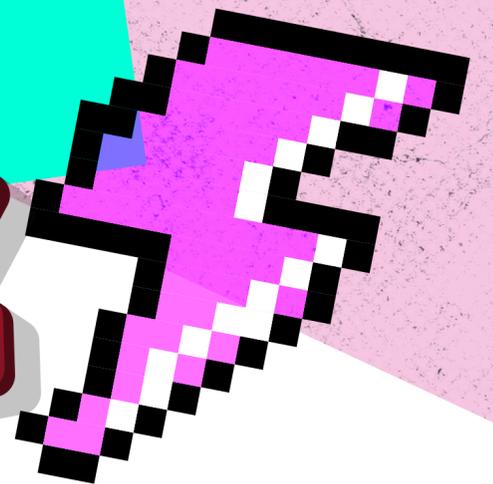




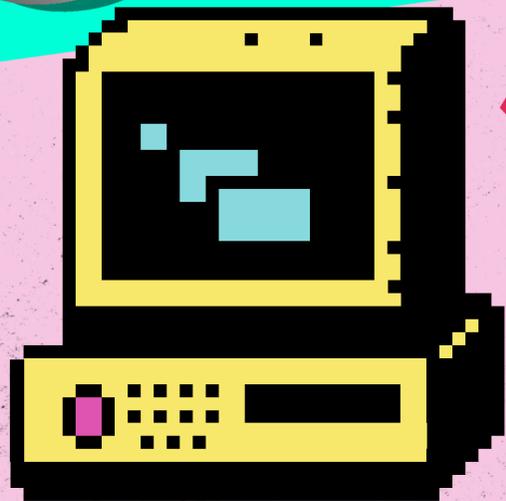
Das

CYBER SICHERHEIT

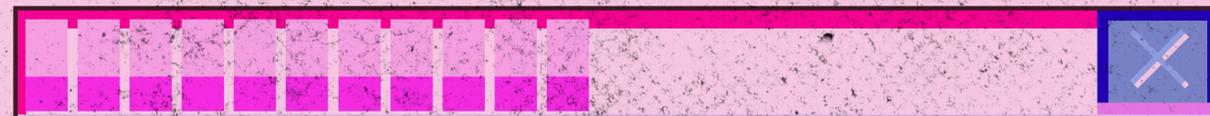
Quiz



**NICE TO
KNOW**



**Danach machst du dein Smartphone sicherer!
Teste dein Wissen zu Hackerattacken,
IT-Sicherheit, Passwörtern, Viren und Co.!**

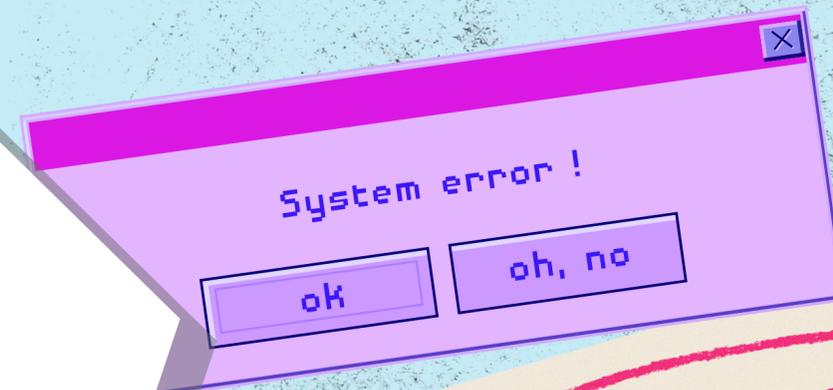


1. Was verstehen wir unter dem Wort Hacking?

✘ IN HECKEN UND GEBÜSCHE SPRINGEN.

✘ UNKONVENTIONELLE LÖSUNGEN FÜR PROBLEME FINDEN.

✘ AUSNUTZEN VON SICHERHEITSLÜCKEN, UM ZUGRIFF AUF COMPUTER UND NETZWERKE ZU BEKOMMEN.





