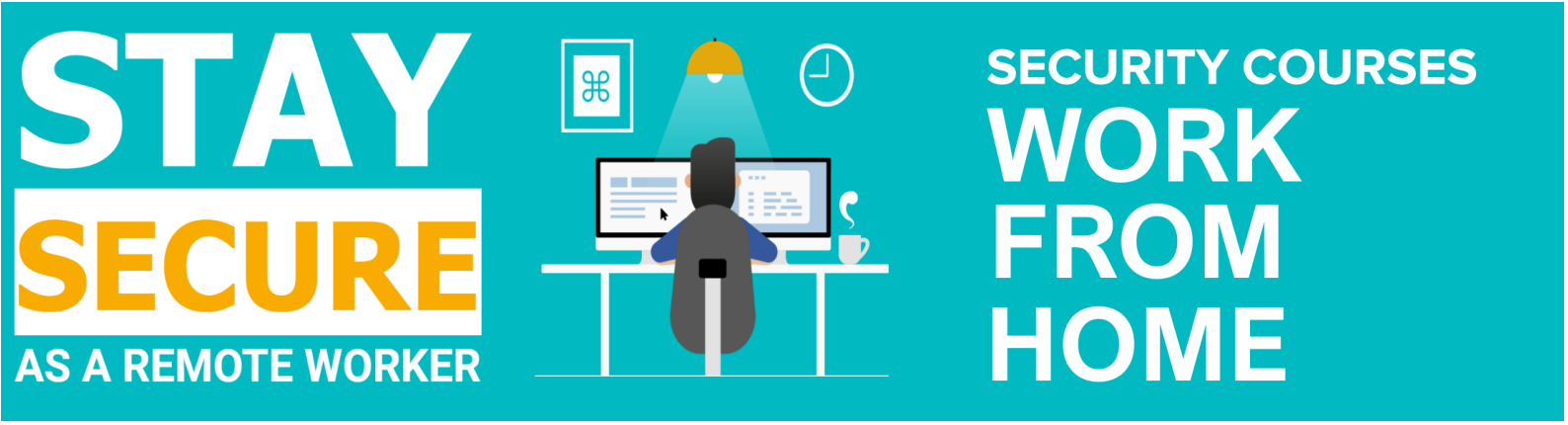


SCHÜTZEN SIE IHREN PC MIT DIESEN TIPPS VON LUCY SECURITY ZUR INTERNETSICHERHEIT

Unabhängig davon, ob Sie Ihren PC für geschäftliche oder private Zwecke verwenden, Sicherheit, auch für dessen Inhalte - sollte an erster Stelle stehen. Führen Sie die nachfolgenden Schritte aus, um das Risiko einer Gefährdung Ihres Computers zu verringern.

✓ TIPP 1: HALTEN SIE DIE SOFTWARE AUF DEM NEUESTEN STAND

Viele Sicherheitsprobleme werden durch Software verursacht, die nicht auf den neuesten Stand gebracht wurde. Die meisten Programme können Updates automatisch installieren. Wenn Sie einem Windows-PC verwenden, müssen Sie nur die automatischen Updates aktivieren, um Windows, Microsoft Office und andere Microsoft-Anwendungen auf dem neuesten Stand zu halten.

Aktivieren Sie auch für Nicht-Microsoft-Anwendungen wie Adobe Acrobat Reader und andere Programme, die Sie regelmäßig verwenden, automatische Updates.

Verwenden Sie für Macs den Software-Update-Mechanismus, den Sie in den Systemeinstellungen im Apple-Menü finden.

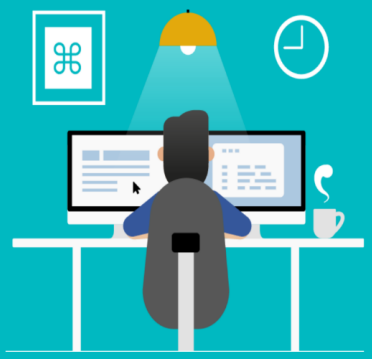
✓ TIPP 2: INSTALLIEREN SIE ANTIVIRUS-SOFTWARE

Antivirensoftware ist ein Muss für alle, sowohl für Windows, als auch für Mac-Benutzer. Antiviren-Programme müssen ebenfalls regelmäßig aktualisiert werden. Wenn Sie USB-Sticks oder externe Festplatten verwenden, scannen Sie diese immer auf Viren, insbesondere wenn dieses Laufwerk einer anderen Person gehört.

