7. *Lassen Sie sich E-Mails immer erst ohne Bilder anzeigen.*

Manche E-Mails enthalten Bilder. Mit den Bildern können Viren transportiert werden. Stellen Sie Ihr E-Mail-Programm so ein, dass alle E-Mails zunächst ohne Bilder angezeigt werden. Prüfen Sie in aller Ruhe, wer Ihnen die Bilder geschickt hat und entscheiden Sie dann, ob Sie dem Absender vertrauen können.

8. *Klicken Sie nicht auf angegebene Links.*

Viele E-Mails enthalten sogenannte „Links". Wenn man auf einen „Link" klickt, wird man automatisch mit einer anderen Internetseite verbunden. Diese Internetseite kann gefälscht sein.

9. *Öffnen Sie nicht jeden Anhang.*

E-Mails können einen „Anhang" haben, eine Datei, die mit der E-Mail verschickt wurde. Wenn Sie eine solche E-Mail erhalten, prüfen Sie auch hier, ob Sie den Absender kennen. Öffnen Sie den Anhang erst, wenn Ihnen klar ist, was darin enthalten sein könnte und warum, denn auch im Anhang können sich Viren verbergen.

10. *Sichern Sie alle wichtigen Daten.*

Um sich vor dem Verlust wichtiger Daten zu schützen (Bilder, Dokumente etc.), sollten Sie Ihre Daten regelmäßig auf einem externen Speichermedium sichern (Daten-Backup).

Externe Speichermedien sind zum Beispiel Festplatten oder USB-Sticks. Sie werden an den Computer angeschlossen und nach der Übertragung Ihrer Daten wieder entfernt.

Sollte Ihr Computer aufgrund von Viren oder Schad-Software nicht mehr einwandfrei funktionieren, können Sie so dennoch auf Ihre wichtigsten Daten zurückgreifen.

Hinweis:

Unsere Tipps erheben keinen Anspruch auf Vollständigkeit.

Es gibt viele weitere Möglichkeiten, sich vor kriminellen Übergriffen im Internet zu schützen.

Informationen hierzu erhalten Sie zum Beispiel unter:

https://www.bsi-fuer-buerger.de

Das ist die Internetseite des **Bundesamtes für Sicherheit in der Informationstechnik**.

Wenn Sie Fragen zu Ihrer Internet-Sicherheit haben, können Sie sich montags bis freitags in der Zeit von 8.00 bis 18.00 Uhr auch telefonisch an das Bundesamt wenden:

Telefonnummer: 0800 274 1000

Ver-netzt!

Das inklusive Projekt „Vernetzt!" zielt darauf ab, vorhandene Barrieren im Zu- und Umgang mit dem Internet abzubauen. Es wird von der Aktion Mensch, dem Diakonischen Werk Schleswig-Holstein und der Diakoniestiftung Schleswig-Holstein gefördert und durch die folgenden **Kooperationspartner** unterstützt:

Business Information Technology

Gruppe Norddeutsche Gesellschaft für Diakonie

Bürger Schule · Offener Kanal Schleswig Holstein · Sender

TOOLIBRI die Kunst der Modularität

Kieler Nachrichten

Senioren-Computer-Club Rendsburg e.V.

[campusciencenomy] wissenschaftszentrumkiel gmbh

Werkstätten Materialhof

VHS

Werkstätten Rendsburg • Fockbek

Projektbüro.....Projekt „Vernetzt!"
IBAF gGmbH
Kanalufer 48
24768 Rendsburg
Telefon 04331 1306 -73
Telefax 04331 1306 -70
E-Mail: vernetzt@ibaf.de

408_9/2016

Ver-netzt!

Ein Projekt des
Institut für berufliche Aus- und Fortbildung

Foto: Shutterstock/Maksim Kabakou

Mehr Sicherheit im Internet

10 wichtige Punkte, die Sie beachten sollten!

Gefördert durch
Aktion Mensch · Diakonie Schleswig-Holstein · Diakonie Stiftung Schleswig-Holstein

Mehr Sicherheit im Internet: **10 wichtige Punkte, die Sie beachten sollten!**

Die meisten Kriminellen, die im Internet unterwegs sind, verwenden unterschiedliche Tricks, um unser Verhalten auszuspähen, unsere persönlichen Daten zu stehlen, unser Geld zu entwenden oder uns zu erpressen.

Trick Nummer 1: „Phishing“

„Phishing“ leitet sich vom englischen Wort „Fishing“ ab (englischer Begriff für Angeln bzw. Fischen). Internet-Betrüger wollen unsere Daten abfischen. Das versuchen sie über zwei Wege:

- über gefälschte E-Mails oder
- gefälschte Internetseiten.

