



CYBERSECURITY-CHECK



IT-Sicherheit stärken, Risiken minimieren und das eigene Unternehmen schützen.



DIE WICHTIGSTEN CYBERSECURITY-MASSNAHMEN

- 1 Klare Zuständigkeiten festlegen**
Stellen Sie Richtlinien für den sorgfältigen Umgang mit Daten, Systemen und Zugriffsrechten für Ihr eigenes Unternehmen auf. Definieren Sie eine verantwortliche Ansprechperson für Informationssicherheit.
- 2 Mitarbeitende sensibilisieren**
Absolvieren Sie und Ihre Mitarbeiter:innen regelmäßig Pflichtschulungen und frischen Sie das Wissen über aktuelle Risiken und sicheres Verhalten kontinuierlich auf.
- 3 Zugriffsrechte einschränken**
Vergeben Sie nur jene Zugriffsrechte, die die Mitarbeiter:innen für ihre Aufgaben benötigen. Konfigurieren Sie die Geräte sicher mit nur aktivierten, notwendigen Funktionen und verwenden Sie starke Passwörter gemäß den Richtlinien.
- 4 IT-System & Netzwerke schützen**
Installieren Sie zeitnah Sicherheitsupdates und schützen Sie Ihr Netzwerk durch Firewall, Virens Scanner und Anti-Malware-Lösungen. Sorgen Sie auch für einen abgesicherten Internetauftritt.
- 5 Daten sichern**
Erstellen Sie regelmäßig Backups und prüfen Sie, ob die Wiederherstellung der Daten jederzeit zuverlässig funktioniert.
- 6 Im Notfall richtig handeln**
Definieren Sie einen Notfallplan und befolgen Sie die vorgesehenen Schritte, um bei IT-Sicherheitsvorfällen schnell und richtig zu reagieren.

Mehr Maßnahmen zur IT-Sicherheit:



HILFE, WAS SOLL ICH JETZT TUN?



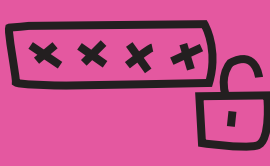
MEINE WEBSITE ZEIGT FEHLER, WERBUNG ODER IST OFFLINE

- Prüfen, ob Fehler auch auf anderen Geräten auftritt
- Hosting- und Serverzugang prüfen
- Sicherheitscheck durchführen
- Wiederherstellung der Website aus dem Backup
- Passwort ändern und Zwei-Faktor-Authentifizierung aktualisieren



ICH HABE AUF EINEN VERDÄCHTIGEN LINK GEKLICKT

- Gerät sofort vom Internet trennen
- Nach Schadsoftware prüfen und gefundene Bedrohungen entfernen
- Passwort ändern und Zwei-Faktor-Authentifizierung aktualisieren
- Verdächtige Aktivitäten überprüfen und melden
- Aufmerksamkeit in den nächsten Tagen erhöhen und ggf. IT informieren



MEIN SOCIAL-MEDIA-PASSWORT WURDE GEHACKT

- Passwort ändern und Zwei-Faktor-Authentifizierung aktualisieren
- Verknüpfte Geräte und Apps überprüfen, ggf. entfernen
- Kontaktinformationen auf Fehler überprüfen
- Letzte Aktivitäten prüfen und Kontakte informieren



MEIN ONLINE-BANKING ZEIGT UNBEKANNTE TRANSAKTIONEN

- Bank sofort informieren und Konto sperren
- Passwort ändern und Zwei-Faktor-Authentifizierung aktualisieren
- Nach Schadsoftware prüfen und gefundene Bedrohungen entfernen
- E-Mails auf verdächtige Nachrichten kontrollieren
- Anzeige erstatten



MEIN E-MAIL-POSTEINGANG WURDE GEHACKT

- Passwort für Email-Posteingang ändern und Zwei-Faktor-Authentifizierung aktualisieren
- Weiterleitungen und Regeln prüfen
- Passwörter bei Banken, Social Media etc. ändern
- Letzte Aktivitäten prüfen und Kontakte informieren

Cyber-Security-Hotline:



TYPISCHE ANZEICHEN FÜR PHISHING

- Absender wirkt seriös, hat aber kleine Unstimmigkeiten**
Schreibfehler oder unbekannte Adresse etwa support@musterfirma-security.com statt richtig support@musterfirma.com
- Starker Zeitdruck**
durch Fristen, Drohungen: „Handeln Sie sofort“ oder „Konto wird gesperrt“
- Anforderung sensibler Daten**
die seriöse Unternehmen nie per E-Mail erfragen (Passwörter, Zahlungsdaten, Ausweise)
- Link leitet auf fast identische, aber gefälschte Domain**
- Unpersönliche oder untypische Anrede**
trotz professionellem Layout
- Behauptete Probleme ohne vorherige Hinweise**
angebliche Sicherheitsvorfälle, Zahlungsfehler
- Unerwartete Anhänge oder Links**

Sofortmaßnahmen – jetzt handeln

- 1 Nichts anklicken oder öffnen – keine Links, keine Anhänge, nicht antworten; die Mail nicht weiterverarbeiten.
- 2 IT oder Sicherheitsverantwortliche informieren und den Vorfall über die internen Meldewege melden.
- 3 Mail löschen oder in Quarantäne verschieben und – falls etwas angeklickt wurde – sofort Passwörter ändern.

GLOSSAR

Anti-Malware / Virens Scanner

Software, die Geräte vor schädlichen Programmen schützt, indem sie diese erkennt und entfernt.

Backup / Datensicherung

Regelmäßige Sicherung wichtiger Daten zur Wiederherstellung im Notfall.

Bedrohungserkennung (Threat Detection)

Erkennen ungewöhnlicher Aktivitäten oder Angriffe, um Schäden früh zu verhindern.

Firewall

Filtert Netzwerkverkehr und blockiert unerlaubte Zugriffe.

Netzwerksicherheit

Maßnahmen zum Schutz von Computern und Netzwerken vor Angriffen.

Passwort-Richtlinie

Regeln für starke, regelmäßig erneuerte Passwörter.

Phishing

Betrugsnachrichten, die sensible Daten erschleichen sollen.

Social Engineering

Manipulation von Personen, um vertrauliche Informationen zu erlangen.

Zugriffsrechte (Access Control)

Bestimmen, welche Personen auf welche Dateien oder Programme notwendigerweise zugreifen dürfen.

Zwei-Faktor-Authentifizierung (2FA)

Sicherheitsverfahren, bei dem zusätzlich zum Passwort ein zweites Element (z. B. SMS-Code) eingegeben werden muss, um Zugriff zu erhalten.