

So gewährleisten Sie die Sicherheit Ihrer Organisation im Büro und unterwegs

Ganz egal, ob Sie zu Hause oder in einem Büro arbeiten – die Sicherheit Ihrer Organisation muss für Sie Priorität haben. Obwohl sich diese beiden Orte für Sie recht unterschiedlich anfühlen können, sollten sie sowohl im Büro als auch bei der Arbeit zu Hause die gleichen Vorsichtsmaßnahmen ergreifen. Sehen wir uns einige wichtige Regeln für die Cybersicherheit an und wie diese sowohl im Büro als auch bei der Arbeit zu Hause angewendet werden können.

Nur sichere Geräte verwenden

- Denken Sie daran, dass Ihr Gerät nur so sicher ist wie die Apps, die darauf ausgeführt werden. Installieren Sie eine Anwendung oder ein Plug-in erst nach Rücksprache mit Ihrer IT-Abteilung.
- Verwenden Sie die von der Arbeit gestellten Geräte nur zur Arbeit. Wenn Sie Ihren privaten Computer für die Arbeit verwenden, empfehlen wir Ihnen, ein separates Benutzerkonto mit einem eigenen Benutzernamen und Passwort anzulegen.
- Im Büro ist wahrscheinlich Ihre IT-Abteilung für die Netzwerksicherheit zuständig. Um die Sicherheit Ihrer Internetverbindung zu Hause zu gewährleisten, sollten Sie ein komplexes Passwort für Ihren Router verwenden. Wenn Ihnen Ihre Organisation den Zugriff auf ein Virtual Private Network (VPN) ermöglicht, stellen Sie auch dazu eine Verbindung her.

Ihren physischen Arbeitsplatz schützen

- Achten Sie im Büro auf Piggybacking und Tailgating. Ein Piggybacker ist eine Person, die behauptet, zu Ihrer Organisation zu gehören und Ihnen in einen gesicherten Bereich folgt, ohne dabei einen Ausweis oder einen Zugangscode zu verwenden. Ein Tailgater hingegen ist eine Person, die darauf wartet, dass Sie einen gesicherten Bereich betreten oder verlassen und sich dann durch die noch geöffnete Tür hineinschleicht. Seien Sie unbekannten Personen gegenüber immer misstrauisch und scheuen Sie sich nicht, nach einem Ausweis zu fragen.
- Suchen Sie sich zu Hause einen privaten und bequemen Arbeitsbereich, in dem niemand während der Arbeit auf Ihren Bildschirm schauen kann. Alle sensiblen Daten müssen für Unbefugte, wie z. B. Ihre Partnerin bzw. Ihren Partner, Kinder und Freunde, unzugänglich aufbewahrt werden.
- Sperren Sie immer Ihren Computer, wenn Sie sich von Ihrem Schreibtisch entfernen! Wenn Sie Ihren Computer nicht sperren, kann jeder darüber auf sensible Daten zugreifen, Ihre Anmeldedaten entwenden oder sogar Malware installieren.

Erst denken, dann klicken!

- Klicken Sie niemals auf einen Link und laden Sie niemals einen Anhang einer E-Mail herunter, die Sie nicht erwartet haben. Selbst wenn der Absender anscheinend aus einer seriösen Organisation stammt, könnte die E-Mail-Adresse gefälscht sein.
- Wenn Sie in einer E-Mail aufgefordert werden, sich bei einem Konto oder Online-Dienst anzumelden, navigieren Sie über Ihren Browser zu diesem Dienst. Klicken Sie niemals auf den Link in der E-Mail. Wenn Sie direkt zur Website navigieren, stellen Sie sicher, dass Sie sich bei der richtigen Website und nicht bei einer nachgestellten anmelden.
- Im Zweifelsfall sollten Sie den Absender der E-Mail anrufen, um sicherzustellen, dass die Anfrage, der Link oder der Anhang echt sind. Rufen Sie nicht die in der E-Mail angegebene Telefonnummer an, da es sich um eine gefälschte Nummer handeln könnte.