Beim Hacking nutzen sogenannte Hacker:innen Sicherheitslücken aus, um Zugriff auf Computer und Netzwerke zu bekommen. Opfer von Cyberangriffen kann eigentlich jeder sein: Einzelne Personen, Unternehmer, und in Kriegssituationen sogar gesamte Staaten.

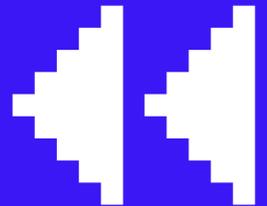
Ganz so negativ ist Hacking aber nicht immer. Ursprünglich bezieht sich der Begriff auf das Austüfteln von kreativen Lösungen. Life-Hacks liefern Tricks für unser alltägliches Leben und in einem Hackathon-Event erarbeitet eine Gruppe innovative Lösungen.

**NÄCHSTE
FRAGE**



FALSCH ANTWORT

REW

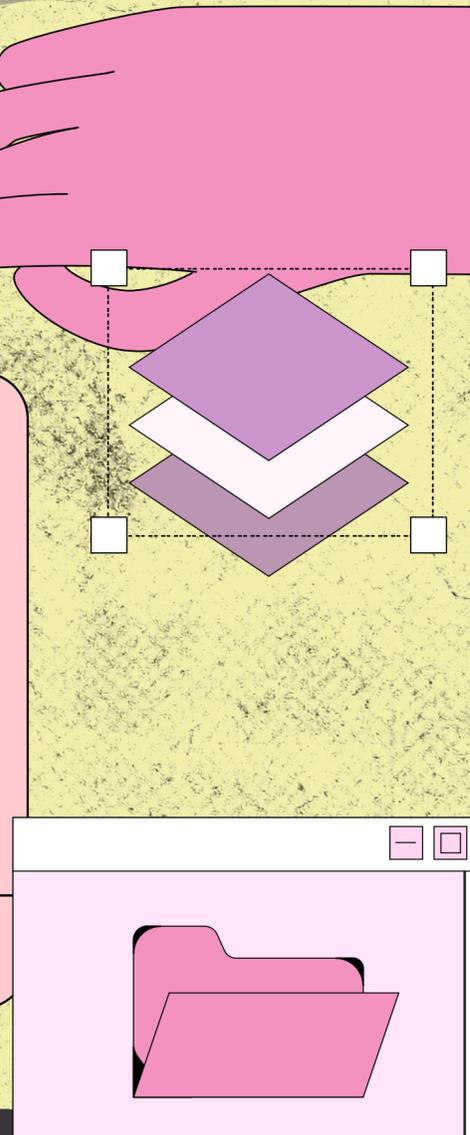
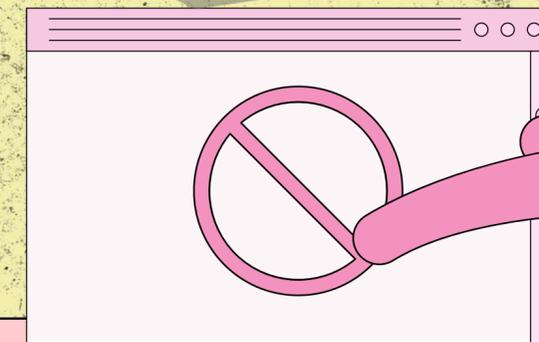
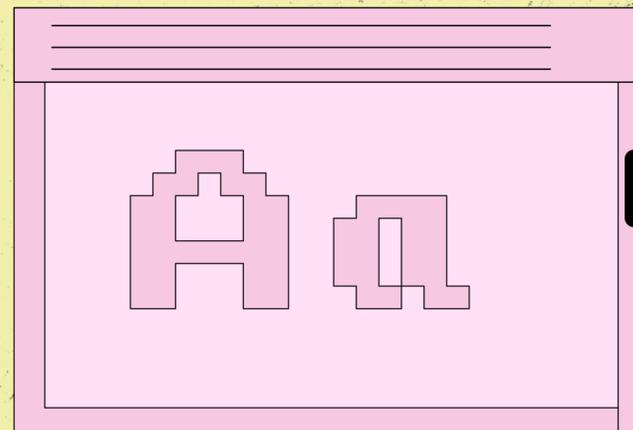
NOCHMAL 

