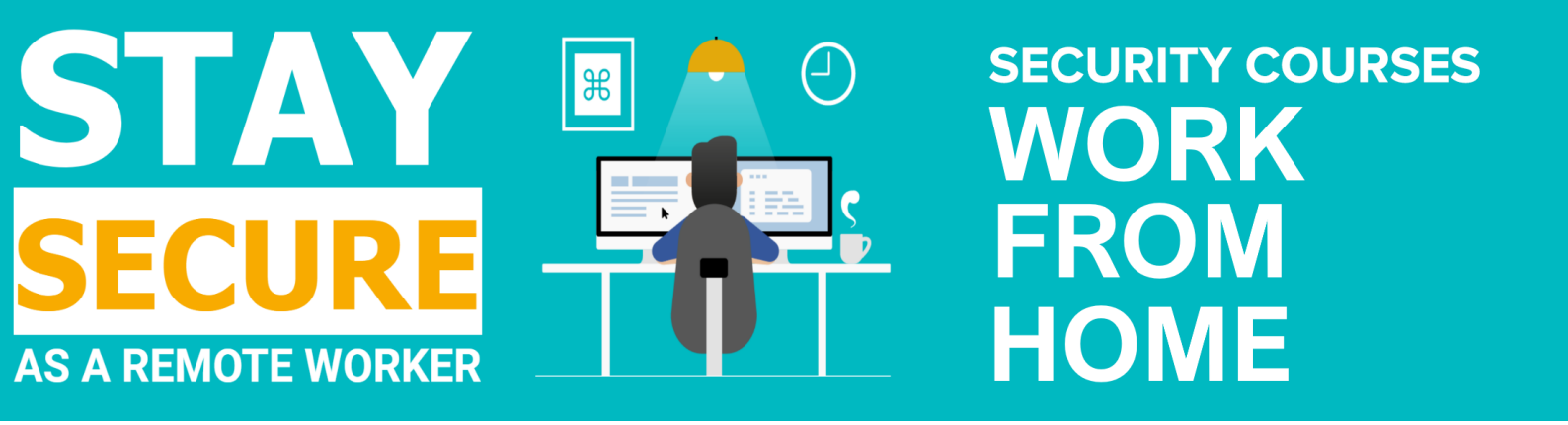


BLEIBEN SIE BEI ARBEIT ZUHAUSE SICHER SICHERHEITSKURS ARBEITEN VON ZU HAUSE

Es gibt viele Vorteile, zu Hause oder außerhalb Ihres Büros zu arbeiten. Dazu gehören weniger Zeit für den Weg zur Arbeit, weniger Ablenkungen im Büro und eine geringere Wahrscheinlichkeit, eine ernsthafte Infektion zu bekommen. Unabhängig davon, ob Sie von zu Hause aus oder an einem anderen Ort der Welt arbeiten, SIE sind dafür verantwortlich, Ihre eigene Sicherheit und die für Ihre Geräte und aller von Ihnen mitgeführten Daten zu gewährleisten.

Sie können sich nicht auf das hohe Sicherheitsniveau wie im Büro verlassen. Sie müssen also gut vorbereitet sein, außerhalb Ihres Büros zu arbeiten. Wenn Sie dies nicht tun, riskieren Sie, ein leichtes Opfer für Diebe, Taschendiebe, skrupellose Konkurrenten und andere Kriminelle zu sein. Diese Kriminellen möchten Ihre persönlichen Daten, Gegenstände oder die Daten Ihres Arbeitgebers stehlen. Eine gute Vorbereitung kann diese Risiken verringern und Ihre Arbeit außerhalb der Firma erfolgreich und sicher gestalten.

WELCHEN SICHERHEITSRISIKEN BESTEHEN, WENN SIE ZU HAUSE ARBEITEN?

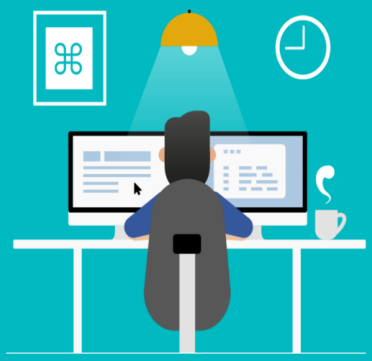
Viele Dinge können die Sicherheit der Arbeit außerhalb der Firma und die Unternehmensdaten, die Sie täglich verwenden, beeinträchtigen.

In diesem Kurs haben wir diese Risiken in vier Hauptkategorien eingeteilt: Realer Diebstahl oder Verlust. Mangel an persönlichem Sicherheitsbewusstsein. Ungesicherte öffentliche Konnektivität und organisatorisch ungeschützter Zugriff auf Daten.

REALER DIEBSTAHL ODER VERLUST

Wenn Sie in einem Büro arbeiten, greifen Sie auf viele unterstützende Systeme zurück. Diese Systeme beinhalten meist umfassende Sicherheit sowie Sicherheitspersonal. Sie werden durch Datensicherheitssysteme, gute Sicherheitspraktiken und Sicherheitsbeauftragte unterstützt.

