Datenschutz im **Berufsalltag**

Der Weg zur Arbeit
7:00 - 9:00 Uhr

Öffnen von E-Mails
Das Abrufen Ihrer E-Mails von Ihrem Mobiltelefon kann gefährlich sein, da Sie nicht immer den vollständigen Absender sehen können. Wenn Sie die Quelle nicht kennen, öffnen Sie die E- Mail nicht. Wenn Sie eine bösartige E-Mail vermuten, z. B. Phishing, melden Sie dies so schnell wie möglich dem IT-Support oder anhand der Schaltfläche "Phishing melden" auf Ihrem Bildschirm.

Gespräche
Achten Sie darauf, was Sie sagen und wie laut Sie sprechen. Es könnte sein, dass Sie Zuhörer haben, die sensible Details mitbekommen, die als "persönliche Daten" einzustufen sind.

Verwenden Ihres Mobilgeräts für E-Mails
Wenn Sie ein Mobilgerät verwenden, ist es nicht immer leicht, zu gewährleisten, dass E-Mail-Adressen, Inhalte und Anhänge korrekt sind, bevor Sie diese versenden. Es empfiehlt sich, dass Sie mit dem Versenden warten, bis Sie im Büro sind. Wenn es dringend ist, stellen Sie sicher, dass Sie das E-Mail-System Ihres Unternehmens verwenden.

Im Büro
9:00 - 17:00 Uhr

Downloads
Bei der Arbeit möchten Sie z. B. eine Drittanbieter-App oder einen Browser herunterladen. Alle Software-Anforderungen (Installationen und webbasierte Anwendungen) sollten zuerst vom IT-Support geprüft werden, um sicherzustellen, dass Sie keine Malware oder andere Bedrohungen herunterladen.

Versenden sicherer E-Mails aus dem Büro
Verwenden Sie nur das E-Mail-System Ihres Unternehmens, um sicherzugehen, dass E-Mails sicher gelesen und versendet werden, und dass keine Prüfungen (z. B. Virenprüfung, Malware-Screening, Aktivitätsüberwachung) umgangen werden. Befolgen Sie die IT-Sicherheitsrichtlinien Ihres Unternehmens zu Bildschirmsperren, Kennwortschutz und Verschlüsselung gespeicherter Daten.

Weitergabe persönlicher Daten
Sie möchten Daten an Dritte senden? Warten Sie damit, bis Sie sicher sind, dass Ihr Unternehmen eine Geheimhaltungsvereinbarung unterzeichnet hat. Nutzen Sie zum Versenden von Dateien und Teilen sensibler Informationen mit zugelassenen Dritten den sicheren Datentransfer.

Bereinigen oder Archivieren veralteter Dateien
Sie haben alte Dateien oder Dokumente? Archivieren oder löschen Sie diese, wenn sie nicht mehr benötigt werden. Informieren Sie sich beim IT-Support über die genehmigten lokalen Prozesse, einschl. Richtlinien zur Aufbewahrung, zum Kennzeichnen und Zerstören.

Persönliche oder sensible Daten
Stellen Sie sicher, dass persönliche oder sensible Daten geschützt sind. Teilen Sie diese nur, wenn ein wichtiger geschäftlicher Grund vorliegt.

Der Weg nach Hause
17:00 - 19:00 Uhr

Informationen unbeaufsichtigt lassen
Achten Sie darauf, dass Sie Ihren Bildschirm sperren, bevor Sie Ihren Arbeitsplatz verlassen und ihren PC oder Laptop herunterfahren, bevor Sie nach Hause gehen.

Etwas aus dem Büro mitnehmen
Wenn Sie im Home-Office arbeiten oder auf Geschäftsreise gehen, möchten Sie vielleicht Daten aus dem Büro mitnehmen, insbesondere, wenn diese sich auf Ihrem Laptop befinden. Seien Sie vorsichtig beim Umgang mit Daten, egal, von wo Sie auf diese zugreifen. Ob USB-Stick oder Ordner – sämtliche Daten sollten entsprechend den in Ihrem Unternehmen üblichen Prozessen verwaltet werden.

Vertrauliche Daten
Lassen Sie sensible oder vertrauliche Unterlagen nicht herumliegen (z. B. im Zug). Stellen Sie sicher, dass Sie diese an einem Ort aufbewahren, auf den nur Sie Zugriff haben, indem Sie sie z. B. einschließen. Wenn Sie sie nicht mehr benötigen, schreddern Sie sie oder entsorgen Sie sie in einer verschließbaren Aktenvernichtungstonne.

Online gehen
Verbinden Sie sich auf dem Heimweg im Zug nicht direkt mit ungesicherten WiFi-Netzwerken. Wenn Sie auf persönliche Daten zugreifen möchten, verwenden Sie immer ein VPN (Virtual Private Network), das Daten auch in potenziell gesicherten Netzwerken verschlüsselt.

#IchSchützeDaten