Sieben goldene Regeln gegen Social Engineering

Sei auf der Hut vor bösartigen E-Mail-Anhängen

- Ignoriere Anhänge bei unangeforderten E-Mails von unbekannten Absendern
- Öffne nur bekannte, unschädliche Dateiarten
- Frage im Zweifel beim Absender nach oder lasse die E-Mail von der IT prüfen
- Halte den Webbrowser aktuell und installiere Erweiterungen mit Bedacht

Erkenne Phishing-Versuche

- Sei skeptisch gegenüber der E-Mail-Absender-Angabe
- Enthülle die tatsächliche URL von Links in E-Mails durch Überfahren mit der Maus
- Gib die URL direkt im Browser ein statt Links aus E-Mails zu folgen

Wähle einzigartige Kennwörter

- Verwende einmalige, lange, komplexe Kennwörter: zufällig generierte Zeichenketten, Passwortsätze, Diceware, mnemonische Passwörter
- Nutze eine Passwort-Management-Software
- Wähle, wenn angeboten, eine Mehrfaktor-Authentifikation

Behalte die Kontrolle am Telefon

- Sei skeptisch gegenüber Telefonnummern von Anrufern oder SMS-Absendern
- Mache dir den Vertraulichkeitsgrad von Informationen bewusst, ehe du sie am Telefon kommunizierst
- Halte im Zweifel Rücksprache und rufe zurück
- Notiere eine Gedankenstütze, um freundlich Nein zu sagen

Schütze dich in fremden WLANs

- Nutze in fremden WLANs das Unternehmens-VPN
- Achte auf HTTPS (Schloss-Symbol)
- Nimm alle Warnmeldungen ernst

Sei vorsichtig mit mobilen Datenträgern

- Schließe nur organisationseigene USB-Sticks an
- Speichere sensible Daten nur verschlüsselt
- Achte bei Smartphones darauf: Telefon verschlüsseln, Bildschirm sperren, Mitlesen verhindern
- Wirke auch dem Verlust analoger mobiler Datenträger (Papier) entgegen

Durchschaue Trickbetrüger

- Sei dir über die Identität deines Kommunikationspartners sicher
- Sei unempfänglich für Versuche dich unter Zeitdruck zu setzen
- Wähle einen zweiten Kanal für Rückfragen
- Halte dich an etablierte Prozesse

aramido GmbH
Beratung für Informationssicherheit
Durlacher Allee 75 - 77
76131 Karlsruhe

ÖFFENTLICH
+49 721 451 991 0
info@aramido.de
https://aramido.de