

Muster: Lösungsansätze zu den Ergebnissen der Vorstellung

Schutz vor Identitätsdiebstahl am Beispiel Phishing-Mail

Einzelarbeit: Tipps und Tricks zum Umgang mit digitaler Identität und Mails erstellen.

* Vorsichtiger und reflektierter Umgang mit Informationen und persönlichen Daten

- keine unnötigen Daten in Webformulare eingeben (z.B. Postadresse, Telefonnummer,...)
- nicht einfach persönliche Daten anderer im Netz verbreiten (z.B. deren Kontaktdaten)

* technische Bildung: Welche Lücken gibt es? / Was für Konsequenzen haben welche Handlungen?

- eine digitale Identität lässt sich leicht fälschen: Der Absender einer E-Mail oder einer Messenger-Nachricht kann relativ einfach beliebigen Namen vorgeben
- der Klick auf einen Link in einer E-Mail führt mindestens dazu, dass der Absender weiß, dass die Adresse vorhanden ist, d.h. er kann weiter Spam verschicken
- ein Klick auf einen Link in einer Mail kann den eigenen PC / das eigene Gerät beeinträchtigen

* Wissen um die Grenzen der Technik: Was sollte besser gar nicht genutzt werden bzw. wo muss ich mich schützen und wie?

- wenn ein Absender suspekt erscheint, sollte diese Mailadresse als Spam gemeldet werden, so dass sie in Zukunft geblockt und die E-Mails einfach gelöscht werden
- sollte der Absender bekannt sein, aber ungefragt z.B. Werbung verschicken, kann auch rechtlich dagegen vorgegangen werden
- ein sicheres Verfahren zur Mailkommunikation ist die Nutzung von pgp und Signaturen (dies ist ein etwas längerer Exkurs, siehe z.B. https://support.mozilla.org/de/kb/nachrichten-digital-signieren-und-verschluseln#w_eine-digital-signierte-undoder-verschlaksselte-e-mail-versenden abgerufen am 26.07.2019)

Schutz vor Idenitätsdiebstahl

Dieses Material wurde erstellt von Hauke Morisse und Torsten Otto und steht unter der Lizenz [CC BY-NC-SA 3.0](https://creativecommons.org/licenses/by-nc-sa/3.0/)