Ein Beispiel:
In einer scheinbar echten E-Mail werden wir von unserer Bank aufgefordert, unsere Benutzerdaten (Benutzername, Passwort) zu aktualisieren. Wir sollen auf einen Link klicken. Dieser Link leitet uns auf die scheinbar echte Seite unserer Bank. Es handelt sich um eine gefälschte Internetseite, die von der Originalseite kaum zu unterscheiden ist.

Auf der gefälschten Internetseite werden wir erneut aufgefordert, unsere „Account-Informationen“ (Benutzernamen und Passwort) zu aktualisieren. Sobald wir das getan haben, werden unsere Daten an die Betrüger gesendet. Die Betrüger können nun problemlos in unserem Namen Geschäfte tätigen.

Trick Nummer 2: Schad-Software

Schad-Software wird im Englischen „Malware“ genannt. Das sind „bösartige“ Programme, die mit Computer-Viren infiziert sind. Zur sogenannten Malware gehören z. B. Viren, Würmer und Trojaner, aber auch Spyware, Scareware oder Ransomware.

Wenn man die Schad-Software herunterlädt, wird der eigene Computer automatisch angesteckt, er wird infiziert. Es kommt zu einem großen Schaden, bei dem für uns wichtige Daten verloren gehen oder nicht mehr zur Verfügung stehen.

Schad-Software kann sich z. B. auf gefälschten Internetseiten, in Datei-Anhängen, in Programmen, Downloads und hinter Links verbergen.

Was können wir tun, um uns vor diesen Tricks zu schützen?
10 wichtige Punkte:

1. ***Halten Sie Ihr Betriebssystem (z. B. Windows, MacOs) und Ihre Programme immer auf dem aktuellen Stand. Sorgen Sie dafür, dass die automatischen Updates (Aktualisierung) aktiviert sind.***

   Das gilt für alle Programme, die Sie offiziell gekauft haben und deren Quelle Sie kennen und vertrauen. Updates sorgen dafür, dass die Programme den derzeit besten Schutz gewährleisten und einwandfrei funktionieren.

2. ***Installieren Sie ein getestetes und aktuelles Antiviren-Programm.***

   Ein Antivirenprogramm ist eine Software, die gefährliche Computer-Viren (Computer-Würmer, Trojaner etc.) entdeckt und unschädlich macht.

3. ***Benutzen Sie sichere und unterschiedliche Passwörter.***

   Verwenden Sie für unterschiedliche Aktionen auch unterschiedliche Passwörter. Sichere Passwörter sind lang und kombinieren kleine und große Buchstaben, Zahlen, Satz- und Sonderzeichen.

4. ***Surfen und kaufen Sie mit größter Vorsicht!***

   Internet-Seiten können Viren übertragen. Achten Sie deshalb darauf, dass Sie niemals mit vollen Administratorenrechten surfen. Richten Sie ein gesondertes Benutzerkonto ein. Surfen Sie nur von diesem Benutzerkonto aus und sorgen Sie dafür, dass Ihre Benutzerkontensteuerung „UAC“ (User Account Control) eingeschaltet ist.

   Die Benutzerkontensteuerung kontrolliert, was Sie machen und welche Aktionen die Programme vornehmen. Sie meldet sich sofort, wenn „jemand“ im Begriff ist, wichtige System-Dateien zu verändern.

   Auch beim Kauf in einem Internet-Shop ist größte Vorsicht gefragt: Kaufen Sie nur in zertifizierten oder Ihnen bekannten Internet-Shops! Prüfen Sie das Impressum, die Datenschutzbestimmungen und die Bezahlmöglichkeiten, bevor Sie sich für einen Kauf entscheiden.

5. ***Übermitteln Sie Ihre Benutzerdaten (Benutzername, Kontodaten, Passwörter) nur auf Internet-Seiten, die mit „https“ geschützt sind oder durch ein Schloss gekennzeichnet sind.***

   Bei Internetadressen, die mit „https“ beginnen (z. B. https://www.fh-kiel.de) oder zu Beginn mit einem kleinen Schloss gekennzeichnet sind, werden Ihre Daten verschlüsselt übertragen. Sie sind dadurch besonders gut vor Missbrauch geschützt. Kaufen Sie deshalb nur in Internetshops, deren Internetadresse mit „https“ beginnt oder zu Beginn mit dem entsprechenden Schloss gekennzeichnet ist.

6. ***Öffnen Sie nicht jede E-Mail.***

   Überprüfen Sie, von wem Ihre E-Mails kommen. Wenn Sie den Absender nicht kennen, dann löschen Sie die E-Mail, ohne sie vorher zu öffnen.

   Wenn Sie Ihre Mailadresse im Internet sichtbar veröffentlichen, können Sie [at] statt @ benutzen. So haben Sie einen besseren Schutz vor ungebetenen E-Mails (Spam-E-Mails).