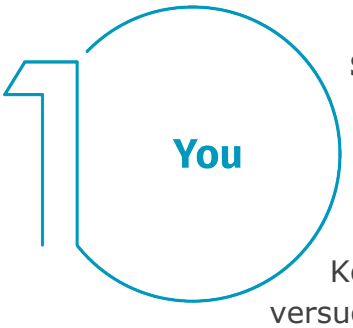
Die 5 wichtigsten Schritte für sicheres Arbeiten von Zuhause

Wir wissen, dass für einige von Ihnen das Arbeiten von zu Hause aus neu und vielleicht auch sehr fordernd ist, während Sie sich auf Ihre neue Umgebung einstellen. Wir möchten Ihnen ermöglichen, so sicher wie möglich von zu Hause aus arbeiten zu können. Unten finden Sie fünf einfache Schritte für sicheres Arbeiten. Und diese Schritte schützen nicht nur Ihre Arbeit, sondern auch Sie selbst und Ihre Familie, indem Sie ein cybersicheres Zuhause schaffen.



Sie: Zu allererst gilt, Technologie allein kann Sie nicht vollständig beschützen – Sie sind der beste Schutz. Angreifer haben gelernt, dass es am einfachsten ist, Sie anzuvisieren und nicht Ihren Computer oder andere Geräte. Wenn Sie ihr Passwort, arbeitsbezogene Daten oder die Kontrolle über Ihren Computer haben wollen, werden sie versuchen, Sie auszutricksen und erzeugen dabei oft ein Gefühl von Dringlichkeit. Beispielsweise könnten sie Sie anrufen und vorgeben, ein Mitarbeiter von Microsofts technischem Kundendienst zu sein und behaupten, Ihr Computer sei infiziert. Oder vielleicht senden sie Ihnen eine E-Mail mit einer Warnung, dass ein Paket nicht zugestellt werden konnte, sodass Sie auf einen schädlichen Link klicken. Zu den gängigsten Anzeichen eines Social-Engineering-Angriffs gehören:

- Jemand erzeugt ein Gefühl größter Dringlichkeit durch Angst, Einschüchterung, eine angebliche Krise oder einen wichtigen Termin. Cyberangreifer sind geschickt darin, überzeugende Nachrichten zu schreiben, die anscheinend von vertrauenswürdigen Organisationen wie Banken, Regierungen oder internationalen Organisationen stammen.
- Es wird Druck ausgeübt, Sicherheitsrichtlinien oder -abläufe zu umgehen oder Sie erhalten ein Angebot, das zu gut klingt, um wahr zu sein (nein, Sie haben nicht im Lotto gewonnen!).
- Eine Nachricht, scheinbar von einem Freund oder Mitarbeiter, aber die Unterschrift, der Ton oder der Wortlaut klingen nicht wie diese Person.

Letztendlich sind Sie der beste Schutz gegen diese Angriffe.

Heimnetzwerk: So gut wie jedes Heimnetzwerk beginnt mit einem kabellosen Netzwerk (oft WLAN genannt). Mit diesem Netzwerk können Sie alle Ihre Geräte mit dem Internet verbinden. Die meisten kabellosen Heimnetzwerke werden von Ihrem Internetrouter oder einem eigenen kabellosen Zugriffspunkt gesteuert. Beide funktionieren auf dieselbe Art: indem sie kabellose Signale aussenden, mit denen sich Ihre Heimgeräte verbinden. Wenn Sie also Ihr kabelloses Netzwerk schützen, schützen Sie gleichzeitig Ihr Zuhause. Dazu empfehlen wir Ihnen die folgenden Schritte:

- Ändern Sie das Standardpasswort des Geräts, mit dem Sie Ihr kabelloses Netzwerk steuern. Über das Administratorkonto können Sie die Einstellungen für Ihr kabelloses Netzwerk ändern.
- Stellen Sie sicher, dass nur vertrauenswürdige Personen sich mit Ihrem kabellosen Netzwerk verbinden können. Das können Sie machen, indem Sie starke Sicherheitsmaßnahmen aktivieren. Dadurch benötigt man ein Passwort, um sich mit Ihrem kabellosen Netzwerk zu verbinden, und sobald eine Verbindung hergestellt wurde, werden die Online-Aktivitäten verschlüsselt.
- Stellen Sie sicher, dass für die Verbindung zu Ihrem kabellosen Netzwerk ein starkes Passwort benötigt wird, das sich vom Administratorpasswort unterscheidet. Denken Sie daran, dass Sie für jedes Ihrer Geräte das Passwort nur einmal eingeben müssen, da die Passwörter gespeichert werden.