✓ TIPP3: SICHERES SURFEN IM WEB

Vermeiden Sie den Besuch von Webseiten, die potenziell illegale Inhalte anbieten. Besuchen Sie vor allem keine Pornoseiten (oder andere fragwürdige Webseiten)! Das Problem ist, dass es Webseiten gibt, die Ihren Computer mit einem Virus infizieren wollen. Viele Pornoseiten zielen absichtlich darauf ab. Verwenden Sie einen modernen Browser wie Microsoft Edge oder die neueste Chrome-Version, mit der Sie schädliche Webseiten blockieren und verhindern können, dass ein bösartiger Code auf Ihrem Computer ausgeführt wird. Niemals Software von nicht vertrauenswürdigen Quellen herunterladen, installieren oder ausführen!

STAY SECURE AS A REMOTE WORKER



SECURITY COURSES

WORK FROM HOME

✓ TIPP 4: E-MAIL SICHER NUTZEN

Achten Sie bei Durchsicht Ihrer E-Mails auf betrügerische Versuche, Ihre persönlichen Daten oder Ihr Geld zu stehlen. Viele dieser Betrügereien werden als „Phishing“ bezeichnet. Öffnen Sie keine seltsamen Anhänge und klicken Sie nicht auf verdächtige Links in Nachrichten. Diese können in E-Mails, Tweets, Posts, Online-Anzeigen, Nachrichten oder Anhängen erscheinen und tarnen sich manchmal als bekannte und vertrauenswürdige Quellen.

✓ TIPP 5: ERSTELLEN SIE IHR EIGENES BENUTZERKONTO MIT BESCHRÄNKTEN BENUTZERRECHTEN

Selbst wenn Sie die einzige Person sind, die Ihren Computer verwendet, richten Sie ein Benutzerkonto ohne Administratorenrechte ein, mit denen Sie arbeiten. Dies schränkt den Schaden ein, den schädliche Software anrichten kann.

✓ TIPP 6: IHR PASSWORT SOLLTE SICHER UND NICHT ZU KACKEN SEIN

Verwenden Sie ein Passwort mit mindestens acht Zeichen und einer Kombination aus Zahlen, Groß- und Kleinbuchstaben. Verwenden Sie keine erkennbaren Wörter oder Kombinationen, die Geburtstage oder andere Informationen darstellen, die mit Ihnen in Verbindung stehen. Verwenden Sie außerdem für jede von Ihnen verwendete Webseite ein anderes Passwort.

✓ TIPP 7: ÜBERPRÜFEN SIE IHRE FIREWALL

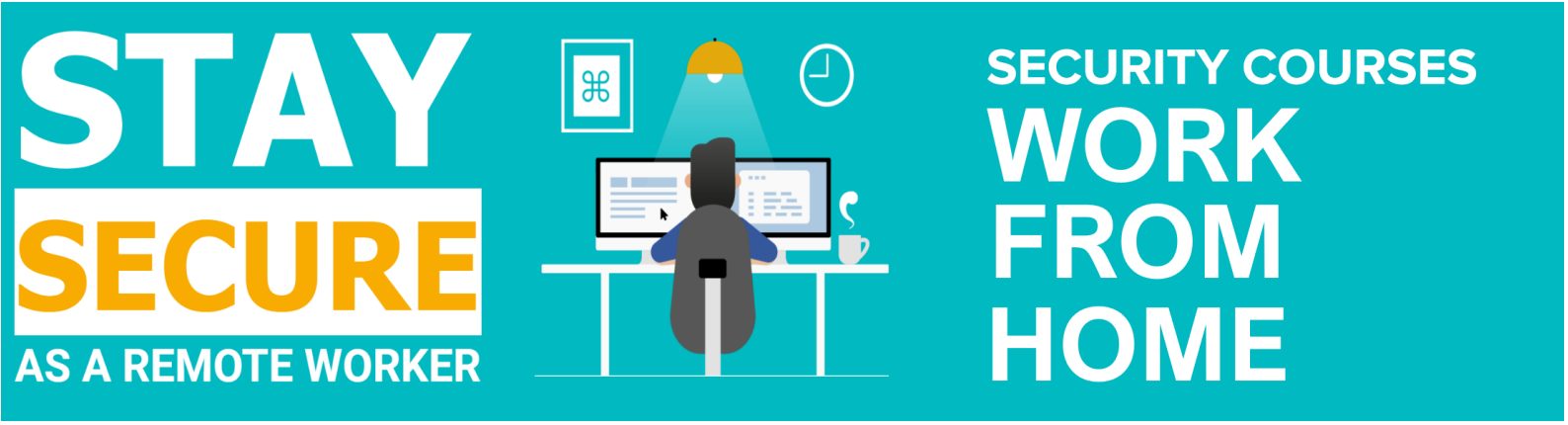
Eine Firewall fungiert als Barriere zwischen Ihrem Computer oder Netzwerk und dem Internet. Das Überprüfen Ihrer Firewall klingt kompliziert, ist es aber nicht. Wenn Sie ein Windows-basiertes System benutzen, rufen Sie einfach die Systemeinstellungen auf und geben Sie „Firewall" in das Suchfeld ein. Wenn Ihre Firewall eingeschaltet oder verbunden ist, können Sie loslegen.

