Leitfaden: So schützen Sie sich vor Phishing-E-Mails

Phishing ist der Versuch, über gefälschte E-Mails oder Webseiten an persönliche Daten wie Passwörter, Kreditkarteninformationen oder Zugangsdaten zu gelangen. Ziel ist es, diese Daten betrügerisch zu nutzen.

Erkennungsmerkmale einer Phishing-E-Mail

- Verdächtige Absenderadresse – weicht leicht vom echten Absender ab (z. B. info@paypall.com statt paypal.com)
- Allgemeine Anrede – kein persönlicher Name: „Sehr geehrter Kunde“ statt „Herr Mustermann“
- Druck und Dringlichkeit – „Handeln Sie sofort!“ ist eine typische Masche
- Ungewöhnliche Links – mit der Maus über den Link fahren, um die echte Zieladresse zu sehen
- Rechtschreib- oder Grammatikfehler – häufige Anzeichen für unseriöse Inhalte
- Anhänge oder Aufforderung zur Eingabe sensibler Daten – niemals Passwörter oder Bankdaten weitergeben

So verhalten Sie sich richtig

- Links nicht anklicken, wenn Sie sich nicht sicher sind
- Keine Anhänge öffnen, wenn der Absender unbekannt ist
- Absender direkt kontaktieren, wenn die Mail ungewöhnlich erscheint
- Kritisch bleiben, auch wenn das Design professionell wirkt
- Verdächtige E-Mails sofort löschen oder an die IT-Abteilung weiterleiten

Technische Schutzmaßnahmen

- Virenschutzprogramme und Firewalls nutzen
- Regelmäßige Updates für Betriebssystem und Programme
- Anti-Phishing-Filter im E-Mail-Programm aktivieren
- Zwei-Faktor-Authentifizierung für wichtige Konten verwenden

Im Ernstfall: Was tun bei Phishing-Verdacht?

- Nicht reagieren, nichts anklicken oder herunterladen
- E-Mail an die IT oder Sicherheitsbeauftragte weiterleiten
- Zugangsdaten ändern, falls versehentlich eingegeben
- Vorfall melden (z. B. bei der Polizei oder Watchlist Internet)