Sind Sie nicht sicher, wie Sie diese Schritte befolgen können? Wenden Sie sich an Ihren Internetanbieter, besuchen Sie seine Webseite, lesen Sie die Anleitung Ihres kabellosen Zugriffpunkts oder besuchen Sie die Webseite des Verkäufers.

Passwörter: Wenn Sie auf einer Webseite ein Passwort erstellen müssen, sollten Sie unbedingt ein starkes Passwort wählen – je mehr Zeichen, desto stärker ist es. Passphrasen zu nutzen ist der einfachste Weg, für ein starkes Passwort zu sorgen. Eine Passphrase ist ein Passwort aus mehreren Wörtern, wie zum Beispiel *„Biene Honig Bourbon.“* Passphrasen sollten einzigartig sein, das bedeutet, Sie sollten für jedes Gerät und für jedes Online-Konto eine andere verwenden. Wird dann eine Passphrase kompromittiert, sind alle anderen Konten und Geräte weiterhin sicher. Sie können sich nicht alle diese Passphrasen merken?

Verwenden Sie einen Passwortmanager. Das ist ein spezielles Programm, das alle Ihre Passphrasen in einem verschlüsselten Format speichert (und viele weitere tolle Funktionen bietet!). Zu guter Letzt sollten Sie, wenn möglich, eine Zwei-Faktor-Überprüfung aktivieren, auch Zwei-Faktor-Authentifizierung genannt. Diese verwendet Ihr Passwort, erweitert den Zugang aber durch einen zweiten Schritt, wie einen Code, der an Ihr Smartphone gesendet wird oder eine App, die den Code für Sie erstellt. Die Zwei-Faktor-Authentifizierung ist eine der wichtigsten Maßnahmen zum Schutz Ihrer Online-Konten und einfacher, als Sie möglicherweise glauben.

Updates: Stellen Sie sicher, dass alle Ihre Computer, Mobilgeräte, Programme und Apps die aktuellsten Versionen ihrer Software verwenden. Cyberangreifer sind ständig auf der Suche nach neuen Schwachstellen in der Software Ihrer Geräte. Wenn sie Schwachstellen entdecken, setzen sie besondere Programme ein, um sie auszunutzen und sich in die Geräte zu hacken, die Sie verwenden. Gleichzeitig arbeiten die Entwickler dieser Software hart daran, diese Schwachstellen mit Updates zu beheben. Indem Sie sicherstellen, dass Ihre Computer und Mobilgeräte diese Updates unverzüglich installieren, machen Sie Hackern das Leben viel schwerer. Um auf dem aktuellsten Stand zu bleiben, sollten Sie, wenn möglich, die Auto-Aktualisierung aktivieren. Das gilt für so gut wie jede Technologie, die mit einem Netzwerk verbunden ist. Dazu gehören nicht nur Ihre arbeitsbezogenen Geräte, sondern auch mit dem Internet verbundene Fernseher, Babyfone, Sicherheitskameras, Internetrouter, Spielkonsolen und sogar Ihr Auto.

Kinder/Gäste: Sie wollen sich im Büro wahrscheinlich keine Sorgen darüber machen müssen, ob Kinder, Gäste oder andere Familienmitglieder Ihren Arbeitslaptop oder andere arbeitsbezogene Geräte verwenden. Stellen Sie sicher, dass Familienmitglieder und Freunde verstehen, dass sie Ihre Arbeitsgeräte nicht verwenden dürfen, weil sie versehentlich Informationen löschen oder ändern, oder im schlimmsten Fall das Gerät infizieren könnten.