

# Phishing

Das Phishing mit E-Mails oder SMS ist zwar im Allgemeinen eher im Kontext von Einzeltricks oder anderem Scam bekannt, doch auch staatliche Akteure nutzen gerne Phishing, um Zielpersonen mit Malware zu infizieren.

Hierbei sind ein paar Sachen zu bedenken. One-Click-Malware, also jene, bei der User\*innen proaktiv auf einen Link klicken, oder einen Download tätigen müssen, damit das Gerät infiziert werden kann, ist um einiges günstiger zu haben, als Zero-Click-Lösungen, bei denen Geräte, ohne weiteres Zutun der Nutzenden infiziert werden können.

Außerdem sind Phishingangriffe auch relativ schwierig zurück zu verfolgen. Fliegt das Phishing auf, bleibt trotzdem meist unklar, von wem der Angriff stammt, was eine ziemlich sichere Angriffsposition ermöglicht. Bei einer heimlichen Wohnraumverwanzung aufzufliegen ist deutlich riskanter und alarmiert die Betroffenen. Phishing hingegen landet bei uns allen ständig im Postfach und weckt kaum Misstrauen.

Hier ist ein Beispiel für, durch geschickte Wahl von Unicodezeichen, gefälschte Links. Erkennst du einen Unterschied in den Links? Welcher Link führt auf welche Seite?

## Beispiel 1

- <https://codeberg.org/esc-it/esc-it.org/releases/tag/@esc-it.org>
- <https://codeberg.org/esc-it/esc-it.org/releases/tag/@esc-it.org>

Ausnahmsweise, nur zum Lernen, kannst du jetzt auf die beiden Links klicken, um zu sehen was passiert. Hat deine Vermutung gestimmt?

Der 1. Link führt nicht auf codeberg.org sondern auf esc-it.org. Durch das @ wird der Teil davor als Nutzernamen verwendet. Eigentlich sollte das nicht funktionieren wenn vor dem @ ein / ist, aber im 1. Link sind Unicode Zeichen, die kein "normales" Slash sind.

Manche Browser zeigen bei dem falschen Link sogar eine Warnung an, wie hier in Firefox und dessen Fork LibreWolf:

Ein Pop-Up in Firefox warnt, dass wir dabei sind uns bei einer Webseite anzumelden die keine Anme

Chromium zeigt beispielsweise keine solche Warnung.

Auffällig an den Links ist, dass am Ende eine Domain steht (...@<esc-it.org>). Aber auch das ist kein eindeutiges Zeichen für Fakes und wird mit immer neuen Top-Level-Domains zunehmend schwer zu erkennen. Hier ein Beispiel mit einer ".zip"-Endung, sodass es sowohl eine .zip-Datei als

auch eine .zip-Domain sein könnte:

Achtung: Der erste Link führt auf eine Domain (*1312.zip*), die nicht uns gehört. Das heißt wir wissen nicht was darauf geschieht. Daher besucht diesen Link bitte nicht einfach, wenn ich nicht genau wisst, was ihr tut.

## Beispiel 2

- <https://codeberg.org/esc-it/esc-it.org/releases/tag/@v1312.zip>
- <https://codeberg.org/esc-it/esc-it.org/releases/tag/v1312.zip>

Auch hier führt der erste Link nicht auf eine Zip-Datei auf codeberg.org, der zweite Link aber schon. Hier erscheint auch keine Warnung, weil es die Domain bisher nicht gibt.

## Fazit

- Klickt nicht auf komische Links
- Hinterfragt den Ursprung des Links. Kann das sein, dass mir diese "Adresse" genau diesen Link schickt.
  - Geht auf Nummer sicher und sucht die Seite über verifizierbare Wege. Speichert originale Links in euren Passwortmanagern, in Lesezeichen im Browser oder nutzt Suchmaschinen.
- Tippt die Links im Zweifel von Hand ab.
  - Das hilft aber nichts, wenn der Link per se ein Fake ist. [systeml1.org] wird Euch so oder so auf die falsche Fährte führen. Hierbei wieder der Verweis auf den Punkt oben drüber um die korrekte URL festzustellen.

---

Version #1

Erstellt: 14 Januar 2025 18:52:22 von ESC-IT Migration Bot

Zuletzt aktualisiert: 14 Januar 2025 18:52:22 von ESC-IT Migration Bot