Hilfe, ich habe eine betrügerische E-Mail erhalten!

Was ist eine betrügerische E-Mail?

Betrügerische E-Mails erwecken den Eindruck, dass sie von einem bekannten Unternehmen (z.B. von limango) an dich gesendet wurden. Urheber von betrügerischen E-Mails haben die Absicht, deine Daten, wie z.B. Kreditkartennummern oder Passwörter für Konten, dazu zu verwenden, Identitätsdiebstahl zu begehen.

Wie kann ich mich vor betrügerischen E-Mails/Websites schützen.

Betrügerische oder "Phishing"-E-Mails sehen häufig täuschend echt aus. Nicht jede betrügerische E-Mail ist gleich und diese E-Mails werden immer professioneller, was die Identifikation als solche erschwert.

Folgend haben wir Anhaltspunkte zusammengefasst, die sowohl einzeln oder in Kombination auftreten können und damit als betrügerische E-Mail identifiziert werden können.

1. **E-Mail-Adresse des Absenders:** Die Zeile "Von" ist meistens eine offiziell aussehende E-Mail-Adresse, die möglicherweise tatsächlich aus einer echten E-Mail kopiert wurde. E-Mail-Adressen können jedoch leicht gefälscht werden. Es handelt sich daher nicht um einen Hinweis auf die Echtheit einer E-Mail.
2. **vorgetäuschte Dringlichkeit:** In vielen Phishing-E-Mails wird versucht, dir weiszumachen, dass dein Konto in Gefahr ist, wenn Du es nicht umgehend aktualisierst. Eine E-Mail, in der Du dazu aufgefordert wirst, dringend vertrauliche persönliche Angaben preiszugeben, ist in der Regel betrügerischen Ursprungs.
3. **Gefälschte Links:** Viele Phishing-E-Mails enthalten Links, die echt aussehen, über die Du jedoch auf eine betrügerische Website gelangst, deren URL u.U. sogar von dem Link abweicht. Prüfe daher, wohin ein Link dich leitet, bevor Du darauf klickst. Zeige mit dem Mauszeiger über den Link in der E-Mail, und prüfe die URL im Browserfenster. Auch hier gilt: wenn sie verdächtig aussieht, klicke nicht darauf.
4. **Anlagen:** Ähnlich wie gefälschte Links können in Phishing-E-Mails auch gefährliche Anlagen verwendet werden. Klicke nie auf eine Anlage, vor allem nicht Anlagen mit den Endungen wie „.exe“ oder „.rar“ oder „.zip“. Dies kann unter Umständen dazu führen, dass Spyware oder ein Virus auf deinen Computer heruntergeladen wird.

Hier kannst Du uns die Betrüger E-Mails melden. Leite die gesamte E-Mail, einschließlich Kopfdaten, oder die URL der Website weiter an

emailbetrug@limango.de

Wir untersuchen jeden gemeldeten Betrugsfall!