



Checkliste: 10 Tipps zur Cybersicherheit

Verhaltensregeln für Mitarbeitende zur Prävention von Cyberangriffen

1. Zuerst prüfen, dann klicken

Fragen Sie sich bei eingehenden E-Mails, die einen Link oder eine Datei enthalten: Erwarte ich eine entsprechende Datei? Kenne ich den Absender?

2. Absender-Email identisch mit Namen

Seien Sie sich bewusst, dass der Absender gefälscht sein kann. Prüfen Sie, ob die E-Mail-Adresse wirklich zum angezeigten Absendernamen passt. Seien Sie misstrauisch, wenn Ihnen die Schreibweise oder der Inhalt des Mails ungewöhnlich erscheint.

3. Vorsicht bei verschlüsselten Dateien

Behandeln Sie mit Passwort verschlüsselte Dateien mit Vorsicht. Diese Methode wird oft verwendet, um die Prüfung durch den Virenschanner zu umgehen.

4. URL von Links hinterfragen

Prüfen Sie den Link: Verweist er auch wirklich dorthin, wo der Absender glaubhaft machen will? Führt der Link auf eine seriöse Website?

5. Im Zweifelsfall nachfragen

Fragen Sie im Zweifelsfall beim Absender nach, ob er Kenntnis von dieser Mail hat.

6. Dateien im Papierkorb löschen

Löschen Sie zweifelhafte Dateien oder Mails (samt Anhang) endgültig - auch aus dem Papierkorb.

7. Unbekannte Medien nicht öffnen

Öffnen Sie keine Dateien von unbekanntem Medien (z.B. Memory-Stick).

8. Tools-Download nur über Hersteller-Website

Nehmen Sie Downloads von Tools nur beim Hersteller selbst vor und nicht über Websites Dritter.

9. Unterschiedliche Passwörter nutzen

Verwenden Sie geschäftlich und privat nicht dieselben Passwörter.

10. Windows-Updates installieren

Nehmen Sie regelmässig die Windows-Updates vor. Diese enthalten unter anderem wichtige Sicherheitsaktualisierungen.

Wenn Sie unsicher sind, kontaktieren Sie im Zweifelsfall Ihre IT-Abteilung.