Prüfen Sie hier Ihr IT-Security Wissen

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

A Wahr	B Falsch

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 dieser Passwörter ist das stärkste?

A halberhahn	B 1M@ntaPl4tt€!!
C Mutti1959	D mEiNb3ll0

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 tun Sie?

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

Lösung: B. In Problemfällen verweisen Emails von Banken auf das Portaleigene Nachrichtensystem und fordern zur Überprüfung auf, versenden dabei jedoch keine Links zum Einloggen.

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

A Wahr	B Falsch

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

Ihr Unternehmen nutzt eine Vielzahl an Anwendungen mit unterschiedlichen Anmeldedaten. Wie gehen Sie mit den vielen Zugängen um?

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

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 eines Anwalts mit angehängter Rechnung. In der Email erscheint Ihre korrekte Anschrift. Wie gehen Sie damit um?

A Sie löschen die Nachricht, ohne in die Rechnung gesehen zu haben	**B** Sie begleichen sofort die Rechnung, um Mahngebühren zu vermeiden
C Sie leiten die Nachricht weiter, da es sich um eine interne Firmenangelegenheit handeln muss	**D** Sie lassen einen Kollegen die Rechnung für Sie ausdrucken

Lösung: A. Anwälte melden sich aus rechtlichen Gründen immer per Briefpost. Anschriften können zudem leicht ermittelt werden und Anhänge können Malware enthalten. Öffnen Sie daher nie fremde anhänge.

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

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

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?

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

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

Über das WLAN im Einkaufscenter ist der Emailabruf sicher.

A Falsch	**B** Wahr

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. Datenaustausch im Klartext ist in der Regel für jeden Teilnehmer sichtbar.

Der Administrator möchte Ihr dringendes Problem beheben und fragt am Telefon nach Ihrem Passwort. Welche 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 Mittagspause
C Sie versenden das Passwort per Email, weil Sie nicht wissen wie eines der Sonderzeichen heißt	**D** Sie verweigern die Herausgabe Ihres Passwortes

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 Problemsuche unerlässlich ist, geben Sie das Passwort im Beisein des Administrators selbst ein.