



# Prüfen Sie Ihr IT-Security Wissen



**Es ist in Ordnung im Café den Laptop stehen zu lassen, um an der Theke den Kaffee abzuholen.**

- A. Wahr
- B. Falsch

**Bei der Anmeldung am Firmenrechner sagt Ihnen das System, dass Sie ein neues Passwort wählen sollen. Welches Passwort ist das stärkste?**

- A. halberhahn
- B. 1M@ntaPI4tt€!!
- C. Mutti1959
- D. mEiNb3II0

**Eine E-Mail fordert Sie auf, sich über einen mitgelieferten Link bei Ihrer Bank online einzuloggen, um eine Transaktion zu überprüfen. Was würden Sie tun?**

- A. Den Link in der E-Mail benutzen, weil der Absender richtig ist.
- B. Die Banking-Website im Webbrowser eingeben und dort einloggen.
- C. Auf die E-Mail antworten und fragen was genau los ist.
- D. Den Link aus der E-Mail an Freunde senden und fragen, ob er bei ihnen funktioniert.

**Das Firmen-Smartphone wurde in einem Moment der Unachtsamkeit gestohlen. Der Vorfall muss der IT-Abteilung gemeldet werden.**

- A. Wahr
- B. Falsch

**Über das WLAN im Einkaufszentrum ist der E-Mail-Abruf sicher.**

- A. Wahr
- B. Falsch

**Ihr Unternehmen nutzt eine Vielzahl an Anwendungen mit unterschiedlichen Anmeldedaten. Wie verwalten Sie diese Zugänge?**

- A. Ein Master-Passwort für alle Zugänge verwenden.
- B. Eine Tabelle mit allen unterschiedlichen Passwörtern pflegen.
- C. Einen Passwortmanager verwenden, der die Passwörter verschlüsselt speichert.
- D. Eine Liste mit Passwörtern im eigenen Rollcontainer ablegen und diesen abschließen.

**Sie erhalten eine E-Mail von einem Anwalt, der eine Rechnung anhängt. In der E-Mail erscheint Ihre korrekte Anschrift. Wie gehen Sie damit um?**

- A. Sie löschen die Nachricht, ohne die Rechnung geprüft zu haben.
- B. Um Mahngebühren zu vermeiden, begleichen Sie die Rechnung sofort.
- C. Sie leiten die Nachricht weiter, weil es eine interne Firmenangelegenheit ist.
- D. Sie lassen einen Kollegen die Rechnung für Sie ausdrucken.

**Sie finden vor dem Firmengebäude einen USB-Stick. Was würden Sie damit tun?**

- A. Liegen lassen.
- B. Mitnehmen und am Firmenrechner anstecken.
- C. Mitnehmen und zu Hause an den Rechner stecken.
- D. Der firmeneigenen IT-Abteilung übergeben.

**Sie befinden sich im Außendienst und fordern von der Zentrale ein vertrauliches Dokument an. Wie sollte es Ihnen zugestellt werden?**

- A. Ganz normal per E-Mail. Es bleibt ja sozusagen in der Firma.
- B. Teilen über einen Clouddienst mit Passwortabfrage.
- C. Als verschlüsselter Anhang an einer E-Mail.
- D. Auf CD oder USB-Stick per Post.

**Der Administrator möchte Ihr dringendes Problem beheben und fragt Sie am Telefon nach Ihrem Passwort. Wie wäre die korrekte Verhaltensweise?**

- A. Sie geben dem Administrator das Passwort, weil Sie ihm vertrauen.
- B. Sie schreiben das Passwort auf einen Zettel und machen dann Mittagspause.
- C. Sie senden das Passwort per E-Mail, da Sie ein Sonderzeichen nicht kennen.
- D. Sie verweigern die Herausgabe Ihres Passworts.

