

# Auflösungen bei simulierten Fallen

Konzept für Vorsicht Falle

***Valentine Auer***

# Phishing-Simulationen auflösen

---

## Wann?

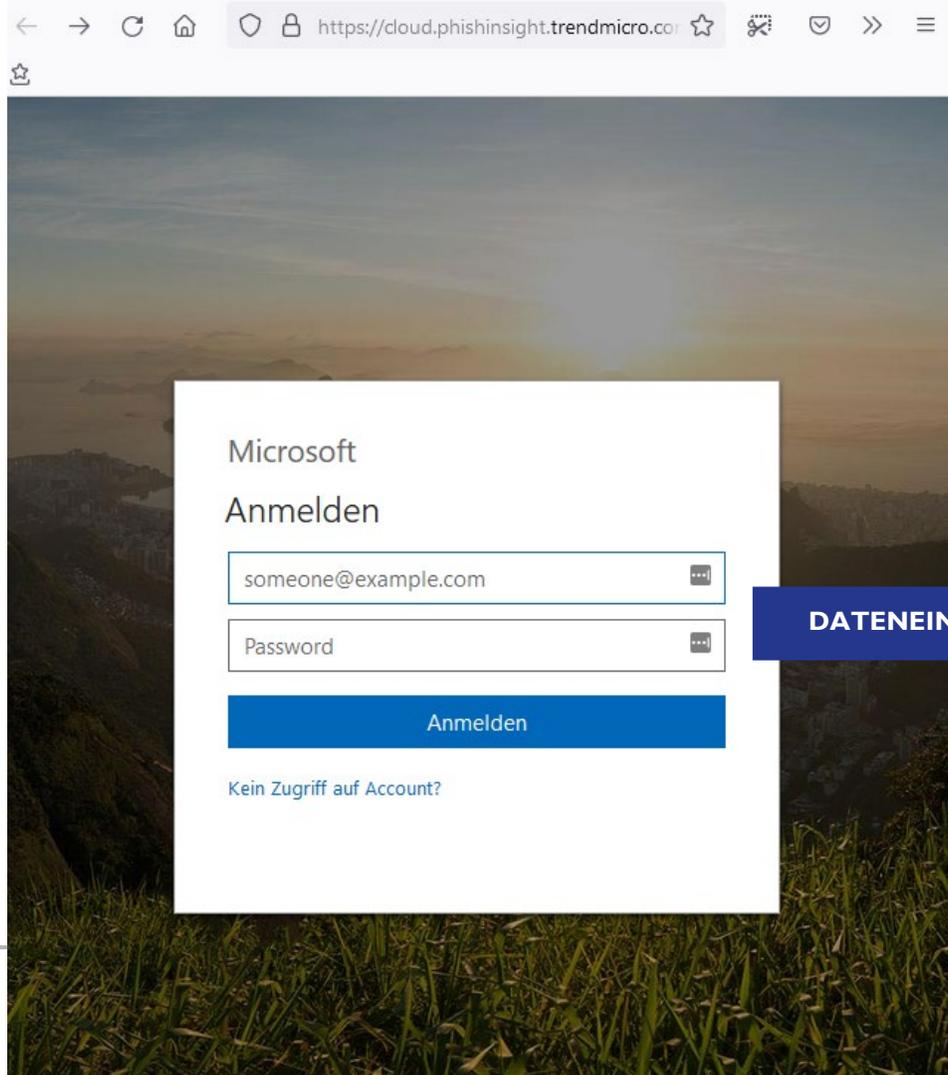
- Keine Auflösung, wenn Phishing-Nachricht ignoriert wird
- Auflösung beim Anklicken eines Links oder Öffnen eines Anhangs
- Auflösung nach Dateneingabe

