# Cybersicherheit im Unternehmen.

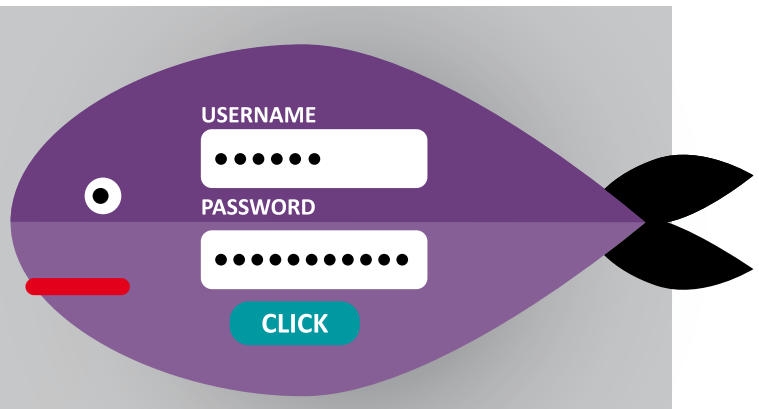
it-safe.at

WKO INFORMATION · CONSULTING

## Cybersicherheit am Arbeitsplatz

1. **Versperren** und sichern Sie **vertrauliche Dokumente**.
2. Versichern Sie sich, dass sensible Daten (zB Passwörter) vor anderen Personen **geheim bleiben**.
3. Schließen Sie **keine unbekannten Datenträger** an Ihre Geräte an.
4. Räumen Sie am Ende des Arbeitstages Ihren Arbeitsplatz auf **(Clean-Desk-Policy)**.
5. **Lassen Sie Ihren Rechner nie unbeaufsichtigt**, während Sie angemeldet sind. Sperren Sie Ihren Rechner auch, wenn Sie den Arbeitsplatz nur kurze Zeit verlassen (Tastenkombination Windows-Taste + L).
6. Befolgen Sie die **organisationsinternen Anweisungen**.
7. **Entsorgen Sie** Dokumente und Datenträger **richtig** (zB Shreddern, professionelle Entsorgung).

## Passwortsicherheit




1. Passwörter sind umso **sicherer je länger** sie sind.
2. Nutzen Sie für verschiedene Anwendungen **unterschiedliche Passwörter**.
3. Geben Sie die Passwörter nicht weiter und lassen Sie diese keinesfalls offen liegen.
4. Verwenden Sie eine Kombination aus **Groß- und Kleinbuchstaben, Ziffern und Sonderzeichen**. Vermeiden Sie Geburtstage, Jahreszahlen, Namen oder gängige Kombinationen wie 1,2,3,4, abcd oder asdf.
5. **Ändern Sie Ihre Passwörter**, wenn Sie feststellen oder vermuten, dass Unbefugte Zugriff auf Ihre Accounts haben.

**TIPP**

- Denken Sie sich einen Satz aus und benutzen Sie nur den ersten Buchstaben jedes Wortes als Passwort. (zB „Mein Schreibtisch hat vier Ecken und hat zwei Tischbeine – er quietscht entsetzlich!“: mSh4E&h2T-eqe!)
- Verwenden Sie Passwort-Manager wie KeePass.
- Verwenden Sie, wo immer es möglich ist, Zwei-Faktor-Authentifizierung für zusätzliche Sicherheit.

## E-Mails und Social Engineering

1. Überprüfen Sie, ob es sich um eine **reale E-Mailadresse/Person/ Telefonnummer** handelt.
2. Öffnen Sie **keine Verlinkungen oder Dateianhänge** in E-Mails von unbekannten Absendern.
3. Leiten Sie verdächtige E-Mails nicht weiter.
4. **Achten Sie auf Rechtschreib-, Grammatikfehler oder unübliche Grußformeln** bei E-Mails. Häufig werden E-Mails mit Schadprogrammen automatisiert erstellt und können daher Fehler beinhalten.
5. Bleiben Sie ruhig und prüfen Sie die Sachverhalte sorgfältig, wenn E-Mails „Reizworte“ („Offene Rechnung“, „Letzte Mahnung“, „Konto gesperrt“, etc.) enthalten. **Löschen Sie Phishing-Mails**, die zur Übermittlung von persönlichen Daten oder Passwörtern (zB PIN oder TAN) auffordern.

**TIPP**

Seien Sie auch abseits des Büros vorsichtig, welche Daten Sie an Fremde weitergeben.