**Es ist in Ordnung im Café den Laptop stehen zu lassen, um an der Theke den Kaffee abzuholen.**

- ▶ Lösung: B. Unbeaufsichtigte Geräte verschwinden schnell und können Ihnen und Ihrem Unternehmen großen finanziellen Schaden zufügen.

**Bei der Anmeldung am Firmenrechner sagt Ihnen das System, dass Sie ein neues Passwort wählen sollen. Welches Passwort ist das stärkste?**

- ▶ Lösung: B. Eine lange Kombination aus Groß- und Kleinbuchstaben, Zahlen und Sonderzeichen macht es automatisierten Passwortknackern deutlich schwieriger ein Passwort zu erraten.

**Eine E-Mail fordert Sie auf, sich über einen mitgelieferten Link bei Ihrer Bank online einzuloggen, um eine Transaktion zu überprüfen. Was würden Sie tun?**

- ▶ Lösung: B. In Problemfällen verweisen E-Mails von Banken auf das portaleigene Nachrichtensystem und fordern zur Überprüfung auf. Dabei werden jedoch keine Links zum Einloggen versendet.

**Das Firmen-Smartphone wurde in einem Moment der Unachtsamkeit gestohlen. Der Vorfall muss der IT-Abteilung gemeldet werden.**

- ▶ Lösung: A. Auch wenn es unangenehm ist, muss der Vorfall gemeldet werden. Nur so kann die IT-Abteilung ihre Möglichkeiten zur Datenlöschung und Gerätesperrung nutzen und einem Datenmissbrauch entgegenwirken.

**Über das WLAN im Einkaufszentrum ist der E-Mail-Abruf sicher.**

- ▶ Lösung: A. Selbst gesicherte HTTPS-Verbindungen sind dort unsicher, da nicht bekannt ist, ob das Gateway als Man-in-the-Middle fungiert und den Verbindungsaufbau manipuliert. In der Regel ist der Datenaustausch im Klartext für jeden Teilnehmer sichtbar.

**Ihr Unternehmen nutzt eine Vielzahl an Anwendungen mit unterschiedlichen Anmeldedaten. Wie verwalten Sie diese Zugänge?**

- ▶ Lösung: C. Damit sich Passwörter für viele Systeme nicht zu sehr ähneln, sollte ein Passwortmanager verwendet werden, der die am besten zufällig erzeugten Passwörter verschlüsselt speichert und mit einem eigenen sicheren Passwort schützt.

**Sie erhalten eine E-Mail von einem Anwalt, der eine Rechnung anhängt. In der E-Mail erscheint Ihre korrekte Anschrift. Wie gehen Sie damit um?**

- ▶ Lösung: A. Aus rechtlichen Gründen melden sich Anwälte immer per Briefpost. Zudem können Anschriften leicht ermittelt werden und Anhänge können Malware enthalten. Öffnen Sie daher niemals fremde Anhänge.

**Sie finden vor dem Firmengebäude einen USB-Stick. Was tun Sie damit?**

- ▶ Lösung: D. Niemals fremde Geräte anschließen, denn auf einem USB-Stick kann sich Malware befinden. Die IT-Abteilung weiß, wie damit umzugehen ist und kann ggf. den Besitzer ausfindig machen.

**Sie befinden sich im Außendienst und fordern von der Zentrale ein vertrauliches Dokument an. Wie sollte es Ihnen zugestellt werden?**

- ▶ Lösung: C. Damit das Dokument schnell übertragen und dabei nicht von Dritten gelesen werden kann, sollte es bereits vor dem Transport verschlüsselt werden.

**Der Administrator möchte Ihr dringendes Problem beheben und fragt Sie am Telefon nach Ihrem Passwort. Wie wäre die korrekte Verhaltensweise?**

- ▶ Lösung: D. Administratoren sollten nie nach Passwörtern fragen. Zudem können Sie nicht verifizieren wer wirklich am anderen Ende der Leitung sitzt. Wenn es bei einer Fehlersuche unerlässlich ist, geben Sie das Passwort im Beisein des Administrators selbst ein.