

FANZIT

IT-AWARENESS-MONAT OKTOBER 2025



BITAL®
SYSTEM

Bital System GmbH
Weilimdorfer Str. 76
70839 Gerlingen

+ 49 7156 / 35 99 - 390
info@bital.de
www.bital.de

Der Oktober stand ganz im Zeichen der **IT- und Cybersicherheits-Awareness**. Er bot geballte Praxis-Tipps, Challenges und konkrete Maßnahmen, die Sie und Ihr Unternehmen sofort umsetzen können.

Das Ziel: Sensibilisierung gegen Gefahren wie Phishing, Social Engineering und schwache Passwörter, denn der Mensch bleibt die größte Schwachstelle – und zugleich die stärkste Verteidigung!

HOW-TO'S

- › E-Mails prüfen, bevor Sie klicken (Absender, Links, Anhänge).
- › Passwörter: mind. 12-16 Zeichen, einzigartig, 2FA aktivieren.
- › Privatsphäre-Einstellungen regelmäßig prüfen.
- › Geräte-Check: Updates, Backups, VPN, Bildschirmsperre.
- › Backups testen und Wiederherstellungsabläufe kennen.
- › Verdächtige Mails immer an IT/Sicherheitsverantwortliche melden.

QUICK-RESPONSE IM ERNSTFALL

- 1 Betroffene Systeme isolieren.
- 2 IT/Sicherheitsverantwortliche informieren.
- 3 Interne Kommunikation ohne Panik.
- 4 Alle Beobachtungen dokumentieren.
- 5 Forensik & Wiederherstellung starten.
- 6 Learnings ziehen & Prozesse verbessern.

WISSENS-CHECK

Was sind typische Erkennungsmerkmale einer Phishing-Mail?

Falsche Absenderadresse, Zeitdruck, generische Anrede, gefälschte Links.

Was ist die wichtigste Maßnahme gegen Phishing?

Details prüfen und verdächtige Mails an die IT-Abteilung weiterleiten.

Welche Regeln gelten für sichere Passwörter?

Mindestens 12-16 Zeichen, komplexe Zeichenkombination, keine Mehrfachverwendung, regelmäßige Erneuerung, 2-Faktor-Authentifizierung.

Wie sollte man seine Privatsphäre-Einstellungen prüfen?

Sichtbarkeit von Beiträgen, App-Zugriffe, Nutzung von 2FA für sensible Konten.

Was sind die ersten Schritte bei einem Cyberangriff?

Sofort reagieren, IT informieren, dokumentieren, professionelle Hilfe aufsuchen.

Welche Grundsätze gelten für IT-Sicherheit im Homeoffice?

Updates durchführen, VPN nutzen, starke Passwörter, Backup einrichten, Geräte sperren.

Wer ist im Unternehmen für IT-Sicherheit verantwortlich?

IT-Sicherheit beginnt beim einzelnen Mitarbeitenden, wird aber von der Unternehmensführung vorgelebt und gesteuert.