



**Phishing: Bei welchem  
Köder werden Sie  
schwach?**





# Phishing

- Die meisten Phishing Angriffe starten per E-Mail und fordern den Nutzer auf einen **Link anzuklicken oder einen Anhang zu öffnen**. Phishing erfolgt jedoch auch auf anderen Wegen z.B. SMS (Smishing).
- Phishing ist heutzutage **eine der größten Cyber-Bedrohungen** für Unternehmen, Organisationen, Behörden aber auch Privatpersonen.
- Moderne Phishing Angriffe, welche teilweise auch mit **künstlicher Intelligenz erzeugt** werden sind sehr **schwer zu durchschauen**.
- Wir stellen ihnen nachfolgend vor worauf sie beim Empfang von E-Mails und SMS achten müssen und wie Sie Phishing erkennen können.





# E-Mail Phishing

The screenshot shows an email window with a sender address 'Onlinebank Konto-service' and a subject 'Verdächtige Aktivitäten auf Ihrem Konto'. The email body contains a salutation, a warning about suspicious activity, a call to action with a link, a 24-hour deadline, and a sign-off. A red dashed box highlights the main body text, and a blue dashed box highlights the call to action and link.

Von Onlinebank Konto-service

Betreff Verdächtige Aktivitäten auf Ihrem Konto

Sehr geehrter Nutzer,

Wir möchten Sie darüber informieren, dass wir verdächtige Aktivitäten in Ihrem Konto festgestellt haben. Um die Sicherheit Ihres Kontos zu gewährleisten, bitten wir Sie, Ihre Kontodaten umgehend zu überprüfen.

Bitte klicken Sie <http://login.payment/bestt3??info/DE> **Klicken oder tippen Sie, um dem Link zu folgen.** bestätigen:

<https://konto-service.info/DE>

Wenn Sie nicht innerhalb von 24 Stunden antworten, sehen wir uns gezwungen, Ihr Konto vorübergehend zu sperren, um es vor unbefugtem Zugriff zu schützen.

Mit freundlichen Grüßen,  
Ihr Kundenservice-Team

## Absenderadresse

Vertrauen Sie nie der Absenderadresse, diese kann gefälscht werden!

## Anrede & Layout

Unpersönliche Anreden sind häufig ein Anzeichen für Phishing. Prüfen Sie zudem das Layout und die Schreibweise!

## Handlungsaufforderung

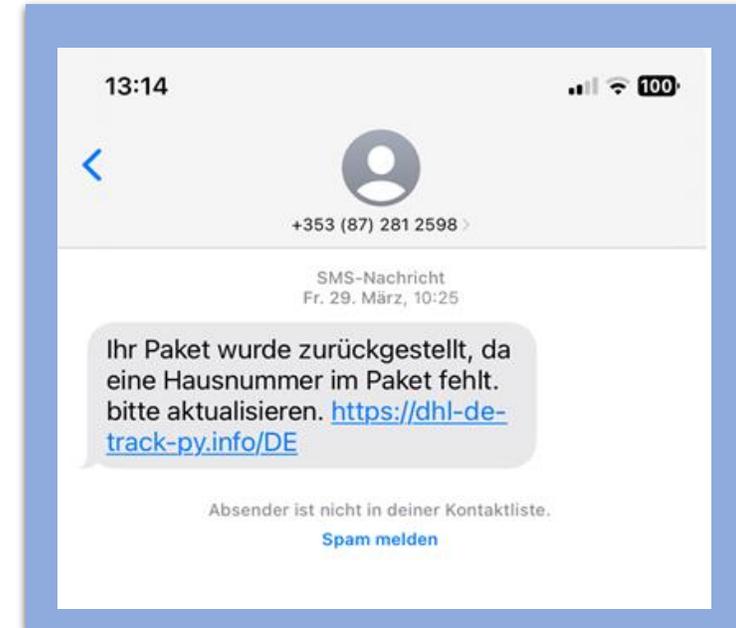
Phishing-Mails enthalten meist eine Handlungsaufforderung um einen Link oder Anhang zu öffnen. Vorsicht: Die Links können gefälscht werden! Fahren Sie mit der Maus über den Link, dann erscheint der eigentliche Link.



# Phishing

## Stellen Sie sich folgende Fragen:

- **Ist der Empfang der Nachricht sinnvoll?**  
z.B. Habe ich überhaupt etwas bestellt? Habe ich ein Konto bei dieser Bank?
- Falls ja gehen Sie trotzdem nicht auf den Link, sondern gehen Sie über ihre Favoriten oder geben Sie die Ihnen bekannte URL ihrer Bank ein.
- Öffnen Sie nie Mahnungen oder ähnliche Anhänge! In diesen ist meist Schadsoftware enthalten.
- Bei Unsicherheit: **Melden Sie die E-Mail an ihre IT** und fragen Sie nach, ob es sich um eine Phishing Mail handelt.



Angreifer täuschen vor, eine vertrauenswürdige Person oder Organisation zu sein, um sensible Informationen wie Benutzernamen oder Passwörter zu stehlen



# Monats-Challenge



## Sind Sie vorbereitet:

- Erkennen Sie Phishing?
- Was machen Sie, wenn Sie doch einmal darauf hereingefallen sind?
  - Geldforderungen
  - Erpresserschreiben
  - Ausgesperrt aus Ihren Konten
- Was machen Sie, wenn Sie doch einmal hereingefallen sind?