## Wie?

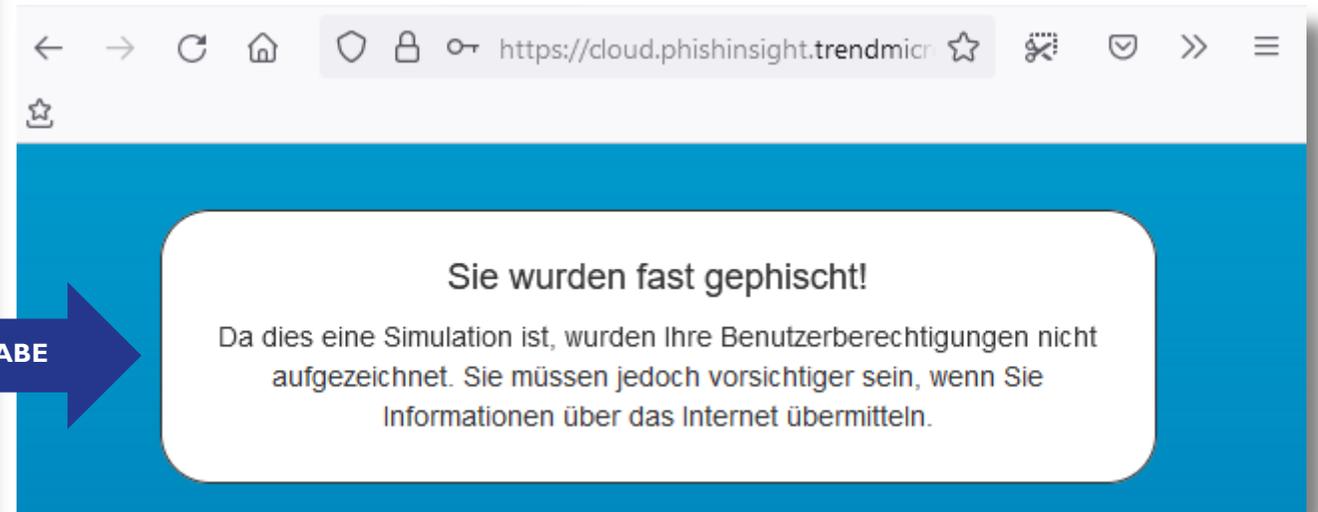
- Allgemeiner Hinweis
- Anzeichen für Phishing anhand der konkreten Nachricht
- Allgemeine Tipps um Phishing zu erkennen
- E-Learning-Modul

# Beispiel: Allgemeiner Hinweis nach Dateneingabe

(Phishing-Simulation von Phish Insight | Trend Micro)



**DATENEINGABE**



# Beispiel: Phishing-Anzeichen nach Dateneingabe

(Phishing-Simulation von Phish Insight | Trend Micro)

## Good thing, it was just a simulated phishing attack!

The email you received is a spear-phishing email we sent out to our employees as part of a security awareness campaign. The next time you encounter such kind of email, please think before you click.

- Make sure the email came from a legitimate email address.
- Always hover over a hyperlink anchor before clicking.
- Verify the website URL before sharing your credentials.

Let us work together to make our workplace secured and safe.

The screenshot shows an email interface with the following content:

From: Facebook <security@faceboookmail.com>  
Sent: Wednesday, July 14, 2021 8:38 AM  
To: Tommy <tommy@trendmicro.com>  
Subject: Login alert for Chrome on Windows

**Non-existing domain name**  
The "faceboookmail.com" domain does not exist

 [Login Alert](#)

**Hi Shiela**  
Your account was recently logged into from a new browser or device. Was this you?

New Login

 July 14, 2021 at 00:37

 Near Panchiaochen, Taiwan

 Chrome on Windows

[Review Login](#) [Manage Alerts](#)

**Mismatched link destination**  
The buttons are not directing to a Facebook website.

<https://www.eservicebits.com/landingpage/4c2a6462-b05d-4d66-88d5-c6b9d1bb49d2>

Facebook, Inc., Attention: Community Support, Menlo Park, CA 94025

# Beispiel: Phishing-Anzeichen nach Klick

(Phishing-Simulation von SoSafe)

## Kleines 1x1 zur Cybersicherheit

Was ist Social Engineering?

Bei Social Engineering geht es darum, Menschen so zu manipulieren, zu beeinflussen oder zu täuschen, dass Kontrolle über deren Computersystem erlangt werden kann. Die Kontaktaufnahme erfolgt in der Regel per E-Mail, Privatnachrichten in sozialen Netzwerken, Telefon oder seltener auch per Briefpost und direkten Kontakt. Ziel bei allen Methoden ist es, illegalen Zugriff auf die Daten des Nutzers oder des zugehörigen Unternehmens zu erhalten. Einige Beispiele für Social Engineering sind Techniken wie Phishing, Spear-Phishing oder der „CEO-Trick“.

