

PHISHING SICHER ERKENNEN



Phishing bezeichnet den **versuchten Identitäts- oder Datendiebstahl** durch manipulierte elektronische Kommunikation, meist E-Mail. Angreifer nutzen gefälschte Absenderadressen, täuschend echte Webseiten oder Schadsoftware, um **Anmeldedaten, Finanzinformationen oder vertrauliche Daten** zu erbeuten. Wissenschaftlich wird Phishing als **häufigste Angriffsform im Bereich Cybercrime-as-a-Service** klassifiziert, da es Skaleneffekte und Automatisierung erlaubt.

1

Vorher

- Absenderadresse und Inhalte (auch Links und Anhänge) kritisch prüfen
- Echtheit von Anfragen über unabhängigen Kanal (z. B. Anruf) bestätigen

2

Währenddessen

- Innehalten statt reagieren: Nicht sofort auf E-Mails antworten, insbesondere bei Druck oder Androhung negativer Konsequenzen
- unsichere E-Mails als potenzielles Phishing kennzeichnen und zur Prüfung an die IT-Abteilung weiterleiten

3

Danach

- Vorfall dokumentieren und auf weitere Anweisungen warten: Was, wann, wo (System, Abteilung), wie wurde es erkannt, wer ist betroffen und welche Auswirkungen sind erkennbar?

Sie können sich über aktuelle Phishing-Fälle und Warnungen über das [Phishing-Radar der Verbraucherzentrale](https://www.verbraucherzentrale.de/wissen/digitale-welt/phishingradar/phishingradar-aktuelle-warnungen-6059) informieren.

[<https://www.verbraucherzentrale.de/wissen/digitale-welt/phishingradar/phishingradar-aktuelle-warnungen-6059>]

VERHALTENSTIPPS

Mit aufmerksamem Verhalten können Sie verhindern, dass Cyberkriminelle mit Phishing Erfolg haben.

Do's

Mail-Inhalte und Absender prüfen
bei Druck oder Drohung skeptisch sein

Don'ts

unsichere Links & Anhänge öffnen
Vorfall außerhalb der Organisation kommunizieren