Wenn Sie einen Mac besitzen, klicken Sie auf das Apple-Symbol in Ihrer Symbolleiste, gehen Sie zu „Systemeinstellungen", dann zu „Sicherheit und Datenschutz" und dann zu „Firewall".

✓ TIPP 8: VERMEIDEN SIE RISKANTE PERIPHERIE-GERÄTE

USB-Sticks und andere Speichermedien könnten mit Malware infiziert sein. Verwenden Sie keine USB-Sticks oder andere externe Geräte, es sei denn, Sie besitzen diese.

Um eine Infektion durch Malware und Viren zu vermeiden, stellen Sie sicher, dass alle externen Geräte entweder Ihnen gehören oder von einer vertrauenswürdigen Quelle stammen.



✓ TIPP 9: TRENNEN SIE DIE VERBINDUNG ZUM INTERNET, WENN DIESE NICHT BENÖTIGT WIRD

Schalten Sie Ihren Computer für einen längeren Zeitraum oder über Nacht aus, wenn Sie nicht arbeiten. Wenn er immer eingeschaltet ist, sind Sie für einen Hacker leichter sichtbar. Durch Herunterfahren wird die Verbindung unterbrochen, die ein Hacker möglicherweise mit Ihrem Netzwerk hergestellt hat, und es wird mögliches Unheil verhindert.

✓ TIPP 10: TRENNEN SIE AUF IHREM PC BERUFLICHE UND PRIVATE AKTIVITÄTEN

Wenn Computer eher für den privaten als für den professionellen Gebrauch verwendet werden, steigt die Wahrscheinlichkeit von Infektionen und anderen Sicherheitsvorfällen - Filme, Spiele, Musik und andere persönliche Anwendungen sind mit Risiken verbunden. Wenn Sie nur einen PC besitzen und Ihre Arbeit und Ihre persönlichen Aktivitäten trennen möchten, nehmen Sie sich Zeit, um verschiedene Benutzerkonten zu erstellen - eines für Ihre Arbeit und eines für den privaten Gebrauch.

✓ TIPP 11: SICHERN SIE ZU HAUSE IHR NETZWERK

Es ist wichtig, dass Sie zu Hause Ihr WLAN sichern. Stellen Sie sicher, dass für Ihr Heim-WLAN die Sicherheitsfunktion aktiviert ist und dass Sie das Administratorenkennwort Ihres Routers geändert haben. Bei den meisten Routern können Sie auch Ihr WLAN „verstecken". Dies bedeutet, dass ein Benutzer sowohl die WLAN-ID als auch das Kennwort kennen muss, um online zu gehen.

Jetzt kennen Sie die wichtigen Schritte, die Sie setzen müssen, um Ihre persönlichen und Unternehmensinformationen zu schützen, wenn Sie an Ihrem privaten PC arbeiten. Gehen Sie auf Nummer sicher!