Phishing-Mails: Betrüger-Mails erkennen und richtig handeln

Was ist Phishing?

Phishing ist eine weit verbreitete Betrugsmasche, bei der sich Kriminelle als vertraute Organisationen ausgeben, um dich über gefälschte E-Mails oder Websites zur Preisgabe sensibler Daten zu bewegen – etwa Passwörter, Bank- oder Kreditkartendaten. Dabei setzen sie auf psychologischen Druck wie Dringlichkeit oder Warnungen und locken dich über gefälschte Links oder infizierte Anhänge zu unüberlegten Handlungen.

Das Hauptziel ist immer gleich: Dich zu einer unüberlegten Handlung zu bewegen, die den Kriminellen Zugriff auf deine Daten, Konten oder Geräte ermöglicht.

Typische Phishing-Methoden

- Gefälschte Identitäten – z. B. angebliche Banken oder Paketdienste
- Links zu täuschend echten Fake-Webseiten
- Dateianhänge, die Schadsoftware enthalten können
- Druck und Panikmache, um dich zum schnellen Handeln zu bewegen

So schützt du dich dauerhaft

✅	Nutze starke und einzigartige Passwörter.
✅	Aktiviere die Zwei-Faktor-Authentifizierung (2FA), wo möglich.
✅	Halte Betriebssystem, Browser und Programme aktuell.
✅	Verwende Spam-Filter und Antiviren-Software.
✅	Sei grundsätzlich skeptisch bei unerwarteten E-Mails.

Woran du eine Phishing-Mail erkennst:

Achte auf folgende Hinweise – je mehr Merkmale zutreffen, desto wahrscheinlicher ist es, dass es sich um eine Phishing-Mail handelt:

Verdächtige Absenderadresse	• Vertauschte oder zusätzliche Buchstaben („amazonn-support“) • Ersetzte Buchstaben durch Zahlen („supp0rt“) • Falsche Domain-Endungen („@amazon-secure.info“ statt „@amazon.de“)
Allgemeine oder unpersönliche Anrede	• Standardanreden wie „Sehr geehrter Kunde“ oder „Sehr geehrter Nutzer“ • Fehlende Anrede oder einer sehr allgemeinen Anrede „Hallo“
Dringlichkeit oder Drohungen	• „Ihr Konto wird gesperrt, wenn Sie nicht sofort handeln.“ • „Letzte Warnung!“ • „Sie müssen innerhalb von 24 Stunden reagieren.“
Unerwartete Anhänge oder Links	• ZIP-, EXE- oder ISO-Dateien • Word- oder Excel-Dokumente mit Makros • PDF-Dateien, die zum Klick auf externe Inhalte auffordern
Rechtschreib- oder Grammatikfehler	• „Ihr Konto wird werd gesperrt wenn Sie nicht sofort bestätigen.“ • „Bitte klicken Sie auf der unten stehende Link für verifizieren Ihre Daten.“ • „Wir haben ein Sicherheitsproblem erkannt, bitte folgen die Schritte zur Aktualisierung.“
Aufforderung zur Eingabe sensibler Daten	• Passwörtern • TANs • Kreditkartendaten
Ungewöhnliches Layout oder Logoabweichungen	• Logos in schlechter Qualität • ungewohnte Farben oder Schriftarten • unprofessionelle Formatierung

Schritt-für-Schritt-Anleitung bei Verdacht auf Phishing

Wenn dir eine Mail merkwürdig vorkommt:

1. **Ruhe bewahren:**
   - Nicht reagieren, nicht klicken, nichts öffnen.
2. **Absender prüfen:**
   - Mauszeiger auf die Absenderadresse halten (ohne zu klicken!).
   - Passt die Domain zum echten Unternehmen?
3. **Links kontrollieren:**
   - Mit Mauszeiger über den Link fahren – stimmt die Adresse mit dem sichtbaren Text überein?
   - Keine Kurzlinks (bit.ly, tinyurl) öffnen.
4. **Inhalt hinterfragen**
   - Hast du eine solche Nachricht erwartet?
   - Passt die Nachricht zu deinen Aktivitäten (z. B. keine Bestellung aufgegeben)?
5. **Anhänge nicht öffnen**
   - Insbesondere ZIP, EXE oder Word-Dateien mit Makros.
6. **Vergleich mit echten Nachrichten**
   - Im Kundenkonto des Anbieters nachsehen (direkt im Browser selbst eingeben!).
   - Unternehmen kontaktieren – aber niemals über Kontaktdaten aus der verdächtigen Mail.
7. **Spam/Phishing melden**
   - Über die Meldefunktion deines Mailprogramms.
   - Alternativ an die IT-Abteilung (bei Firmen) oder an die Verbraucherzentrale.
8. **Nachricht löschen**
   - Wenn der Verdacht bestätigt ist.

Was tun, wenn du doch geklickt hast?

- Wenn betroffen: Konto oder Karten beim Anbieter sperren lassen.
- Sofort Passwörter ändern (insbesondere bei E-Mail, Banken, Shops).
- Computer mit Antivirus prüfen.
- Vorfall melden (Unternehmen, Arbeitgebersupport, Polizei bei Schaden).