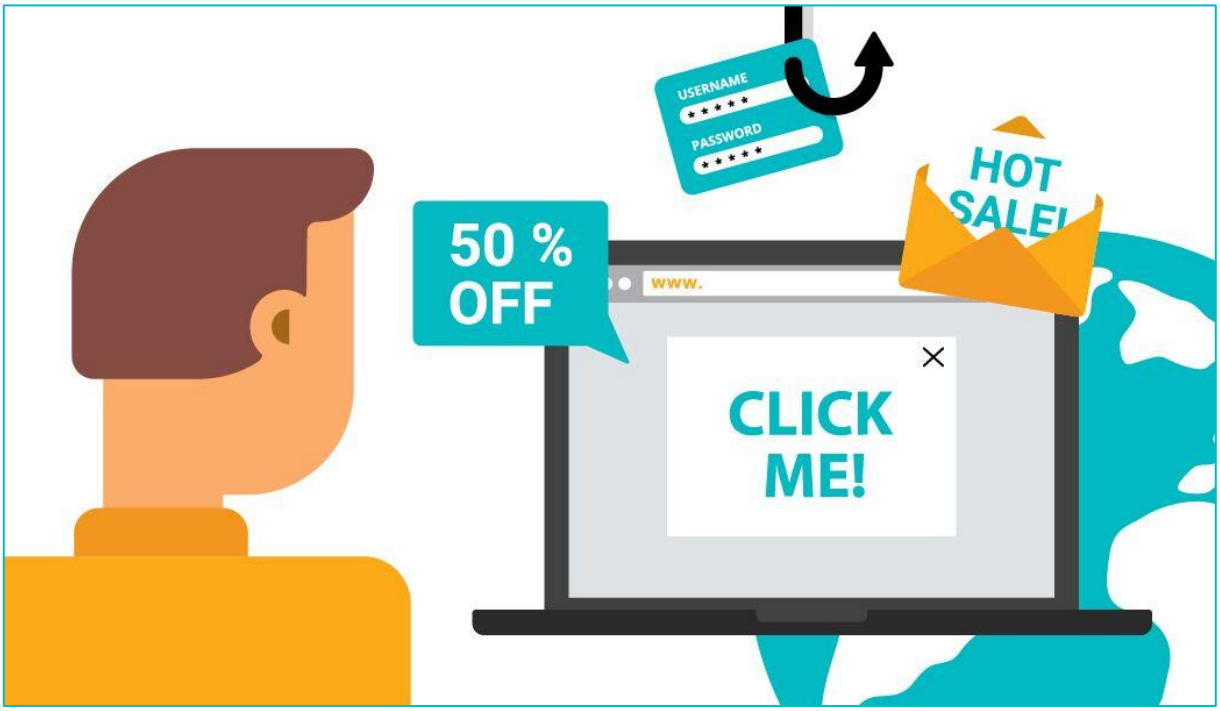
STAY SECURE AS A REMOTE WORKER



SECURITY COURSES WORK FROM HOME

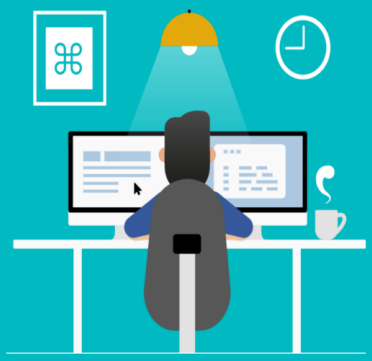
MANGEL AN PERSÖNLICHEN SICHERHEITS-BEWUSSTSEIN

In vielen Fällen bringt die Arbeit zu Hause weniger Ablenkungen. Wenn Sie gut organisiert sind, können Sie sich außerhalb des Büroumfelds besser konzentrieren. Aber ohne ständige Wachsamkeit bemerken Sie vielleicht nicht, dass Sie für andere eine Zielscheibe sind.



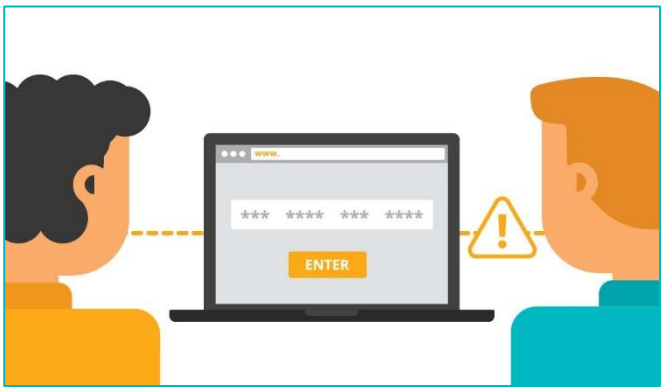
Möglicherweise greifen Sie mit Ihrem persönlichen oder auf einem öffentlichen Gerät auf die Daten Ihres Arbeitgebers zu. Oder schlimmer noch: Sie surfen von einem offiziell aufgestellten Gerät aus im Internet. Jede dieser Vorgehensweisen kann Ihre Sicherheit und die Daten Ihres Arbeitgebers gefährden.

STAY SECURE AS A REMOTE WORKER



SECURITY COURSES WORK FROM HOME

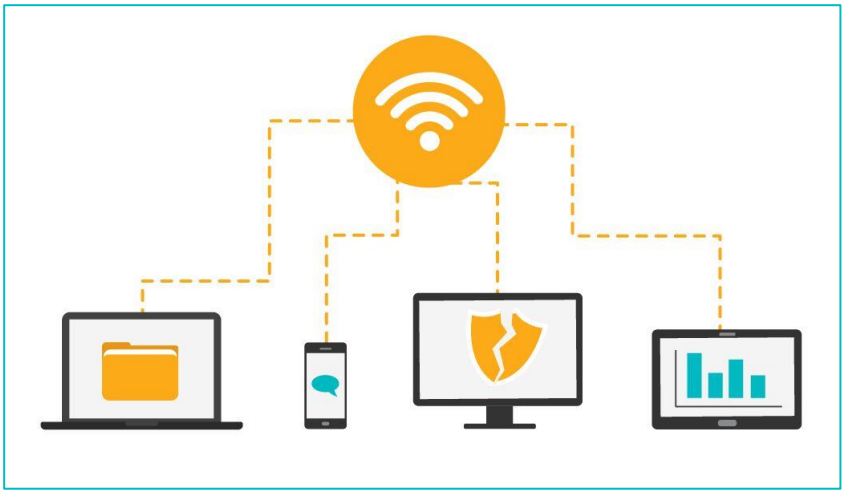
UNEINGESCHRÄNKTER UNTERNEHMENSZUGANG



Viele Unternehmen gewähren Mitarbeitern außer Haus dieselben Zugriffsrechte wie in einem sicheren Büro. Dies umfasst den vollständigen Zugriff auf alle Netzwerke, Cloud-Speicher, interne Systeme, usw.

