

IT-SICHERHEIT FÜR LEHRKRÄFTE



IT-SICHERHEIT BEDEUTET:



- Schutz von EDV-Endgeräten (Computer, Smartphones, Tablets usw.) vor unbefugten Zugriffen und Bedrohungen.
- Schutz der persönlichen und vertraulichen Daten.
- Einhaltung von IT-Vorgaben des Arbeitsgebers.
- Schutz der eigenen EDV-Technik.

SCHUTZ VOR PHISHING



Phishing (= fishing, [Passwörter angeln]) Betrüger versuchen, über gefälschte E-Mails oder Nachrichten an persönliche Daten wie Passwörter oder Bankinformationen zu gelangen.

- E-Mails und Links immer kritisch prüfen, besonders wenn sie unerwartet kommen.
- Keine persönlichen Daten weitergeben, wenn Sie dazu aufgefordert werden.
- Verwenden Sie sichere Passwörter (Erklärung siehe „Passwort-Sicherheit“).
- Aktualisieren Sie regelmäßig die Software-Updates.



SICHERES SURFEN IM INTERNET

Sicheres Surfen im Internet ist entscheidend, um die eigene Privatsphäre zu wahren und sich vor Online-Bedrohungen wie Viren und Betrug zu schützen.

Achten Sie auf:

- Eine aktuelle Software bei der Nutzung Ihres mobilen Endgerätes (Betriebssystem, Browser, Programme usw.).
- Surfen Sie online nie ohne aktuelle Antiviren-Software.
- Eine sichere Verbindung im Internet. Diese erkennen Sie in der Browserleiste an „https“ anstatt „http“.
- Keine persönliche/sensible Informationen an fragwürdige Anbieter übermitteln.

Empfehlung: In öffentlichen Netzwerken mit einem VPN surfen (VPN = Virtual Private Network).



Stärken Sie Ihr Passwort, schützen Sie Ihre Daten, surfen Sie sicher – so bleibt Ihre IT-Welt geschützt!



PASSWORT-SICHERHEIT

Ein sicheres Passwort ...

- sollte mindestens 12 Zeichen lang sein.
- sollte eine Mischung aus großen und kleinen Buchstaben, Zahlen und Sonderzeichen sein.
- sollte keine leicht zu erratenden Informationen enthalten (wie Namen, Geburtsdaten oder einfache Wörter).

Zur Passwortverwaltung ...

- kann ein Passwortmanager verwendet werden.
- gibt es Methoden wie Passkey oder 2-Faktor-Authentifizierung (2-FA oder MFA).

Verwenden Sie für jedes Konto ein eigenes und einmaliges Passwort.



GUTE UND SCHLECHTE LINKS

URL (= Uniform Resource Locator) - Adresse einer Website/-page im Internet.

Klicken Sie nur auf einen Link, wenn Sie sich sicher sind, dass dieser echt ist!

Vorsicht, wenn ...

- die Seite mit Werbung/Pop-ups überladen ist.
- die URL verkürzt ist.
- der Link mit „http“ anstatt mit „https“ beginnt.
- die Absenderquelle eine andere ist (es gibt einen Unterschied zum Ursprungslink).
- die Rechtschreibung nicht stimmt, sich Glyphen bzw. ausländische Schriftzeichen im Link verstecken (www.bildung-lsa.de wird zu www.bildung-lsα.de).



ABSICHERN DER EIGENEN TECHNIK

Auch den Schutz bei eigenen EDV-Geräten nicht vergessen. Mit diesen vier Maßnahmen schaffen Sie einen sehr guten Grundschutz für Ihre genutzte Technik:

- Halten Sie die Antiviren-Software aktuell.
- Führen Sie regelmäßig die Software- und Programm-Updates (Betriebssystem, Browser) durch.
- Aktivieren Sie die Firewall. Diese schützt den Computer, indem sie unerwünschten Netzwerkverkehr blockiert.
- Erstellen Sie ein regelmäßiges Backup.