Ausbildungs-Guide

Erfolgreich ausgebildet!

#6 Checkliste: IT-Sicherheit am Arbeitsplatz

Das Projekt wird gefördert vom
Baden-Württemberg
MINISTERIUM FÜR WIRTSCHAFT, ARBEIT UND WOHNUNGSBAU

Als Auszubildende bekommt ihr, je nach Beruf, an eurem ersten Tagen im Unternehmen einen Arbeitsplatz mit PC oder Laptop zugewiesen und Du kannst evtl. zusätzlich ein Smartphone für die Arbeit nutzen. Sicherlich gibt es betriebliche Richtlinien zur Nutzung. Darin steht u.a. was beim Schreiben geschäftlicher E-Mails zu beachten ist. Aber umfasst diese Richtlinie auch die Sicherheit beim digitalen Arbeiten?

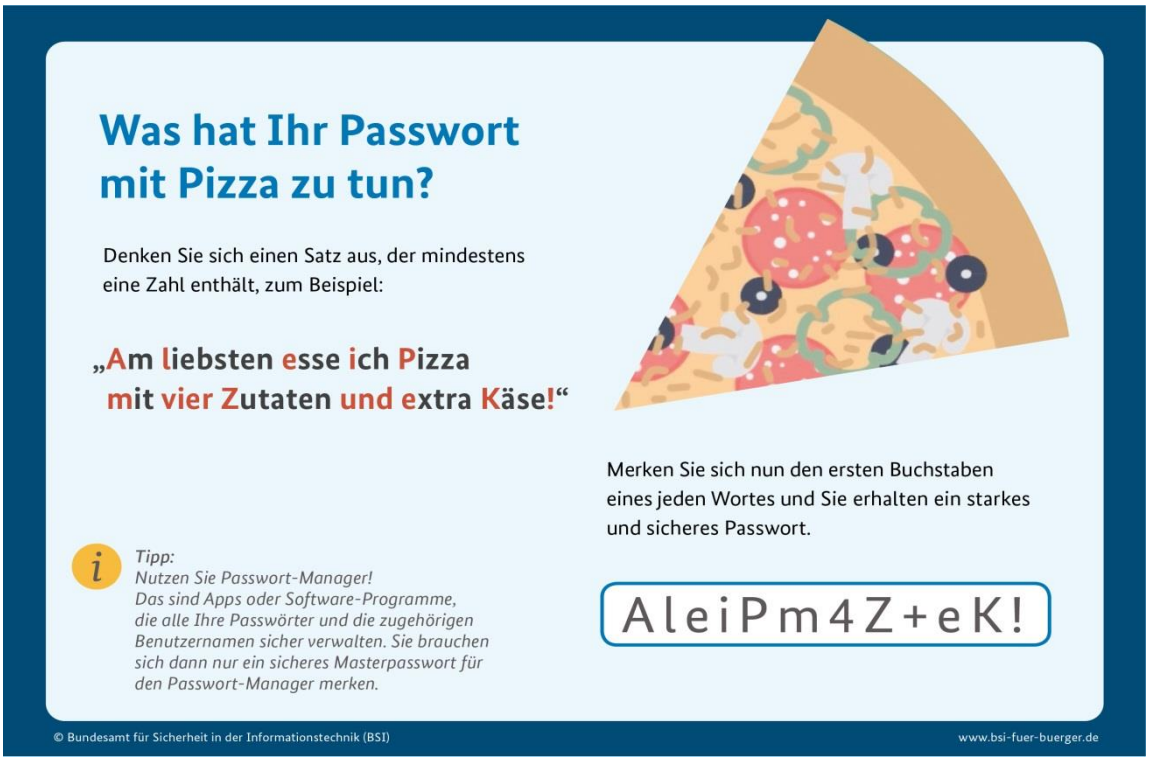
Die wichtigsten Tipps für die IT-Sicherheit am Arbeitsplatz findest du hier zusammengestellt:

E-Mails kritisch prüfen

- Bei E-Mails von externen Kontakten, aber ebenso so von Kollegen und Kolleginnen sowie der Führungsebene solltest du vorsichtig sein, da Urheber von Phishing-Mails (gefälschte E-Mails, um an persönliche Daten eines Internet-Nutzers zu gelangen und damit Identitätsdiebstahl zu begehen) seriöse Absender immer besser nachahmen.
- Damit du nicht in die Falle tappst, solltest du dir Zeit für den 3-Sekunden-Sicherheits-Check nehmen: Prüfe Absender, den Betreff und achte auf Rechtschreibfehler in der E-Mail. In unerwarteten E-Mails dürfen Anhänge keinesfalls heruntergeladen oder geöffnet werden! Um sicher zu gehen kannst Du beim Absender kurz nachfragen, ob die Mail vom ihm oder ihr stammt.
- Manche Phishing-Mails sind sehr gut gemacht. Der Absender scheint vertrauenswürdig, der Link im Text auch und das Deutsch ist korrekt. Trotzdem muss diese E-Mail nicht echt sein. Auch Absenderangaben von E-Mails lassen sich fälschen. Wenn du das - um letzte Zweifel auszuräumen - prüfen willst, musst du dir den so genannten Mail-Header anschauen. Dort steht die IP-Adresse des Absenders. Nur diese ist fälschungssicher!

Verantwortungsvoller Umgang mit Passwörtern

- Notiere dir deine Passwörter keinesfalls auf sichtbaren Zetteln oder Post-its - auch nicht an scheinbar versteckten Stellen wie z. B. unter der Tastatur.
- Sorge dafür, dass du bei der Eingabe deines Passworts nicht beobachtet wirst.
- Nutze für jedes Gerät und jede Anwendung verschiedene Passwörter und ändere sie in regelmäßigen Abständen.
- Falls du deine Passwörter selbst festlegen darfst und diese nicht durch die IT-Abteilung vorgegeben werden, wähle ein möglichst sicheres Passwort, das sich nicht leicht erraten lässt – also nicht deinen Geburtstag, 12345 oder den Namen des Haustiers.



Schutz sensibler Daten auf PC, Laptop und Co.

- Sperre den Zugriff auf deinen PC, sobald du deinen Arbeitsplatz verlässt – auch wenn du nur kurz weg bist.
- Schließe keine Wechseldatenträger unbekannter Herkunft, wie beispielsweise USB-Sticks (unbekanntes Werbegeschenk) oder DVDs, an deinem Arbeitsplatzrechner an. Es besteht die Gefahr einer Infektion mit Schadprogrammen.
- Setze keine private Hardware im Unternehmensnetz ein und speichere keine Unternehmensdaten auf privaten Datenträgern.
- Nutze nur die offiziell von der IT-Abteilung freigegebene Software auf deinen Arbeitsgeräten.
- Gib auf USB-Sticks mit Arbeitsdokumenten Acht und schütze diese ggf. ebenfalls mit einem Passwort.

Sichere Internetnutzung

- Surfe am Arbeitsplatz so wenig wie möglich privat.
- Lasse den Browser so konfigurieren, dass Pop-up-Meldungen unterdrückt werden. Wenn du unsicher bist wie das geht, frage in der IT-Abteilung oder der damit beauftragten Person nach.
- Achte auf Hinweise bei ungültigen und/oder abgelaufenen Sicherheitszertifikaten von Web-Diensten.
- Grundsätzlich solltest du mit deinen persönlichen Daten in sozialen Medien sparsam umgehen. Dies gilt umso mehr im beruflichen und betrieblichen Zusammenhang, da Internet-Betrüger auch hier nach Informationen suchen, die sie z. B. für die Gestaltung von unechten E-Mails nutzen.

Die eigene Rolle ernst nehmen

Durch bedachtes und umsichtiges Handeln kannst du einen Beitrag zum Schutz der IT-Sicherheit in deinem Betrieb oder Unternehmen leisten!

Quellenangaben/weiterführende Links:

https://www.wirausbilder.de/arbeitshilfen/checkliste-fuer-azubis-it-sicherheit-am-arbeitsplatz/ (abgerufen 12.11.2019)

https://www.bsi-fuer-buerger.de/BSIFB/DE/Service/Aktuell/Informationen/Artikel/IT_Sicherheit_am_Arbeitsplatz.html (abgerufen 12.11.2019)

https://www.sicher-im-netz.de/e-mail-co-im-beruf-sicher-nutzen (abgerufen 12.11.2019)

https://www.verbraucherzentrale.de/wissen/digitale-welt/phishingradar/merkmale-einer-phishingmail-6073 (abgerufen am 03.12.19)

https://www.bsi-fuer-buerger.de/SharedDocs/Bilder/DE/BSIFB/Aktuell/Sicheres_Passwort_passwoerter_merken_pizza.jpg?__blob=poster&v=2 (abgerufen am 03.12.19)