Wenn Sie nicht besonders sorgsam sind oder nicht über das nötige Sicherheitsbewusstsein verfügen, können solche Berechtigungen einem Angreifer den vollen Zugriff auf die Daten Ihres Arbeitgebers gewähren.

UNGESICHERTE ÖFFENTLICHE VERBINDUNGEN

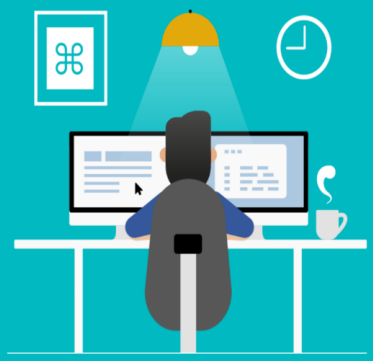


Wie oft haben Sie auf Reisen ein öffentliches WLAN benutzt? In einem Café, am Flughafen oder in einem Hotelzimmer?

Die meisten dieser Netzwerke bieten keinerlei Sicherheit. Das bedeutet, dass aufgrund der Arbeitsanforderungen Ihr Gerät und Ihre Daten potenziellen Hacker-Attacken ausgesetzt sind.

Die Bedrohung ist real, da die meisten öffentlichen Netzwerke nicht verschlüsselt sind. Das Netzwerk fordert Sie nicht zur Authentifizierung auf, um eine Verbindung herzustellen. Solche Netzwerke können Hackern Zugriff auf alle Informationen gewähren, die Sie über das Internet senden. Von vertraulichen E-Mails über sicherheitsrelevante Daten Ihres Unternehmens bis hin zu Kreditkartendaten.

STAY SECURE AS A REMOTE WORKER



SECURITY COURSES WORK FROM HOME

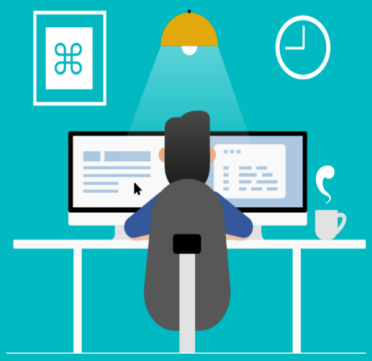
WAS KÖNNEN SIE TUN, UM SICH UND IHR UNTERNEHMEN ZU SCHÜTZEN, WENN SIE AUSSERHALB DES BÜROS ARBEITEN?

Es gibt gute Nachrichten! Jeder kann sein „Remote“-Büro absichern. Sie müssen nur einige wichtige Gewohnheiten entwickeln. Achten Sie stets auf die erforderlichen Sicherheitsmaßnahmen.

SCHRITT 1: BEREITEN SIE SICH UND IHRE ARBEITSMATERIALIEN VOR

Wenn Sie außerhalb des Büros arbeiten müssen, egal ob Sie auf Reisen sind oder nur von zu Hause aus arbeiten, stellen Sie sicher, dass Sie vorbereitet sind, Ihre Aufgaben sicher durchzuführen. Ihr IT-Support-Team gibt Ihnen gerne Ratschläge und zeigt Ihnen, wie Sie sicher Fernzugriff auf Dateien und Systeme erhalten, die Sie für Ihre Arbeit benötigen.

STAY SECURE AS A REMOTE WORKER



SECURITY COURSES

WORK FROM HOME

Bevor Sie von Ihrem Büro nach Hause arbeiten gehen, nehmen Sie Ihren Computer und alle jene Dokumente mit, die Sie für Ihre Arbeit benötigen. Nehmen Sie jedoch nicht alles mit. Lassen Sie vertrauliche Kundendaten, Geschäftspläne, geschützte Informationen und Daten im Büro. Diese Vorsichtsmaßnahme verringert die Anzahl der Dinge, die Sie sicher aufbewahren müssen. Wenn ein Dieb Ihr Gerät stiehlt oder Sie es verlieren, sind die Auswirkungen für Sie und Ihren Arbeitgeber vermindert.

SCHRITT 2: HALTEN SIE IHRE GERÄTE UP-TO-DATE UND SICHER

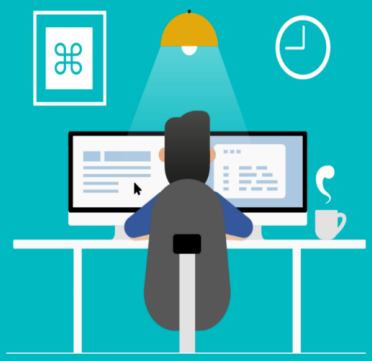
Um Ihre Geräte zu sichern, müssen Sie darauf achten, dass die gesamte installierte Software, einschließlich des Betriebssystems, auf dem neuesten Stand ist. Beachten Sie, dass kein Betriebssystem vollständig sicher ist. Sicherheitsunternehmen und Hacker stellen ständig Schwachstellen fest, die sich auf jede Version Ihrer Software auswirken. Das Risiko ist viel höher, wenn das Betriebssystem älter ist und nicht mehr unterstützt wird. Wir empfehlen Ihnen, Ihre Geräte immer mit der neuesten unterstützten Betriebssystemversion laufen zu lassen.

Die meisten Sicherheitslücken brauchen mehr als zwei Monate, um behoben zu werden. Stellen Sie sich vor, was mit einem System passieren kann, wenn es für diesen Zeitraum Bedrohungen ausgesetzt ist. Vermindern Sie Verzögerungen beim Aktualisieren Ihres Geräts mit den neuesten Sicherheitspatches: Aktivieren Sie die Option für automatische Updates. Es ist immer der beste Rat, Ihrem System zu erlauben, diese Updates herunterzuladen und anzuwenden, sobald sie verfügbar sind.

