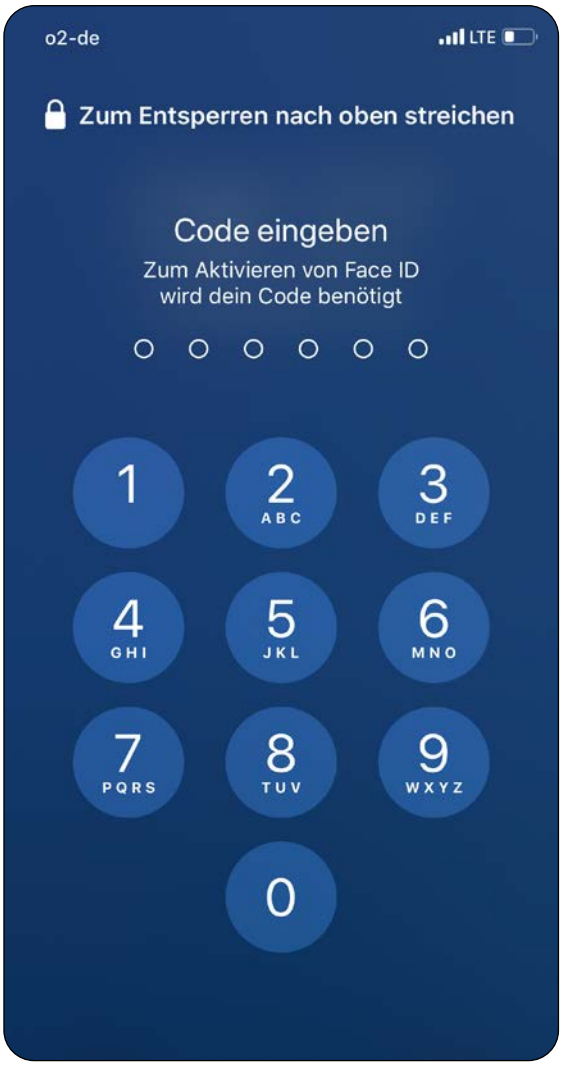
58 Updates, gesprochen: Appdäits, engl., Aktualisierungen.

Sicherheit auf dem Smartphone und Tablet

Beide Geräte sind recht gut gegen Angriffe geschützt. Um ganz sicherzugehen, sollten Sie aber folgende Sicherheitshinweise beachten:

- Machen Sie regelmäßig *Backups*[59].
- Installieren Sie Updates, sobald sie Ihnen angeboten werden.
- Verriegeln Sie Ihre Geräte mit einem *Code*[60].
- Verschlüsseln Sie Ihre Daten. Sie finden diese Möglichkeit in den Einstellungen unter Sicherheit.
- Installieren Sie nur Apps aus vertrauenswürdigen Quellen, am besten aus dem App Store Ihres Anbieters und nicht unüberlegt.
- Seien Sie bei unbekannten Absendern und außergewöhnlichen Anfragen besonders skeptisch.
- Seien Sie vorsichtig in fremden WLANs.
- Wenn Sie Ortungssysteme benutzen, machen Sie sich sichtbar.
- Achten Sie darauf, dass Ihre Geräte nicht leicht entwendet werden können. Im Fall des Falles: Lassen Sie Ihre SIM-Karte umgehend sperren.
- Setzen Sie ein gebrauchtes Gerät vor dem ersten Einsatz auf Werkseinstellung zurück.

Natürlich können Sie Ihr Tablet und Smartphone durch zusätzliche Software weiter absichern. Sie erhalten Programme als App in Ihrem App Store.



Bildschirm mit Code-Eingabe

Für die verschiedenen Betriebssysteme werden unterschiedliche Programme angeboten. Bitte recherchieren Sie diese passgenau für Ihr Betriebssystem. Testergebnisse und Kaufberatungen finden Sie auf den Internet-Seiten der Stiftung Warentest (www.test.de) und von Computerzeitschriften wie z. B. www.chip.de, www.computerbild.de, www.heise.de/ct und www.pcwelt.de.

59 *Backup, gesprochen: Bäckab, engl,. Sicherung.*

60 *Code, gesprochen: Kod.*