60 Anos Setronix desde 1966

OKTOBER
2026
2. MONATSHÄLFTE | PRÄVENTION



CYBERSICHERHEIT
STOPPEN UND PRÜFEN

Auch eine dringende Nachricht muss geprüft werden.

1. Gefahren und Risiken

Gefahren: Gefälschte Nachrichten, verdächtige Anhänge und Links.

Risiken: Datendiebstahl, Betrug und unbefugter Kontozugriff.

2. Vor Arbeitsbeginn

- Prüfen Sie die vollständige Absenderadresse.
- Bestätigen Sie Anfragen über einen bekannten Kontakt.
- Nutzen Sie nur freigegebene Anwendungen und Kanäle.

3. Stoppen und melden

- Anfragen nach Passwort oder Zugangscode.
- Zeitdruck, Geheimhaltung oder geänderte Bankdaten.
- Schon geklickt oder Daten gesendet? Sofort melden.

4. So handeln Sie: vier Schritte zur Prävention

1 

Lesen
Absender und Kontext prüfen.

2 

Bestätigen
Unabhängigen Kontakt nutzen.

3 

Schützen
Keine Zugangsdaten oder Codes weitergeben.

4 

Melden
Den vorgesehenen internen Meldeweg nutzen.

5. Die passende Schutzmaßnahme wählen

Situation	Schutzmaßnahme
E-Mail / SMS	Anhänge und Links erst öffnen, wenn die Herkunft bestätigt ist.
Zahlungsaufforderung	Änderungen über einen anderen bekannten Kanal bestätigen.
Konten / Zugangsdaten	Für jedes Konto ein eigenes Passwort; MFA nutzen, falls verfügbar.
Möglicher Vorfall	Nachricht aufbewahren; Anweisungen des IT-Supports befolgen.

Gute Praxis: Verlassen Sie sich nicht nur auf den angezeigten Namen oder das Aussehen der Nachricht. Multi-Faktor-Authentifizierung (MFA) erhöht den Schutz; geben Sie die Codes nie weiter.

6. AKTION DER MONATSHÄLFTE Prüfen Sie bei unerwarteten Nachrichten vor dem Klicken die Herkunft. Klären Sie den internen Meldeweg für Verdachtsfälle.

LESEN • BESTÄTIGEN • SCHÜTZEN • MELDEN

CNCS: gute Praxis CNCS: Passwörter