Sobald Ihr System durch regelmäßige Updates sicher läuft, ist es Zeit, Ihre Aufmerksamkeit auf alle anderen Programme zu lenken, die darauf ausgeführt werden. Office oder Creative Suite, Browser und jede andere Software, die Sie anfällig machen könnte. Die meisten Softwareprogramme suchen automatisch nach Updates, sie müssen also nur den automatischen Download von Updates aktivieren.

SCHRITT 3: SPERREN SIE IHREN COMPUTER, WENN SIE WEGGEHEN

Wenn Sie nicht im Büro arbeiten, müssen Sie sicherstellen, dass Ihr dienstlich anvertrauter Computer sicher ist. Sowohl der Laptop selbst als auch die darin gespeicherten Informationen. Diese sind für einen Dieb oder einen Konkurrenten sehr wertvoll. Treffen Sie entsprechende Vorsichtsmaßnahmen, um die Sicherheit Ihres Geräts und aller darin enthaltenen Daten zu gewährleisten:



SCHRITT 3.1: GERÄTESPERRE AKTIVIEREN

Stellen Sie sicher, dass Sie das Gerät immer dann sperren, wenn Sie weggehen. Richten Sie Ihr Gerät so ein, dass es automatisch gesperrt wird, falls Sie das einmal vergessen. Stellen Sie die Sperre so ein, dass diese für ein Mobiltelefon / Tablet nach 30 Sekunden oder bei einem Laptop nach 5 Minuten Inaktivität greift.

✓ SCHRITT 3.2: AUTOMATISCHES LOGIN AUSSCHALTEN

Niemand außer Ihnen sollte auf Ihr Gerät zugreifen können. Stellen Sie daher sicher, dass für die Anmeldung eine Authentifizierung erforderlich ist. Verwenden Sie ein sicheres Passwort, eine PIN oder eine biometrische Alternative. Automatische Anmeldungen sind eine echte Bedrohung für die Sicherheit Ihres Arbeitgebers. Sorgen Sie also dafür, dass diese permanent ausgeschaltet ist.

✓ SCHRITT 3.3: VERWENDEN SIE NUR STARKE PASSWÖRTER

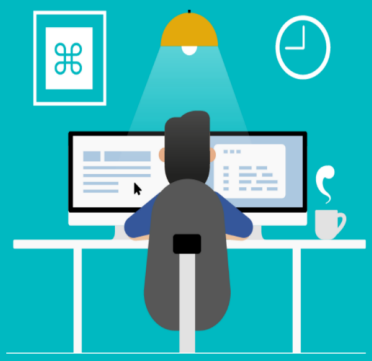
Wir können es nicht oft genug betonen, wie wichtig es ist, für all Ihre Geräte sichere Passwörter und PINs zu verwenden.

Schwache Passwörter enthalten gleiche oder aufeinanderfolgende Buchstaben / Zahlen, leicht zu erratende gebräuchliche Wörter und persönliche Informationen, die in sozialen Medien verfügbar sind (wie Geburtsdatum, Geburtsort, Nummernschild, usw.).

Ein sicheres Passwort muss für andere wie zufällig aussehen. Es sollte mindestens 8 Zeichen mit Klein- und Großbuchstaben, Zahlen und Symbolen gemischt enthalten.

✓ SCHRITT 3.4: INVESTIEREN SIE IN EINEN PASSWORTMANAGER (VIELE SIND KOSTENLOS)

Wenn Sie sichere, eindeutige Passwörter für alle Ihre Geräte und Konten verwenden, wird es schwierig, diese zu verwalten. Sie könnten ein Passwort vergessen, sollten es jedoch nicht auf einem Blatt Papier notieren. Hier kommt ein Passwort-Manager ins Spiel. Er kann viele Informationen speichern, verschlüsseln und in einem einzigen Passwort zusammenfassen, das Sie verfolgen können. Zu den Optionen gehören „1Password”, „LastPass” sowie viele andere.



✓ SCHRITT 3.5: VERWENDUNG DER ZWEI-FAKTOR-AUTHENTIFIZIERUNG (2FA)

In vielen Fällen reicht es nicht aus, nur ein Passwort zum Schutz Ihrer Konten zu haben. Insbesondere, wenn Sie sich bei einem IT-System, zu Online-Banking, E-Mail oder Ihrem Passwort-Manager anmelden. Alle diese Einrichtungen enthalten wichtige und hochwertige Daten, die Sie jederzeit sicher aufbewahren müssen.

Was ist die Zwei-Faktor-Authentifizierung (2FA)? Sie ist ein System, für das Sie ein Passwort und eine zusätzliche Identifikation benötigen, um Ihre Identität zu bestätigen. Dies kann ein einmaliger Code sein, der per SMS gesendet wird oder über eine Authentifizierungs-App läuft. Wenn eine 2FA für alle Ihre Geräte und Konten aktiviert ist, können Sie leichter atmen.

✓ SCHRITT 3.6: AKTIVIEREN SIE DIE OPTIONEN „FIND MY DEVICE“ UND „REMOTE WIPE“

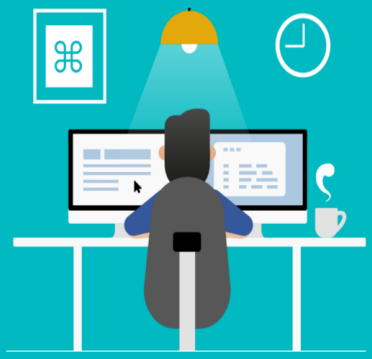
Bei Verlust oder Diebstahl Ihres Geräts ist es wichtig, dass Sie Ihr Gerät aus der Ferne lokalisieren und den Inhalt löschen können. Durch das Löschen können Ihre persönlichen und geschäftlichen Daten nicht in die Hände von Angreifern gelangen.

✓ SCHRITT 3.7: AUF WERKSEINSTELLUNGEN ZURÜCKSETZEN

Sie sollten Ihre Geräte immer auf die Werkseinstellungen zurücksetzen, wenn diese nicht mehr benötigt werden. Setzen Sie das Gerät auf die Werkseinstellungen zurück, bevor Sie es verkaufen, weitergeben oder anderweitig entsorgen.

