Wenn ihr euch Sorgen wegen Phishing-E-Mails macht oder einfach sicherer im Netz unterwegs sein möchtest, dann zeigen die TeBo's euch hier, wie ihr verdächtige E-Mails erkennt eure Konten schützen könnt.

Phishing ist eine Form des Online-Betrugs, bei der Betrüger versuchen, über gefälschte Nachrichten persönliche Daten wie Passwörter, Kreditkartennummern oder andere sensible Informationen zu erlangen. Phishing-E-Mails oder -Nachrichten wirken oft so, als kämen sie von bekannten Unternehmen oder Personen und setzen den Empfänger unter Druck, schnell zu reagieren. Das Ziel ist es, das Vertrauen der Empfänger zu gewinnen, um sie dazu zu bringen, auf Links zu klicken oder persönliche Daten preiszugeben.

Phishing-E-Mails erkennen

Phishing-E-Mails sehen oft aus wie ganz normale Nachrichten von Kollegen oder bekannten Unternehmen. Hier sind einige typische Merkmale, an denen ihr verdächtige E-Mails erkennen und entsprechend reagieren könnt:

1. **Verdächtiger Absender**
   Überprüft die E-Mail-Adresse des Absenders sorgfältig. Phishing-E-Mails stammen oft von Adressen, die leicht abgeändert oder falsch geschrieben sind.
   Hinweis für mobile Nutzer: Auf mobilen Geräten kann der Header über die „Details" oder „Mehr Optionen"-Funktion in deinem E-Mail-Programm angezeigt werden. Je nach Programm sind die Schritte unterschiedlich, daher ist es hilfreich, in den App-Einstellungen nach der „Header anzeigen"-Option zu suchen.
2. **Ungewöhnliche Sprache oder Fremdsprache**
   Ein weiteres Warnsignal ist die Sprache. Wenn ihr normalerweise deutschsprachige E-Mails von einem Unternehmen erhaltet, aber plötzlich eine Nachricht in Englisch oder einer anderen Fremdsprache bekommt, dann kann das ein Hinweis auf Phishing sein.
3. **Beunruhigende oder vage Sprache**
   Allgemeine oder dringende Nachrichten wie „Dein Konto wird deaktiviert" sind oft Anzeichen für Phishing. Seriöse Unternehmen sprechen euch in der Regel persönlich an und beziehen sich auf konkrete Details.
4. **Grammatik- und Rechtschreibfehler**
   Tippfehler oder schlechte Grammatik sind oft ein Warnsignal. Seriöse Unternehmen achten auf eine einwandfreie Kommunikation.
5. **Verdächtige Links und Anhänge**
   Haltet den Mauszeiger über Links, um die URL zu überprüfen. Klickt nicht auf unbekannte Links und ladet keine verdächtigen Anhänge herunter.
   Tipp für mobile Nutzer: Auf mobilen Geräten ist es schwieriger, URLs zu überprüfen, da es keine einfache Möglichkeit gibt, über den Link zu fahren. Haltet stattdessen den Link gedrückt, um eine Vorschau der URL zu sehen, bevor ihr ihn öffnet. So könnt ihr sehen, wohin der Link führt, ohne direkt darauf zuzugreifen. Seid bei unbekannten Links oder Anhängen stets vorsichtig, da sie ein Sicherheitsrisiko darstellen können.
6. **Aufforderungen zu persönlichen Angaben**
   Wenn eine E-Mail nach Passwörtern oder Zahlungsinformationen fragt, ist Vorsicht geboten. Seriöse Unternehmen werden solche sensiblen Daten nicht per E-Mail anfordern.

Wie ihr an dieser Liste schon seht, ist die frühe Erkennung von Phishing mit dem richtigen Blick und mithilfe von einigen Tipps gar nicht so kompliziert. Vor allem, weil viele Betrüger nicht auf die Qualität der E-Mails setzen, sondern auf die reine Quantität der E-Mails, die sie verschicken. Total verlassen könnt ihr euch auf euren eigenen Sinn für Phishing aber natürlich trotzdem nicht immer. Deshalb ist es wichtig, sich einmal anzuschauen, wie eine Phishing-E-Mail in der Praxis eigentlich konkret aussehen kann.

Was tun, wenn ihr Phishing vermutet

Wenn ihr denkt, dass eine E-Mail ein Phishing-Versuch ist, könnt ihr Folgendes tun:

- **Nicht klicken und nichts herunterladen**
  Öffnet keine Links und ladet keine Anhänge herunter.
- **Absender prüfen**
  Besucht die offizielle Website des Unternehmens und nutzt deren Kontaktinformationen, um die Echtheit der E-Mail zu überprüfen.
- **Bei unerwarteten Rechnungen**
  Meldet euch direkt in eurem Konto an und geht zum Abrechnungsbereich, um dort nach offenen Rechnungen zu suchen.
  So stellt ihr sicher, dass alle Zahlungsinformationen direkt aus eurem Konto stammen.
- **E-Mail melden**
  Markiert die E-Mail als Spam. Das hilft, ähnliche E-Mails in Zukunft zu blockieren.