Was ist Phishing?

Was ist Spear Phishing?

Was ist CEO-Fraud?

Siehe auch Vorsicht Falle: [amazon.gewlwnspiel.at](https://www.amazon.gewlwnspiel.at)

Stefanie Hahneman <stefanie.hahneman@gmail.com>  
Bewerbung Büroassistent

**Allgemeiner Anlass** 1 von 4

Sehr geehrte Damen und Herren,  
Häufig verwenden Angreifer einen Anlass, der auf möglichst viele Firmen und Empfänger passt, hier z. B. eine Bewerbung auf eine Position, die in vielen Firmen und Abteilungen vorzufinden ist. Je unspezifischer der Grund der E-Mail ist, umso vorsichtiger sollten Sie sein – insbesondere bei Initiativbewerbungen.

Nach achtungsbewolgender Prüfung Ihrer Bewerbungsunterlagen und nach Rücksprache mit dem Personalmanagement des internationalen Konzerns möchte ich mich nun beruflich mit Ihnen in Verbindung zu setzen. Ich würde mich freuen, Sie persönlich an unserem Unternehmen durch meine Erfahrung im Vertrieb und in der Kundenbetreuung zu unterstützen. Bitte senden Sie mir Ihre ausführlichen und angehängten Bewerbungsunterlagen zu [stefanie.hahneman@amazon.gewlwnspiel.at](mailto:stefanie.hahneman@amazon.gewlwnspiel.at) oder an [Ihrer Website](mailto:stefanie.hahneman@amazon.gewlwnspiel.at) gesehen.

Sämtliche Bewerbungsunterlagen können auch über den folgenden Link heruntergeladen werden:  
<https://www.dropbox.com/sh/740kldjwtsusm/AAAjrtkZheapHRH8-mnsOsEa?dl=0>

Ich freue mich auf ein persönliches Vorstellungsgespräch.

Mit freundlichen Grüßen  
Stefanie Hahneman

--  
Stefanie Hahneman  
Bahnstr. 181  
59063 Hamm  
M: Stefanie.Hahneman@gmail.com  
T: 0161 13545092152

# Beispiel: MicroLearning-Einheit nach Klick

(nachgebildete Phishing-Simulation von Lucy)