Denken Sie daran, dass beim Löschen alle auf dem Gerät gespeicherten Informationen gelöscht werden. Wenn Sie diese Informationen für künftige Verwendung benötigen, stellen Sie sicher, dass Sie sie zuerst anderweitig sichern!

STAY SECURE AS A REMOTE WORKER

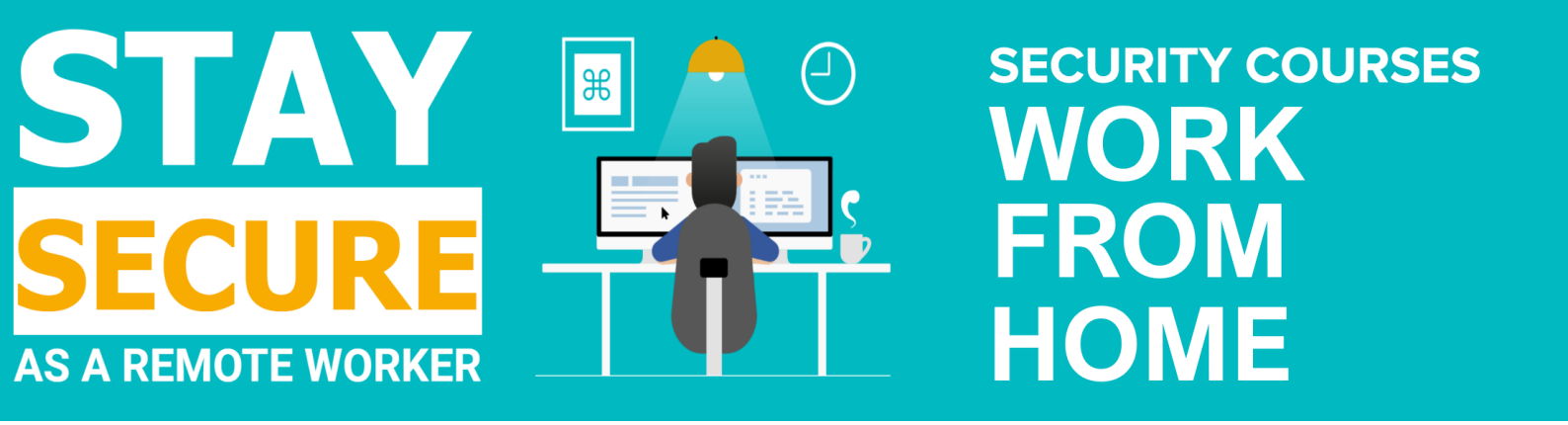


SECURITY COURSES WORK FROM HOME

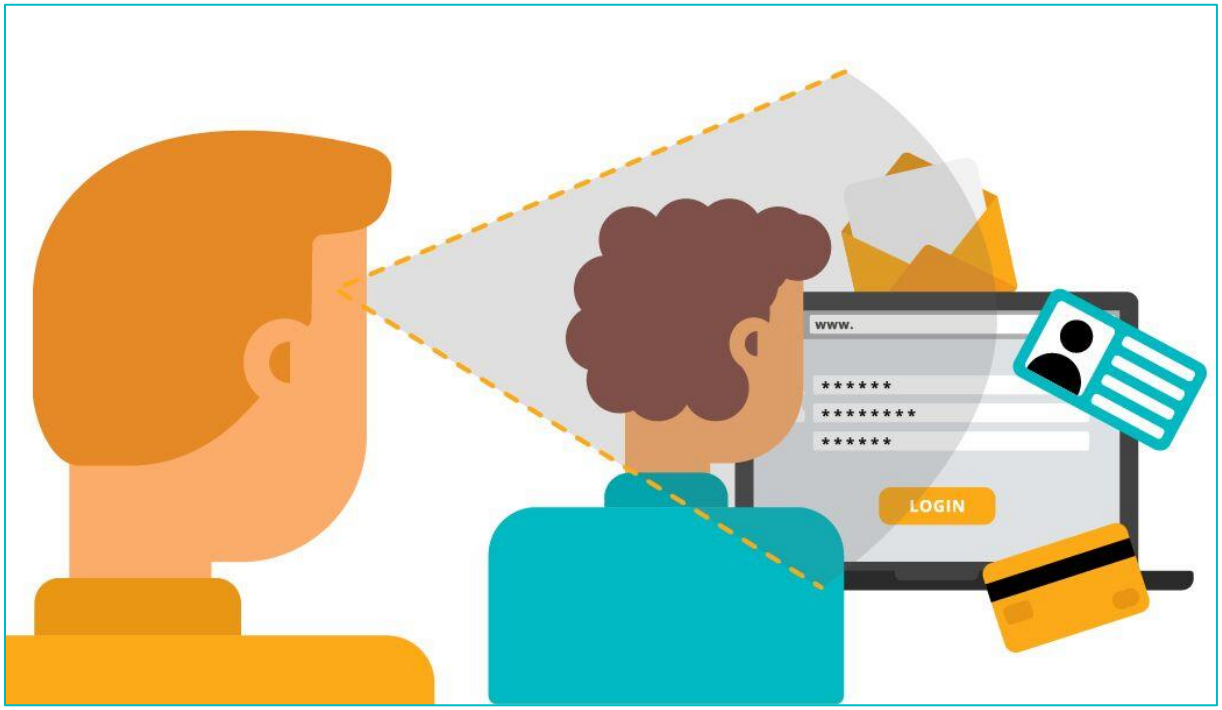
SCHRITT 4: ACHTEN SIE AUF IHRE UNMITTELBARE UMGEBUNG

Ihre unmittelbare Umgebung ist ebenso wichtig. Wenn Sie diese vernachlässigen, können Ihre persönliche Sicherheit, Ihr Gerät oder die Daten Ihres Arbeitgebers gefährdet sein. Dies gilt insbesondere für die Arbeit zu Hause. Schließen und verriegeln Sie immer Ihre Türen.

