Phishing

Phishing ist ein Begriff für verschiedene Formen der Datenkriminalität im Internet. Er setzt sich aus den englischen Worten „password“ und „fishing“ zusammen – es geht also um das **Abfischen sensibler Daten**. Betrüger:innen versuchen, sich beispielsweise Zugang zu Ihrem Online-Banking zu verschaffen und sich dadurch zu bereichern. Dabei nutzen sie die verschiedensten Kanäle:

✓ **E-Mail** ✓ **SMS** ✓ **Telefon** ✓ **Websites** ✓ **Social-Media- und Verkaufs-Plattformen**

Miles & More

Erkennen

Dringlichkeit

Seien Sie skeptisch, wenn Sie dringend zum Handeln aufgefordert werden, bei E-Mails oftmals schon in der Betreffzeile.

Anrede

Achten Sie auf eine persönliche Anrede. „Sehr geehrte Kundin“ bzw. „Sehr geehrter Kunde“ sollte Sie misstrauisch machen.

Rechtschreibung

Prüfen Sie Rechtschreibung, Groß- und Kleinschreibung sowie Zeichensetzung. Viele Fehler weisen auf eine Fälschung hin.

Links

Achten Sie auf die URL-Adresse der Seite, auf die Sie weitergeleitet werden sollen. „http“ steht für eine unsichere URL. Ein sicherer Link beginnt mit „https“.

Schützen

Absender

Öffnen Sie keine E-Mails, SMS und Links, deren Absender:in Sie nicht kennen.

Anhänge

Öffnen Sie keine Dateianhänge, die Sie nicht erwarten.

PIN und TAN

Geben Sie nie Ihre PIN oder TAN per E-Mail, SMS oder Telefon weiter und geben Sie im Online-Banking nie mehrere TAN zeitgleich ein.

Online-Kartenkonto

Starten Sie das Online-Banking immer über diese URL: **https://www.miles-and-more.kartenabrechnung.de** oder die aktuelle Version der **Miles & More Credit Card-App**.

Reagieren

Bei Verdacht auf eine gefälschte E-Mail oder SMS

Leiten Sie diese als Anhang an uns weiter: **service@lufthansacard.de**

Bei versehentlicher Weitergabe sensibler Daten

Sperren Sie Ihre Karten in der Web-Version Ihres Online-Kartenkontos unter „Service > Karte sperren oder ersetzen“ oder unter **+49 - 69 - 66 78 88 444**.

Für weitere Details zum Thema

Informieren Sie sich auf unserer Internetseite: **www.miles-and-more-kreditkarte.com/lp/phishing/**

Für Informationen über aktuelle Betrugsmaschen

Nutzen Sie den Phishing-Radar unter: **www.verbraucherzentrale/phishing**