Die 10 wichtigsten Tipps zum Schutz Ihrer persönlichen Daten und Ihrer Identität

Immer wenn Sie online gehen, um E-Mails oder Instant Messages (IMs) zu lesen und zu schreiben, etwas bestellen oder Ihre Bankgeschäfte erledigen, übermitteln Sie persönliche Daten, wie Adressen, Telefon- und Kontonummern, Benutzernamen und Kennwörter. Damit riskieren Sie unglücklicherweise auch, dass Ihre persönlichen Daten oder sogar Ihre Identität gestohlen werden oder Ihr PC von Hackern als Startplattform für Angriffe gegen andere Systeme missbraucht wird.

Schützen Sie sich und Ihren Computer, indem Sie diese zehn wichtigen Tipps befolgen:

1. **Investieren Sie in bewährte, vielseitige Sicherheits-Software.** Wählen Sie umfassende, vielseitige PC-Sicherheits-Software, die Sie vor Viren, Spyware, Adware, Hackern, unerwünschten E-Mails, Phishing-Angriffen und Identitätsdiebstahl schützt. Entscheiden Sie sich für eine Marke, der Sie vertrauen können, wie z.B. McAfee®.

2. **Gehen Sie nie ohne aktivierte Firewall ins Internet.** Eine Firewall sorgt für einen Schutzschild zwischen Ihrem PC und dem Internet und verhindert, dass Hacker Ihre Identität stehlen, Ihre Dateien zerstören oder Ihren PC für Angriffe auf andere benutzen.

3. **Nutzen Sie einen PC, von dem Sie wissen, dass er sicher ist.** Hacker können leicht sensible Daten abfangen, die über eine ungesicherte Internetverbindung gesendet werden. Wenn Sie sensible Informationen versenden oder Online-Transaktionen vornehmen müssen, nutzen Sie einen PC, von dem Sie wissen, dass er sicher ist und vergessen Sie nicht, dass Sicherheit viele Facetten hat. Einige Computer verfügen nur über ein absolutes Minimum an Schutz, während andere, z.B. solche mit McAfee Total Protection™, über umfassenden Schutz verfügen.

4. **Achten Sie auf Phishing-Mails.** Bei Phishing-Angriffen werden gefälschte E-Mails und Websites, die den Anschein erwecken, aus einer seriösen Quelle zu stammen, dazu benutzt, ahnungslosen Benutzern Angaben zu persönlichen Konto- oder Anmeldedaten zu entlocken. Auch wenn Sie über Sicherheits-Software verfügen, können Sie ohne Ihr Wissen auf eine bösartige Webseite geraten. Seriöse Unternehmen werden Sie nie auffordern, Ihre persönlichen Daten per E-Mail zu aktualisieren. Überprüfen Sie Internetadressen, bevor Sie Ihre persönlichen Informationen abschicken.

5. **Sichern Sie Ihr drahtloses Netzwerk.** Sie gehen ein Risiko ein, wenn Sie über ein Wi-Fi-Netzwerk ins Internet gehen. Da die Funkwellen Ihres drahtlosen Netzwerks durch Wände dringen, kann ein Hacker Sie mit einer einfachen Antenne aus großer Entfernung angreifen, um Ihre Daten zu stehlen und Ihr drahtloses Netzwerk für eigene Zwecke zu nutzen. Ergeifen Sie zusätzliche Schutzmaßnahmen für Ihr drahtloses Netzwerk.

6. **Installieren Sie keine potenziell unerwünschten Programme (PUPs) wie Spyware oder Adware auf ihrem PC.** Viele kostenlose Programme, die Sie aus dem Internet herunterladen, erscheinen harmlos, wurden aber speziell dazu entwickelt, Ihre Tastaturanschläge und Internet-Anmeldedaten aufzuzeichnen, Ihre vertraulichen Informationen zu übermitteln oder Ihren Browser auf gefälschte Websites umleiten. Einige dieser Programme werden durch einfaches Anklicken eines Werbe-Links im Internet auf Ihrem PC installiert.

   Mit Sicherheits-Software können Sie die Installation solcher Programme verhindern. Installieren Sie niemals Programme, wenn Sie die betreffende Webseite und das Programm nicht genau kennen und die Endbenutzer-Lizenzvereinbarung nicht sorgfältig gelesen haben.

7. **Beantworten Sie keine Kettenbriefe.** Auch wenn Ihr PC geschützt ist - Sie werden vielleicht in einem Kettenbrief von Freunden nach persönlichen Informationen gefragt. Laden Sie keine Dateien von Freunden oder Familienangehörigen herunter, wenn Sie den Inhalt der Datei nicht kennen und wissen, dass sie sicher ist.

8. **Überprüfen Sie Ihre Kreditkartenabrechnungen und seien Sie wachsam.** Überprüfen Sie mindestens ein Mal im Jahr Ihre Kreditkartenabrechnungen. Das ist eine der besten Möglichkeiten, herauszufinden, ob jemand ohne Ihr Wissen Ihre persönlichen Finanzdaten benutzt. Informieren Sie sich auf der Gateway Support-Seite über die neuesten Tipps zur Sicherung Ihres Computers oder lesen Sie auf der Webseite der amerikanischen Federal Trade Commission über die jüngsten Trends beim Identitätsdiebstahl.

9. **Überwachen Sie die Online-Aktivitäten Ihrer Kinder.** Begrenzen Sie die Online-Zeit Ihrer Kinder. Installieren und nutzen Sie Software mit Kindersicherung, die es Ihnen ermöglicht, die Online-Aktivitäten Ihrer Kinder zu überwachen. Auf diese Weise können Sie Ihre Kinder von unerwünschten Seiten fernhalten und sie daran hindern, persönliche Daten online weiterzugeben.

10. **Sichern Sie kritische Daten regelmäßig.** Sichern Sie wichtige Dateien auf externen Speichermedien wie Zip-Disketten oder beschreibbaren CD-ROMs (CD-R oder CD-RW). Verwenden Sie nach Möglichkeit Backup-Software und bewahren Sie die Backup-Disketten für den Notfall auf.

McAfee GmbH
Ohmstr. 1
85716 Unterschleissheim
+49-89-3707 0
www.mcafee.de