Seien Sie wachsam gegenüber Aktivitäten in Ihrer Umgebung. Lassen Sie Geräte oder USB-Sticks an öffentlichen Orten niemals unbeaufsichtigt. In der kurzen Zeit, die Sie für die Benutzung der Toilette benötigen, könnte ein Dieb Ihren Laptop stehlen. Ein Krimineller könnte Ihren Computer mit Malware infizieren. Der Verlust Ihres Geräts und der darauf gespeicherten Informationen kann enormen Stress verursachen und Ihren Arbeitsprozess erheblich stören. Verlorene Daten können zu Geldstrafen für Sie und Ihren Arbeitgeber führen.



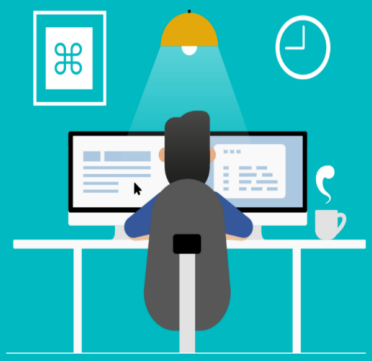
SCHRITT 5: ACHTEN SIE AUF DIE SICHTLINIEN



Achten Sie bei der Arbeit an einem öffentlichen Ort auf die Sichtlinien. Wenn möglich, setzen Sie sich mit dem Rücken zur Wand, damit niemand von hinten auf Ihren Bildschirm schauen kann (auch als Schulter-Surfen bekannt). Eine weitere Option ist die Verwendung eines Blickschutzfilters. Der Filter verdeckt jedem anderen - außer Ihnen - den Blick auf Ihren Bildschirm.