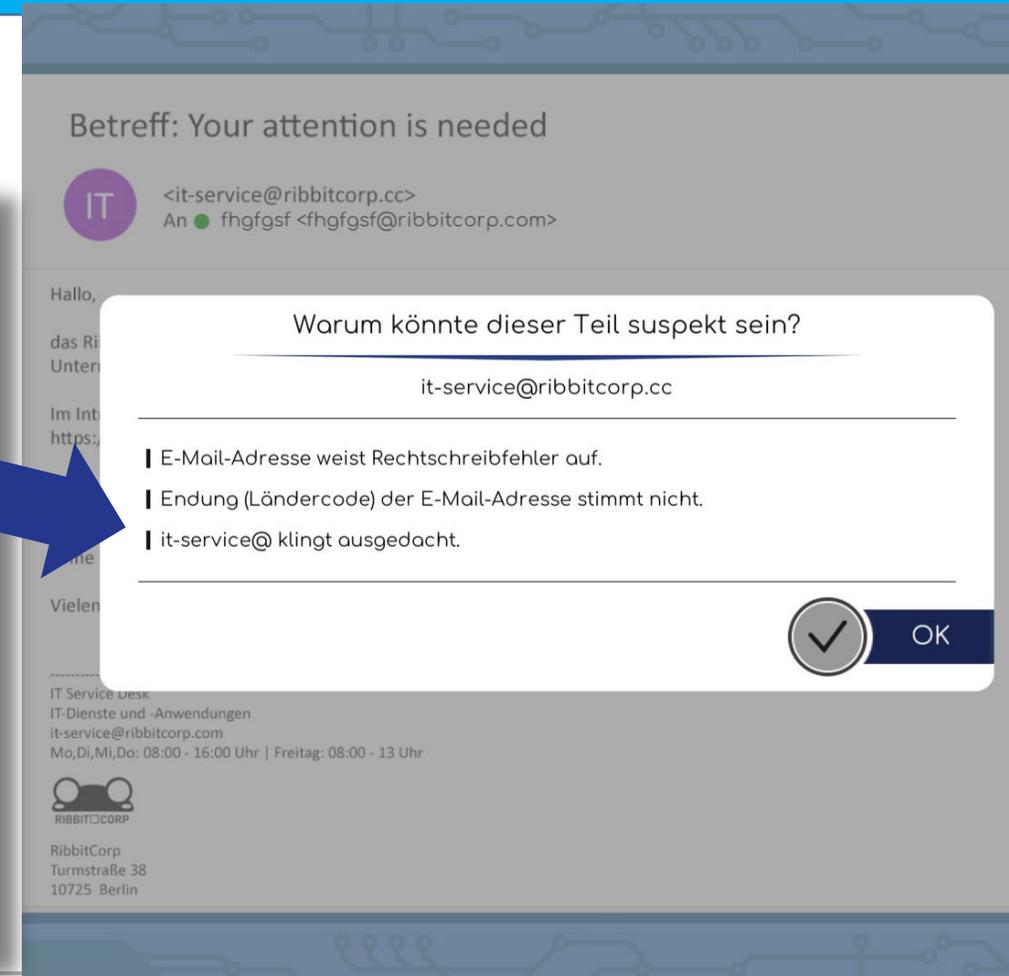
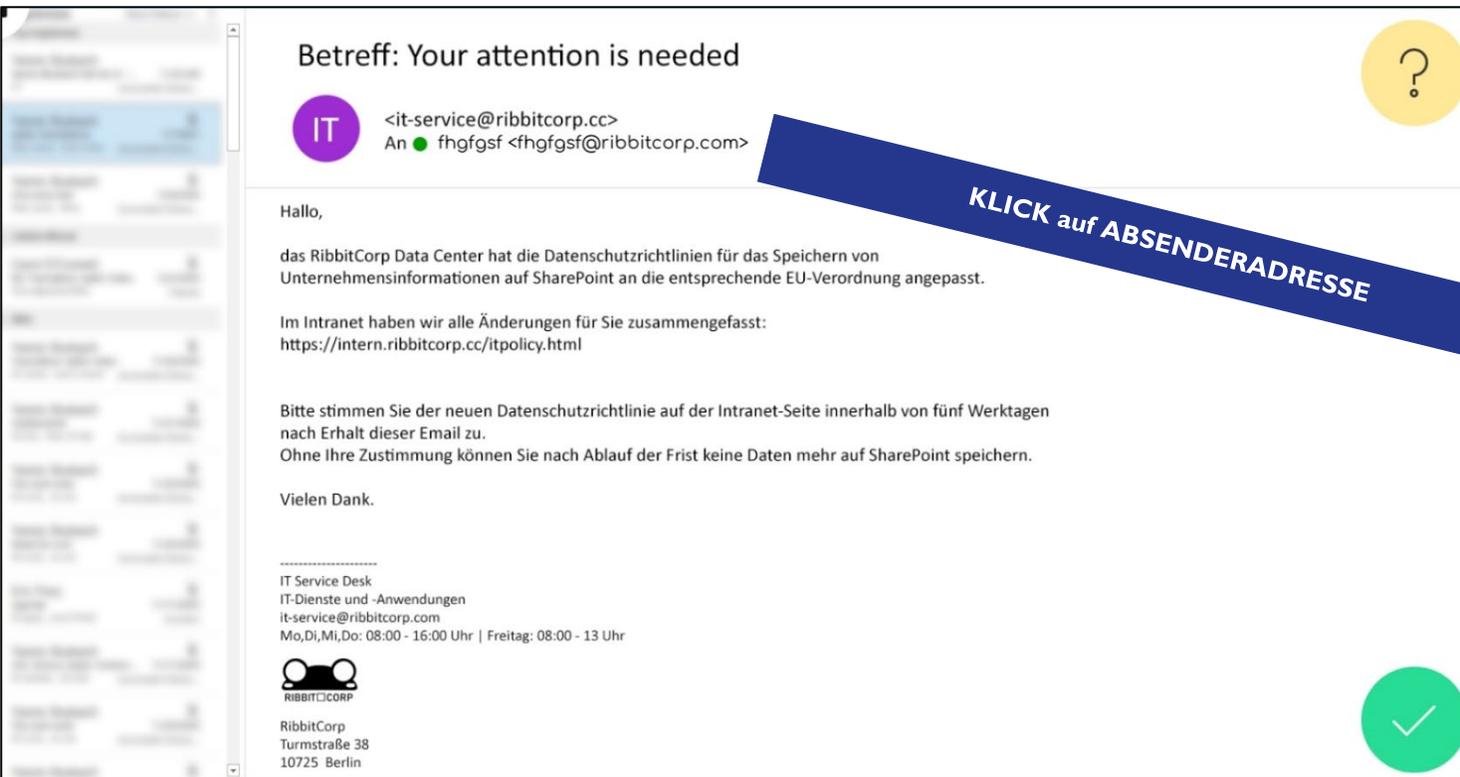
Man kommt auf eine Seite mit unterschiedlichen Micro-Learnings: Texterklärungen, Video, Quiz, wichtigsten Tipps etc.



