Vorsicht vor Email Phishing!

So schützt Du Dich vor betrügerischen E-Mails und anderen Gefahren im digitalen Arbeitsalltag

Ein Merkblatt für alle Mitarbeitenden der Bolz Entsorgung GmbH

□□ Was ist eigentlich Phishing?

Phishing ist ein Trickbetrug – Kriminelle versuchen, Dich mit gefälschten E-Mails, Links oder Anhängen dazu zu bringen, vertrauliche Daten preiszugeben oder auf schädliche Inhalte zu klicken.

Ziele sind oft:

- Die Zugangsdaten zu Deinem E-Mail- oder Firmenkonto
- Zugang zu internen Systemen
- Infektion Deines PCs mit Viren oder Trojanern

□□ Wie erkennst Du eine Phishing-Mail?

Einfache Checkliste

□□ 1. Wer ist der Absender?

- Kommt die Mail von einer komischen Adresse wie `sicherheits-check@micr0soft.net`?
- Ist der Name vertraut, aber die Adresse passt nicht dazu?

> **Beispiel:** Du bekommst scheinbar eine Mail vom Chef, aber die Absenderadresse endet auf `@gmail.com`.

□□ 2. Was steht im Betreff und Text?

- Klingt es bedrohlich oder besonders dringend?

> *„Letzte Warnung: Ihr Konto wird gesperrt!“*

- Wird Druck aufgebaut?

> *„Sie haben nur 24 Stunden Zeit!“*

- Ist die Sprache ungewohnt oder fehlerhaft?

> *„Sehr geehrte Benutzer, Ihre wichtig Postfach ist voll!“*

□□ 3. Wohin führen Links?

- Gehe **nie direkt** auf Links in verdächtigen E-Mails.
- Fahre mit der Maus über den Link (nicht klicken!) und prüfe, wohin er führt.

> **Beispiel:** Statt `www.dhl.de` steht da plötzlich `www.dhl-paket-verlust.ru`.

□□ 4. Was für Anhänge sind dabei?

Öffne **keine Anhänge**, wenn:

- Du sie nicht erwartest
- Die Datei eine seltsame Endung hat:
  `.exe`, `.zip`, `.html`, `.js`, `.bat`

□□ Praxisbeispiele

□□ Beispiel 1 – Gefälschte IT-Wartung

- **Absender:** `support@firma-sicherheitsdienst.de`
- **Betreff:** *„Dringend: Passwort läuft ab!“*
- **Text:** *„Bitte bestätigen Sie hier Ihre Zugangsdaten.“*
  □ **Richtiges Verhalten:** Nicht klicken! Weiterleiten an IT, dann löschen.

□□ Beispiel 2 – Paketbetrug

- **Betreff:** *„Ihr Paket konnte nicht zugestellt werden“*
- **Anhang:** `Sendungsverfolgung_DHL.html`
  □ **Richtiges Verhalten:** Nicht öffnen! Du wartest ja gar nicht auf ein Paket.

□□ Beispiel 3 – Chef-Mail mit ungewöhnlicher Bitte

> *„Hallo, kannst Du mir schnell Amazon-Gutscheine besorgen? Ich brauche sie dringend für eine Besprechung.“*

□ **Richtiges Verhalten:** Immer persönlich oder telefonisch rückfragen, **nicht antworten!**

□ Was kannst Du tun, um sicher zu bleiben?

- □□ **Bleib wachsam.** Wenn Dir eine Mail komisch vorkommt – lieber einmal zu viel nachfragen.
- □□ **Klicke nie auf Links oder Anhänge,** wenn Du Dir nicht sicher bist.
- □□ **Weiterleiten statt reagieren:**
  Verdächtige Mails sofort an `it@bolz-entsorgung.de` weiterleiten.
- □□ Danach: Mail löschen.
- □□ **Passwörter sind vertraulich.** Gib sie niemals weiter – auch nicht auf Nachfrage per E-Mail oder Telefon!
- □□ **Zweifel?** Ruf uns an!
  IT-Abteilung: Durchwahl **284**

□□ Deine Sicherheits-Checkliste für jeden Tag

- □□ PC sperren bei Verlassen (`Strg + Alt + Ende` → `Eingabetaste`)
- □□ Updates nie ignorieren
- □□ Keine USB-Sticks anschließen
- □□ Keine privaten Dateien oder Programme auf dem Firmen-PC
- □□ Passwörter nicht aufschreiben oder weitergeben

□□ Merksatz

> □□ Wenn Du unsicher bist:
> **Nicht klicken, nicht antworten – weiterleiten, dann löschen!**

Du bist ein wichtiger Teil der IT-Sicherheit bei Bolz Entsorgung! □□

Version #3
Erstellt: 2025-07-08 09:30:52 UTC von Frank Dengel
Zuletzt aktualisiert: 2025-07-24 12:17:39 UTC von Frank Dengel