SCHRITT 6: VERTRAULICHE

STAY SECURE AS A REMOTE WORKER



SECURITY COURSES

WORK FROM HOME

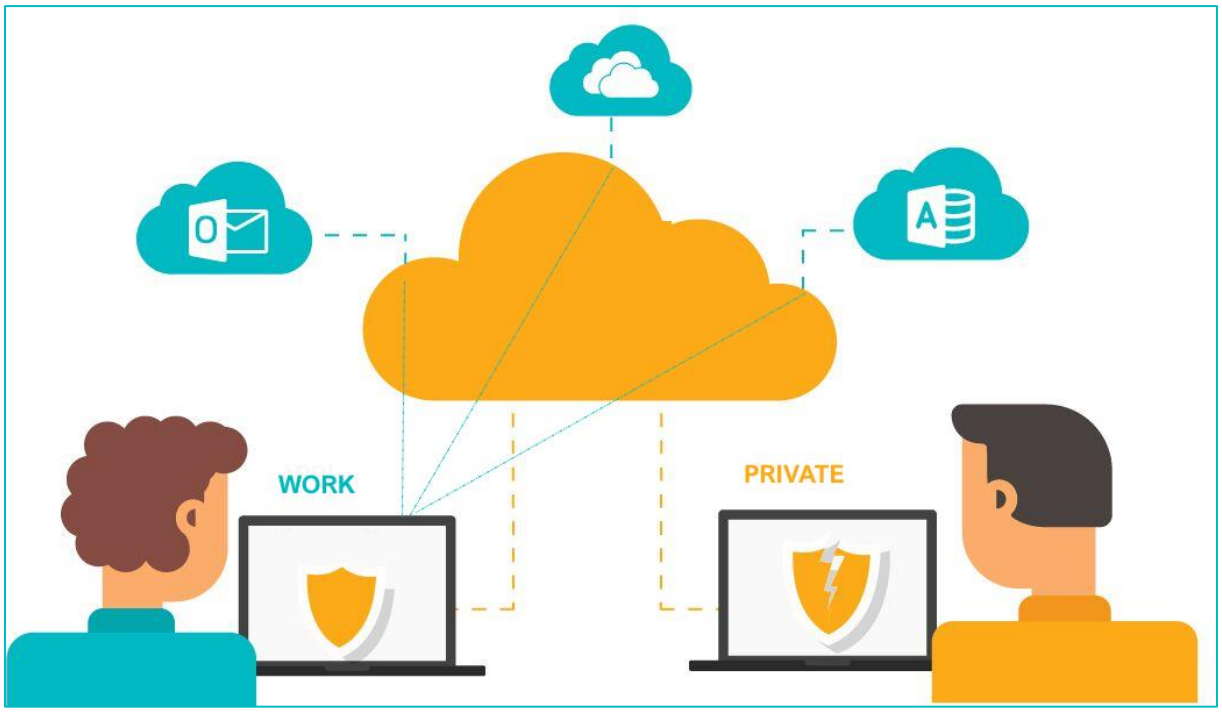
INFORMATIONEN SCHÜTZEN

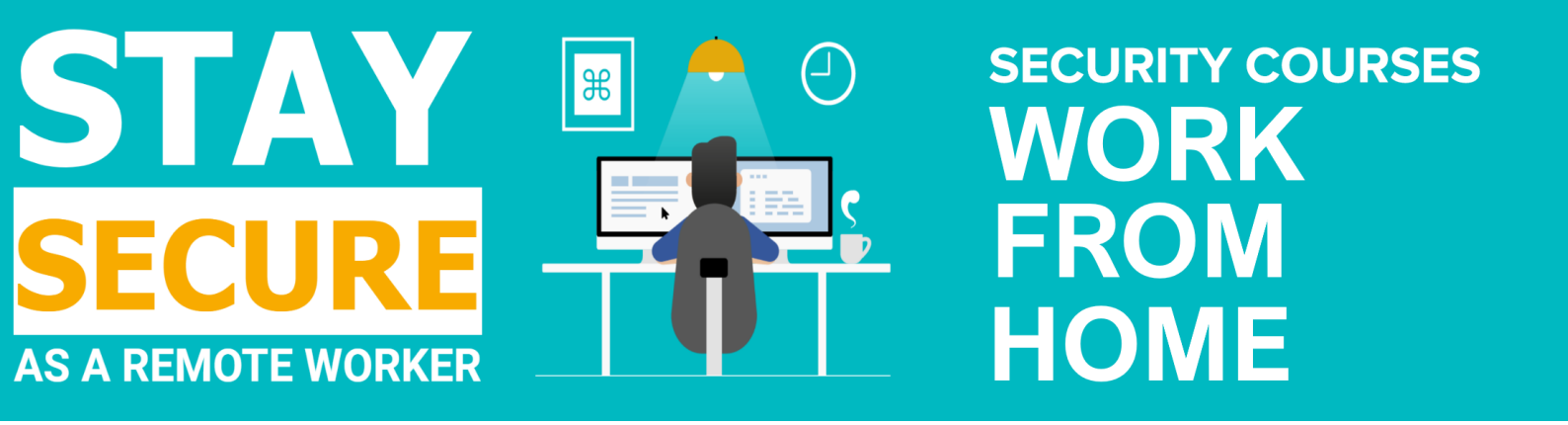
Wenn Sie außerhalb ihres Büros arbeiten, schützen Sie vertrauliche oder persönliche Informationen, die Sie verwenden oder bei sich tragen bzw. speichern. In einer öffentlichen Umgebung könnten viele Menschen böswillige Absichten haben. Wenn Sie personenbezogene Daten verlieren, kann Ihr Unternehmen für die Offenlegung geschützter Daten haftbar gemacht werden.

Öffentliche Computer sind nicht sicher. Sie sollten diese niemals verwenden, wenn es um persönliche oder vertrauliche Daten geht. Sie wissen nicht, ob auf einem öffentlichen Computer eventuell schädliche Software installiert wurde. Vermeiden Sie daher die Eingabe vertraulicher Informationen. Dies umfasst Anmelde- und Bankkontoinformationen, wie auch Sozialversicherungsnummern. Wenn Sie einen öffentlichen Computer verwenden müssen, stellen Sie sicher, dass Sie „privates Surfen" nutzen. Aktivieren Sie keine Kontrollkästchen zum Speichern oder Erinnern. Löschen Sie Ihren Browserverlauf und löschen Sie alle Downloads, bevor Sie den Browser schließen.

Sind Sie mit Ihrem Firmencomputer unterwegs oder arbeiten Sie damit zu Hause? Es besteht immer die Gefahr, dass andere Personen Zugang darauf bekommen. Verwenden Sie den dienstlich anvertrauten Computer nur für die Arbeit. Erlauben Sie niemandem, ihn zu benutzen, auch nicht Freunden und Familienmitgliedern. Selbst bei einem unbeabsichtigten Verlust von vertraulichen Daten können Sie für den Verlust haftbar gemacht werden.

SCHRITT 7: SPEICHERN SIE FIRMENDATEN NUR AUF DEM ARBEITSCOMPUTER





Es ist durchaus möglich, dass Ihr privater Computer nicht immer aktualisiert wird, nicht gescannt wird und nicht ständig ein gut abgestimmtes Antivirenprogramme ausgeführt wird. Sie sitzen in einem privaten Netzwerk nicht hinter einer Firewall mit Verschlüsselung. Wenn Sie selbst kein IT-Spezialist sind (und selbst das ist keine 100%ige Garantie!), kennen Sie wahrscheinlich nicht alle Vorsichtsmaßnahmen, die ein effizientes IT-Team auf Unternehmensebene trifft.

Möglicherweise möchten Sie Ihren Firmencomputer für persönliche Zwecke wie Online-Einkäufe, Bankgeschäfte oder zum Abrufen Ihrer E-Mails verwenden. Und möglicherweise möchten Sie Ihren privaten Computer für berufliche Aufgaben verwenden. Ein privates Gerät mit Ihrem Unternehmensnetzwerk zu verbinden, ist sehr gefährlich. Dies kann die Sicherheit Ihres gesamten Firmensystems gefährden und Sie für Verlust oder Schäden vertraulicher Daten, die auf Unternehmensservern gespeichert sind, haftbar machen.

Wenn Sie schon von Ihrem PC aus arbeiten müssen, können Sie das Risiko minimieren. Sie können Cloud-basierte Programme wie Office 365 verwenden. Über diese Dienste arbeiten Sie online, ohne Dateien oder E-Mails auf Ihr persönliches Gerät herunterzuladen oder synchronisieren zu müssen.

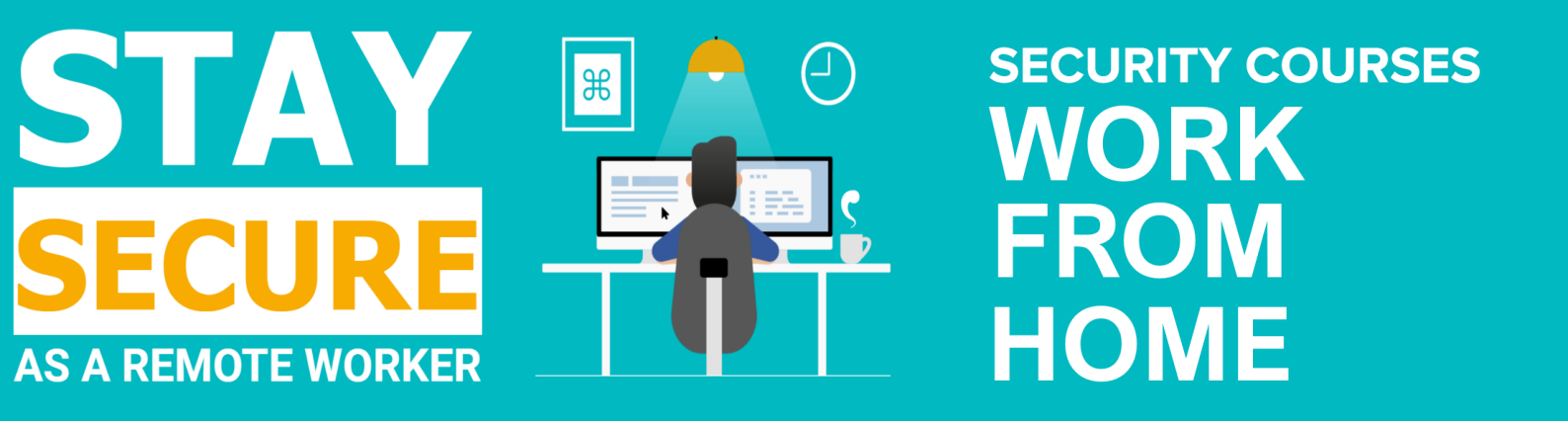
SCHRITT 8: VERMEIDEN SIE ÖFFENTLICHES WLAN

