TeamViewer

Cybersicherheits-Checkliste für das Homeoffice

- [ ] **Verbinden Sie sich mit dem Unternehmensnetzwerk**, meiden Sie die Nutzung von öffentlichem WLAN und verbinden Sie sich niemals mit unbekannten Netzwerken.
- [ ] **Klicken Sie nicht auf verdächtige Links** oder Anhänge. Fragen Sie Ihre Kollegen, Ihre IT-Abteilung, oder Ihren IT-Dienstleister, falls Sie sich unsicher sind.
- [ ] **Seien Sie gegenüber Anrufen und SMS von unbekannten Nummern misstrauisch** und geben Sie vertrauliche Informationen niemals telefonisch weiter.
- [ ] **Melden** Sie jegliche Betrugversuche sofort Ihrer IT-Abteilung oder Ihrem IT-Dienstleister.
- [ ] Erstellen Sie sichere, individuelle Passwörter für jeden Login. Fragen Sie Ihren IT-Ansprechpartner, ob Sie einen **Passwort-Manager** verwenden können, falls Sie dies noch nicht tun. Verwenden Sie, wenn möglich, die **2-Faktor-Authentifizierung**.
- [ ] **Überprüfen Sie die URL** der Website, bevor Sie Ihre Anmeldedaten eingeben, und seien Sie misstrauisch, wenn Sie aufgefordert werden, Ihr Passwort zu ändern.
- [ ] **Installieren Sie keine Software oder Browser-Add-ons**, es sei denn, sie werden von Ihrem Unternehmen bereitgestellt.
- [ ] Halten Sie sich an die Unternehmensrichtlinien zur **Softwareaktualisierung** (Patching).
- [ ] **Sperren** Sie auch im Homeoffice Ihr Gerät (Tastenkombination ⊞ + L bei Windows, Cmd + Ctrl+ Q bei Mac), wenn Sie es gerade nicht benutzen. Lassen Sie Ihr Gerät unterwegs nie unbeaufsichtigt.
- [ ] **Sichern Sie Ihre Daten regelmäßig** über den Cloud-Speicher Ihres Unternehmens.
- [ ] Seien Sie vorsichtig, **welche Informationen Sie online stellen**. Cyber-Kriminelle können Ihre persönlichen Daten nutzen, um Ihnen und Ihrem Unternehmen zu schaden.

Was sind persönliche Daten?

Persönliche Daten sind Informationen, mit denen Sie als Einzelperson identifiziert werden können, z. B. Ihre E-Mail-Adresse, Ihre Adresse oder auch der Geburtsname Ihrer Mutter. Cyber-Kriminelle können diese Daten nutzen, um Ihre Identität zu stehlen, Ihre Kollegen zu täuschen oder durch Beantwortung von Sicherheitsfragen Zugang zu Ihren Konten zu erhalten.

Woher weiß ich, ob eine Website sicher ist?

- [ ] Überprüfen Sie, ob die URL mit “https” beginnt. Das “s” steht für sicher (engl. secure).
- [ ] Achten Sie auf das Schloss-Symbol (🔒) neben der URL-Leiste oben in Ihrem Browser. Wenn Sie das Symbol sehen, wurde die Website von Ihrem Browser verifiziert.
- [ ] Überprüfen Sie die URL, um sicherzustellen, dass Sie auf der richtigen Website sind. Selbst eine scheinbar sichere Website kann eine gefälschte Website sein, die einer bestimmten seriösen Seite zum Verwechseln ähnlich sieht.