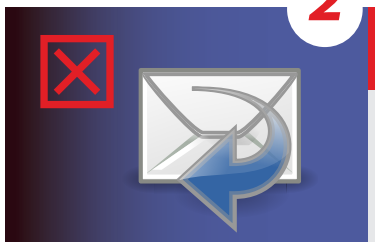
20 Sicherheitshinweise von Avira

1-5

1 Seien Sie vorsichtig bei Emails mit Anlagen.

Es kann riskant sein, Emails zu öffnen, die unbekannte Dateien enthalten, da diese Dokumente oder Fotos oft Angriffe ausführen. Sie sollten daher jede verdächtige Email vorab scannen.



2 Beantworten Sie keine unerwünschten Emails.

Wenn Sie eine automatische, nicht abonnierte Email erhalten, sollten Sie diese nicht beantworten oder sich von dem Abo abmelden. Sonst weiß der Spammer, dass Sie seine Email geöffnet haben, was Sie zu einem leichten Angriffsziel macht.

3 Kaufen Sie nie etwas aus Spam-Emails.

Die Spam-Angebote sind oft zu gut, um wahr zu sein! Vermeiden Sie den Kauf von Produkten oder Services aus fragwürdigen Emails.

4 Klicken Sie nicht auf Email-Links, die fragwürdige Handlungen verlangen.

Ganz gleich, wie dringend die Nachricht erscheint oder wie unglaublich das Angebot (das natürlich in der nächsten Minute verfällt) wirkt, klicken Sie auf keinen Link und geben Sie keine Informationen weiter. Vernichten Sie die Email.

5 Ihre Bank wird niemals persönliche Informationen per Email verlangen.

Sollten Sie jemals eine Email von Ihrer Bank erhalten, in der Ihre persönlichen Informationen verlangt werden oder von Ihnen bestätigt werden sollen, antworten Sie nicht! Eine Bank wird derartige Informationen niemals per Email abfragen.

6-10

6

Antworten Sie auf keine Email, die vertrauliche oder persönliche Informationen verlangt.

Ganz gleich, was Ihnen jemand für Ihre persönlichen Informationen verspricht, antworten Sie nicht! Die Einsatzmöglichkeiten dieser Daten könnten sich für Sie als äußerst schädlich erweisen.

7

Benutzen Sie sichere Passwörter.

Generieren Sie komplizierte Passwörter, die nicht leicht zu erraten sind. Tipps für sichere Passwörter finden Sie hier:

http://techblog.avira.com/de/

8

Benutzen Sie verschiedene Passwörter für unterschiedliche Konten.

Je mehr Passwörter Sie haben, desto geringer ist die Chance, dass ein Hacker oder Dieb Zugang zu Ihren Konten erhält.

9

Speichern Sie niemals Ihr Passwort auf einem Computer, der Ihnen nicht gehört.

Viele Websites machen eine erneute Nutzung leichter mit der Option, Ihre Login-Informationen zu speichern. Lehnen Sie diese Option ab, wenn Sie nicht Ihren eigenen Computer oder ein sicheres Gerät benutzen.

10

Installieren Sie nicht jedes angebotene Programm.

Viele Webseiten bieten „kostenlose" Programme zum Download an, die jedoch zum Teil Malware enthalten können. Um sich hiervor zu schützen, achten Sie darauf, dass Ihnen vor dem Herunterladen alle Details über das Produkt oder die Firma bekannt sind.

11-15

11 Benutzen Sie einen Virenschutz!

Machen Sie es den Cyberkriminellen nicht leicht. Für alle Plattformen gibt es kostenfreie und kostenpflichtige Virenschutzlösungen.

http://www.avira.com/de/for-home

12 Stecken Sie nicht jedes beliebige USB-Gerät an.

Viele USB-Geräte (wie Memorysticks, SD-Karten und Festplatten) enthalten Malware, die aktiviert wird, sobald das Gerät mit Ihrem Computer verbunden wird. Vor der Benutzung sollten Sie immer einen Scan des Gerätes durchführen.

13 Sperren Sie Ihren Computer in Ihrer Abwesenheit.

Verlassen Sie niemals Ihren Arbeitsplatz, ohne zuerst Ihren Computer zu sperren. Achten Sie darauf, dass er passwortgeschützt ist, sodass niemand unerlaubt Zugang zu Ihren Dateien erhalten kann.

14 Sperren Sie Ihr Smartphone und aktivieren Sie eine automatische Sperre.

Richten Sie für Ihr Smartphone ein Passwort oder eine Wischbewegung ein und achten Sie darauf, dass es sich nach einer Minute automatisch sperrt. Das erschwert es einem Dieb, Ihre Daten einzusehen.

15 Ein Smartphone ist ein leistungsfähiger Computer – nutzen Sie es mit Bedacht.

Smartphones sind kleinere Computer: Sie verfügen über ähnliche Konnektivität und Kapazitäten wie herkömmliche PCs und speichern ebenso persönliche Daten – und bilden damit auch ein potenzielles Ziel für Angriffe.

16-20

16 In Ihrem sozialen Netzwerk „vermisst“ Sie in Wirklichkeit niemand.

Emails von bekannten oder unbekannten Personen, die behaupten, sie würden Sie online „vermissen“, sind wahrscheinlich nur Spam. Sie wissen was zu tun ist – einfach löschen.

17 Beachten Sie, dass Sie niemals der millionste Besucher sind.

Wenn Sie auf einer Webseite einen Banner sehen, auf dem behauptet wird, Sie seien der millionste Besucher und können einen unglaublichen Preis gewinnen ... nun, dieser Banner ändert sich nie. Und gewinnen werden Sie auch nichts.

18 Veröffentlichen Sie keine unangebrachten Fotos auf Facebook.

Ganz gleich wie klein Ihr Freundeskreis online sein mag, unangemessene Fotos können eventuell mit Personen geteilt werden, die sie nicht sehen sollen. Fotos könnten Ihren Chef, Verwandte und wer weiß wen erreichen.

19 Machen Sie keine Nacktfotos von sich ... selbst wenn Sie gut aussehen.

Sobald diese Fotos Ihren Computer oder Smartphone verlassen, wird es äußerst schwierig, sie vollständig zurückzuerhalten. In Zukunft könnten diese Bilder Sie auf höchst unerwünschte Weise heimsuchen.

20 Das Internet vergisst nichts.

Im Internet gibt es sehr viel Speicherplatz. Es hebt Ihre Dokumente oder Fotos auf und wird Sie daran erinnern, wenn Sie es am wenigsten erwarten. Selbst wenn Sie das Original löschen, besteht die Möglichkeit, dass es bereits irgendwo kopiert und gespeichert wurde.

Avira Operations GmbH & Co. KG
Kaplaneiweg 1 | 88069 Tettnang | Deutschland
Telefon: +49 7542-500 0
www.avira.de