Wenn Sie von einem öffentlichen Ort aus arbeiten, ist es sehr verlockend, das öffentlich verfügbare kostenlose WLAN zu nutzen. Die Sicherheitsrisiken, die ein „einfacher“ Zugriff verursachen kann, sind jedoch groß. Ein „Zwischenfall“ wird sehr wahrscheinlich zu Problemen für Sie und Ihren Arbeitgeber führen.

Die beiden Probleme, die ein öffentliches WLAN verursacht, sind:
1) Ungeschütztes Netzwerk, das von vielen Geräten gleichzeitig gemeinsam genutzt wird
2) Ungeschützter Datenverkehr zwischen dem von Ihnen verwendeten öffentlichen WLAN und dem Netzwerk an Ihrem Arbeitsplatz.

Um den ersten Teil dieses Problems zu beheben, können Sie Ihr eigenes persönliches Wi-Fi-Netzwerk einrichten. Das ist wie ein Hotspot. Es verwendet Ihr Telefon oder ein anderes mobiles Gerät, um eine Verbindung herzustellen. Ein Hotspot verschlüsselt Ihren Datenverkehr nicht, ermöglicht es jedoch sonst niemandem im selben Netzwerk, Ihre Daten zu erfassen. Möglicherweise fällt seitens des Mobilfunkanbieters für die Einrichtung Ihres eigenen privaten Wi-Fi-Netzwerks eine Gebühr an. Die Gebühr ist jedoch unbedeutend im Vergleich zu den potenziellen Schäden, die durch die Nutzung öffentlicher drahtloser Netzwerke entstehen.

Um das zweite Problem zu umgehen, ist es eine gute Lösung, ein VPN einzurichten. Ein VPN ist ein virtuelles privates Netzwerk. Es bietet einen sicheren und verschlüsselten Kanal für Ihren Datenverkehr auf dem Weg durch das Internet. Ein VPN macht es Cyberkriminellen extrem schwer,



Ihre Daten abzufangen. Es verbirgt Ihren tatsächlichen Standort und bietet Ihnen die Online-Privatsphäre, die Sie benötigen.

Einige Länder verbieten die Verwendung von VPNs. Wenn ein VPN an Ihrem Standort legal ist, empfiehlt es sich, ein solches einzurichten, wenn Sie von öffentlichen Standorten aus arbeiten.

SCHRITT 9: VERSCHLÜSSELN SIE SENSIBLE DATEN AUF IHREM GERÄT UND IN E-MAILS

Informationen per E-Mail gesendet, sind keinesfalls sicher, es sei denn, dass sie verschlüsselt wurden. Die Verschlüsselung ist ein Prozess, der die Informationen chiffriert. Dies geschieht auf eine Weise, die das Öffnen durch Unbefugte erschwert. Wenn Sie vertrauliche Daten per E-Mail senden müssen, stellen Sie sicher, dass Sie diese zuerst verschlüsseln.

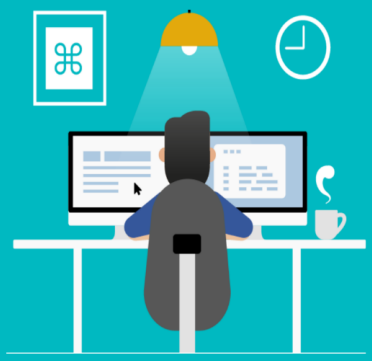
Vorsichtshalber sollten Sie immer alle gespeicherten Daten verschlüsseln, damit bei Verlust oder Diebstahl Ihres Geräts ohne Ihr Passwort oder Ihre PIN kein Zugriff auf die gespeicherten Informationen möglich ist.

SCHRITT 10: VORSICHT BEI USB-STICKS UND PORTS

Sollen Sie einen herrenlosen USB-Stick nehmen und an Ihren Computer anschließen? Bitte niemals! Das ist eine klassische Hacking-Methode, aber viele Leute fallen immer noch darauf herein.

Wenn ein USB-Stick über die Datenanschlussbuchse Ihres Computers verbunden wurde, können Ihre Daten und Ihr gesamtes Unternehmensnetzwerk gefährdet sein. Schließen Sie niemals einen gefundenen USB-Stick an.

Eine gefährliche Praxis besteht darin, Ihr Gerät über USB an einer öffentlichen Telefonladestation aufzuladen. Wenn dies Ihre einzige Lademöglichkeit ist, müssen Sie einen USB-Datenblocker verwenden. Der Datenblocker erlaubt nur die Stromübertragung des Ports und blockiert die Datenübertragung.



SCHRITT 11: LASSEN SIE NIEMALS EINEN COMPUTER ODER ANDERE GERÄTE IN EINEM FAHRZEUG, EINEM HOTELZIMMER ODER EINEM ANDEREN UNSICHEREN ORT ZURÜCK

Um den Diebstahl Ihrer Arbeitsgeräte und sensibler persönlicher und Unternehmensdaten zu verhindern, behalten Sie diese Geräte immer bei sich, wenn Sie auswärts arbeiten. Lassen sie diese nicht in Ihrem Auto, auch nicht im Kofferraum. Hotelzimmer sind auch nicht sicher, da das Hotelpersonal jederzeit darauf zugreifen könnte.