Beispiele wie man online betrogen wird

Heutzutage wird man im Netz hauptsächlich durch
Phishing, Social Engineering, Abofallen und Betrügereien reingelegt.

Durch gezielte Tricks (E-Mails, SMS, Anrufe, etc.) versuchen Angreifer unser Vertrauen auszunutzen und Dringlichkeit zu erzeugen.
Um an unsere Daten zu gelangen, versuchen sie uns dazu zu bringen, auf Links zu klicken und/oder Anhänge zu öffnen.

Phishing & Spear-Phishing

Du erhältst eine E-Mail, die aussieht, als käme sie von einer bekannten Firma (Bank, Paketdienst, Streaming-Anbieter o.ä.)

Darin wird oft eine dringende Handlung gefordert, z.B.:

Konto gesperrt, Paket nicht zugestellt usw.

Man versucht dich zu verleiten um auf einen gefälschten Link zu klicken und deine Daten preiszugeben.

Sie Haben Eine ausstehende Lieferung #352-3874170 Verfolgen Sie Ihre lieferung.

Post Tracking (milmilada@t-online.de) Kontakt hinzufügen

An: Hermes Paketankundigung;

#352-3874170 Verfolgen Sie Ihre lieferung.

Sendungsverfolgungsbenachrichtigung für Ihr Paket, ID#34632900-3717

Hermes

Wir konnten Ihr Paket nicht zustellen, da niemand anwesend war, um die Lieferung zu unterzeichnen.

Wir benötigen eine Adressbestätigung, um den Versand des Pakets zu bestätigen.

ÜBERPRÜFE HIER

Ihre Kontoinformationen sind falsch

ING App (Alexinana0200@1blu.de) Kontakt hinzufügen

An: peter.

ING

Die Bank und Du

Sehr geehrter ING-Kunde,

Um die Sicherheit unserer Kunden zu gewährleisten, informieren wir Sie, dass Ihre iTan-Liste in den nächsten 24 Stunden abläuft. Um Probleme mit Ihrem Online-Banking zu vermeiden, klicken Sie bitte auf den folgenden Link und folgen Sie den Anweisungen, um eine neue iTan-Liste anzufordern

https://www.ing.de/log/banking

Laden im App Store

JETZT BEI Google Play

Social Engineering

Angreifer nutzen psychologische Tricks, um dich zu manipulieren.
Das kann z.B. durch Anruf, SMS oder E-Mail geschehen.

Es erzeugt in uns emotionale Reaktionen und bewegt uns zu Handlungen, die man normalerweise nicht tun würde:

Überweisungen tätigen, Kennwörter nennen, Software installieren, etc.

Und dann noch der alte Enkeltrick

Abofallen

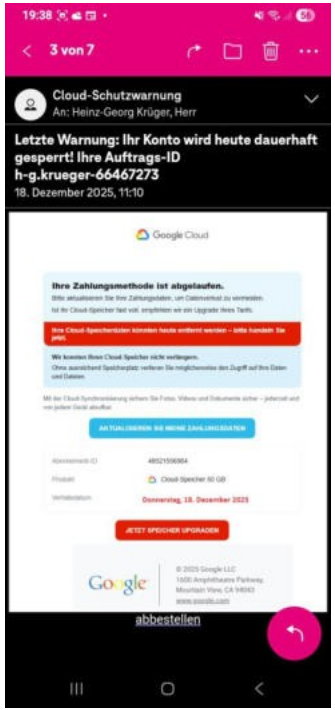
Du klickst auf einer Webseite (oft bei vermeintlich kostenlosen Angeboten) auf einen Button, schließt unwissentlich ein kostenpflichtiges Abo ab und erhältst dann Mahnungen oder Rechnungen, die du bezahlen sollst.

Malware & Ransomware

Du lädst unwissentlich Schadsoftware herunter (z.B. über infizierte Anhänge), die deinen Computer sperrt (Ransomware) oder Daten stiehlt.

Immer öfter tauchen Messages auf Handys auf:

Zahlungen



Optimieren

Rechnungen

Banken

Wie kann ich mich schützen?

1.

Misstraue E-Mails & Nachrichten: Prüfe Absenderadressen genau und klicke nicht sofort auf Links, besonders wenn Dringlichkeit suggeriert wird.

Hat man ein Konto, dann wähle selbst den Login im Browser!

z.B.:
https://www.bank.de/login

2.

Gib keine Daten preis: Gib Passwörter oder Kreditkartendaten niemals auf unbekannten Seiten ein, die du über Links in E-Mails erreicht hast.

Nutze stattdessen die offizielle Website!

3.

Nutze sichere Passwörter & Zwei-Faktor-Authentifizierung (2FA) bzw. Secure Go App

Das erschwert Angreifern den Zugriff!

Secure Go App:

4.

Sei vorsichtig bei "Gratis"-Angeboten: Lies das Kleingedruckte, bevor du irgendwo zustimmst.

5.

Am PC/Laptop sind SPAM und JUNK E-Mails besser zu erkennen als an einem Handy.

Geht man mit der Maus auf einen Link und/oder Mailadresse erscheint die vollständige Adresse links unten (Thunderbird).
NICHT KLICKEN!
So kann man erkennen um was für einen Link es sich handelt.

Handelt es sich um eine vertrauenswürdige E-Mail und der Anhang lautet z.B.:
Muster.pdf
Kann dieser geöffnet werden.

Handelt es sich dagegen nicht um eine vertrauenswürdige E-Mail und der Anhang lautet z.B.:
Muster.pdf.exe
Sollte man auf keinen Fall öffnen.


Posteingang
Entwürfe
Gesendete Objekte
Archiv
Junk
Spam
Papierkorb
Lokale Ordner
Feed
g.muster911@gm.com
Von: G.Muster
g.muster911@gm.com
Mauszeiger
Nachrichtentext:
Hi,
bla bla bla
Kind regards,
G.M.
https://www.bla.com

ENDE