# Beispiel: Hinweise selbst finden

(Adventure Game „Social Engineering Trap“ von Fabula Games)

Wir haben einen Demo-Zugang zu diesem Game: [https://demo.fabula-games.de/set\\_tb/](https://demo.fabula-games.de/set_tb/) unter dem Modul „Phishing“, findet ihr dieses Element.



# Beispiel: Hinweise selbst finden

(Adventure Game „Social Engineering Trap“ von Fabula Games)

**Betreff: Your attention is needed** Suspekt: Der Betreff ist englischsprachig, die E-Mail auf Deutsch.

**IT** <it-service@ribbitcorp.cc>  
An fhgfsf <fhgfsf@ribbitcorp.com> Suspekt: Endung (Ländercode) der E-Mail-Adresse stimmt nicht.

Hallo,

das RibbitCorp Data Center hat die Datenschutzrichtlinien für das Speichern von Unternehmensinformationen auf SharePoint an die entsprechende EU-Verordnung angepasst.

Im Intranet haben wir alle Änderungen für Sie zusammengefasst:  
<https://intern.ribbitcorp.cc/itpolicy.html> Suspekt: Der Link führt auf eine unbekannte Website.

Bitte stimmen Sie der neuen Datenschutzrichtlinie auf der Intranet-Seite **innerhalb von fünf Werktagen** nach Erhalt dieser Email zu. Suspekt: Hier wird ein akuter Handlungsbedarf vorgetäuscht.  
Ohne Ihre Zustimmung können Sie nach Ablauf der Frist **keine Daten mehr auf SharePoint speichern.**

Vielen Dank.

-----  
IT Service Desk  
IT-Dienste und -Anwendungen  
it-service@ribbitcorp.com  
Mo,Di,Mi,Do: 08:00 - 16:00 Uhr | Freitag: 08:00 - 13 Uhr

  
RIBBITCORP

RibbitCorp  
Turmstraße 38  
10725 Berlin

Suspekt: Eine Androhung von Konsequenzen soll mich zum Handeln zwingen.

? ✓

# Beispiel: Hinweise selbst finden

(Adventure Game „Social Engineering Trap“ von Fabula Games)



## WISSEN KOMPAKT



Hinweise auf eine Phishing-E-Mail können sein:

- **Absenderadresse:** Prüfe, ob jeder einzelne Buchstabe zum/zur erwarteten Absender:in passt.
- **Betreff:** Vergleiche, ob die Sprache zum restlichen Text passt.
- **Links und Anhänge** nur dann anklicken oder öffnen, wenn du dir zu 100% sicher bist, dass die E-Mail aus einer vertrauenswürdigen Quelle stammt.



# Simulationen auflösen

---

## Wann?

- Auflösung nach Dateneingabe bzw. anderer Aktion
- Wer nicht geklickt oder Daten eingegeben hat, erhält einige Tage später eine Auflösungs-Mail.

## Wie?

- Zwei verschiedene Auflösungsseiten
  - Geklickt: „Das war knapp. Das hätte auch ein Phishing-Mail sein können. Aber woran erkennt man solche betrügerische Nachrichten?“
  - Nicht geklickt: „Wir haben Ihnen ein Phishing-Mail geschickt. Woran haben Sie erkannt, dass es sich um Betrug handelt?“
- Screenshot der Phishing-Mail mit Aufforderung, Hinweise selbst zu finden.