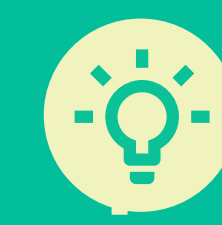


# Wie Hacker Ihre Psyche entschlüsseln...



## Phishing =

Das "Abfischen" von Zugangsdaten, Pincodes und Geschäftsgeheimnissen über präparierte E-Mails, Nachrichten oder Anrufe.

## Social Engineering =

Soziale Manipulation mit dem Ziel, bei Personen bestimmte Verhaltensweisen (z.B. Preisgabe von vertraulichen Informationen, Freigabe von Finanzmitteln) zu bewegen.

## Druck / Angst

Mögliche Strafen werden angedroht, falls nicht gehandelt wird (z.B. Mahngebühren in einer falschen Rechnungs-E-Mail) oder künstlicher Zeitdruck wird erzeugt („Handeln Sie jetzt oder ein wichtiges Projekt ist in Gefahr“).

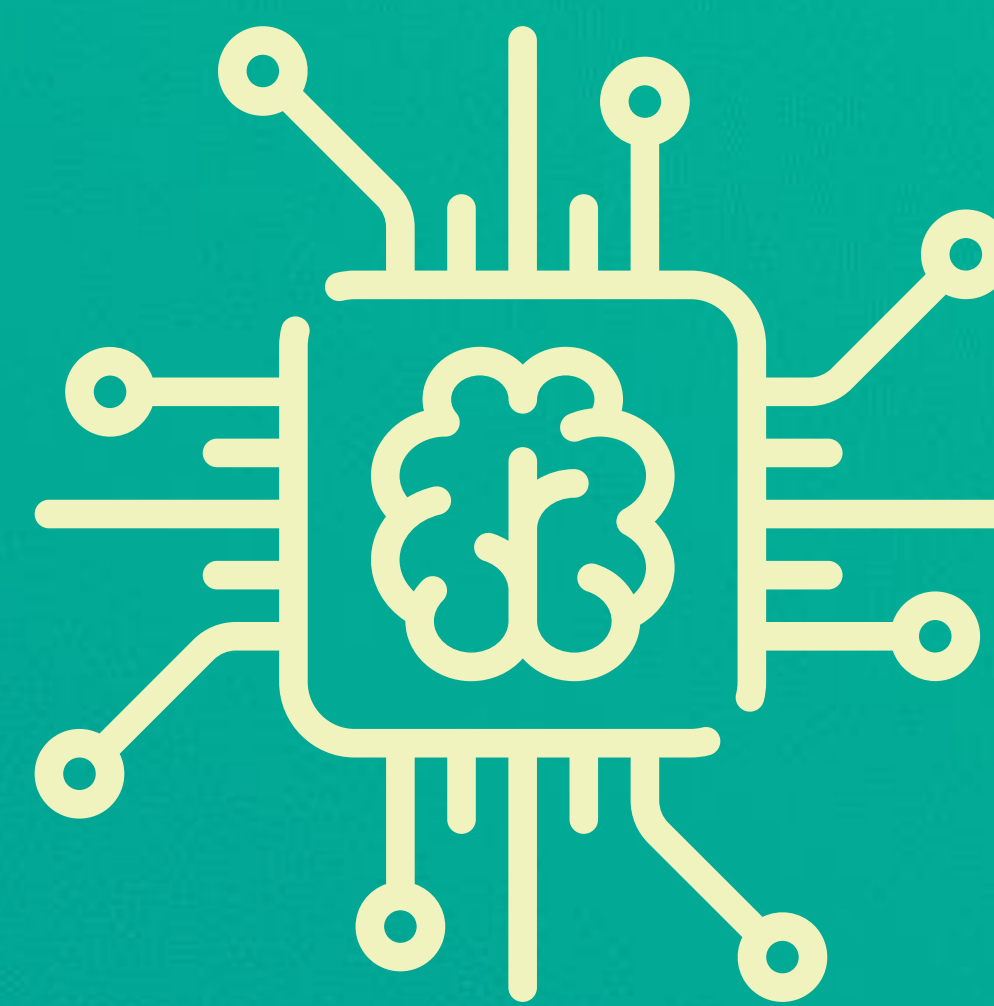


## Gier

Eine Belohnung oder mögliche Vorteile werden in Aussicht gestellt („Melden Sie sich hier an, um Mitarbeitervorteile zu erhalten“).

## Neugier / Interesse

Vermeintlich brisante Informationen werden in Aussicht gestellt (z.B. eine Excel-Datei mit dem Titel „Gehaltsdaten-2018.xlsx“) oder spannende Inhalte werden angedeutet („Bist Du das auf dem Video?“).



## Vertrauen

Vermeintliche Gemeinsamkeiten werden angeführt, um zusätzliches Vertrauen zu erzeugen („Wir haben doch kürzlich zu diesem Thema gesprochen“).

## Lob / Schmeichelei

Das Opfer wird bei seiner Eitelkeit gepackt, um Informationen zu erlangen (z.B. in Form einer Interviewanfrage an einen „ausgewiesenen Experten in einem speziellen Feld“)



## Hilfsbereitschaft

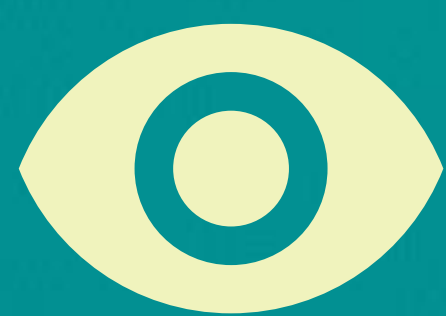
Menschen möchten anderen Menschen gerne helfen. Dies nutzen Angreifer aus, indem sie Verhalten anregen, dass einem Dritten vermeintlich in einer Notsituation hilft (z.B. ein USB-Stick liegt vor dem Werksgelände. Durch Einstecken kann man evtl. den Besitzer ausfindig machen.)

## Autorität

Der Angreifer nutzt die natürliche Hierarchie in einem Unternehmen (z.B. indem er sich als Vorgesetzter oder Behörde ausgibt).



# ...und wie Sie sich davor schützen können



## Grundhaltung: wachsam

Seien Sie vorsichtig bei ungewöhnlichen Anfragen – insbesondere, wenn Sie die genannten Prinzipien wiedererkennen! Fragen E-Mails direkt nach Geld oder Passwortdaten, ist dies zudem ein sicherer Hinweis auf Phishing.



## Absender: verifizieren

Versuchen Sie im Zweifel den Absender zu verifizieren, z.B. indem Sie ihn auf einem anderen Wege oder in einer gesonderten E-Mail kontaktieren. Wenden Sie sich zudem an Ihre IT-Abteilung.



## Wissen: laufend informieren

Halten Sie sich auf dem Laufenden, was aktuelle Betrugs- oder Phishingwellen angeht. Ihr Arbeitgeber bietet u.U. laufend Informationen über laufende Phishing-Angriffe oder besitzt eine eLearning-Plattform zu Sicherheitsthemen.

Weitere Information zu Phishing und Security-Awareness unter:

[www.allianz-fuer-cybersicherheit.de](http://www.allianz-fuer-cybersicherheit.de)

[www.sosafe.de](http://www.sosafe.de)