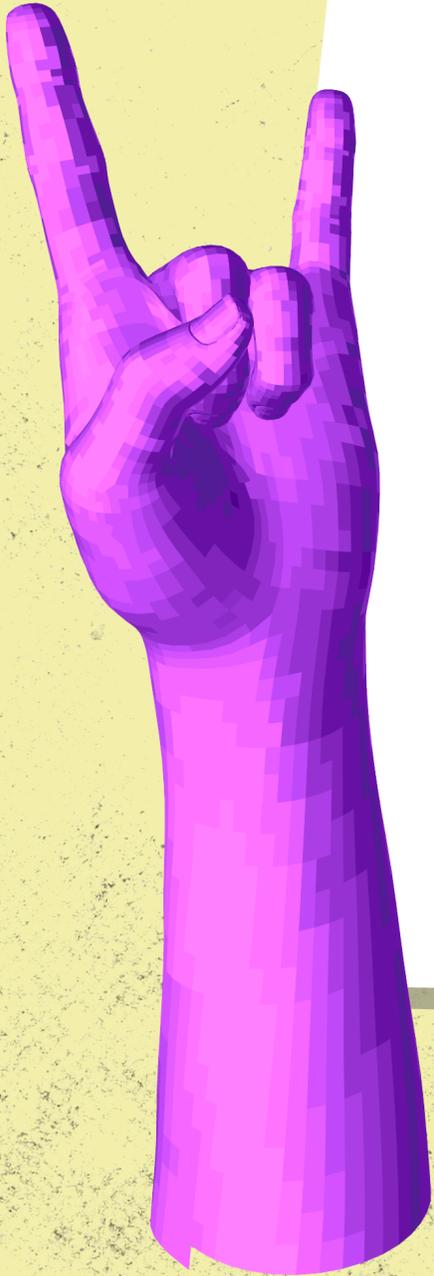
2. Was davon ist das beste Passwort?

✘ 1234

✘ PASSWORT4444

✘ QSUE-QW'33-ERP5-509M





Je kryptischer und rätselhafter desto besser! Sichere Passwörter sollten mindestens zehn Zeichen haben und aus Groß- und Kleinbuchstaben sowie Sonderzeichen bestehen. **Also nehmt keine echten Wörter, die ihr kennt!** Bei Datenlecks gelangen immer wieder Accounts und Passwörter in Listen, die sich im Internet verbreiten. Daher empfehlen wir auch, Passwörter regelmäßig zu ändern.

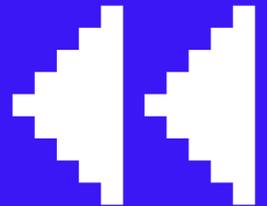


**NÄCHSTE
FRAGE**



FALSCH ANTWORT

REW

NOCHMAL 

3. Welcher ist der sicherste Messenger?



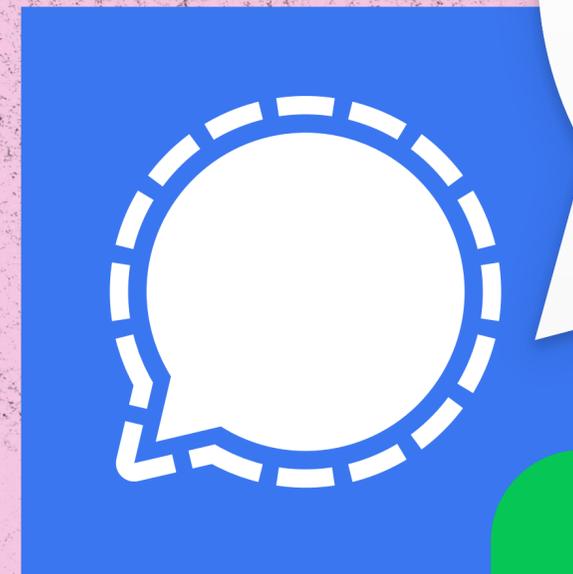
WHATSAPP

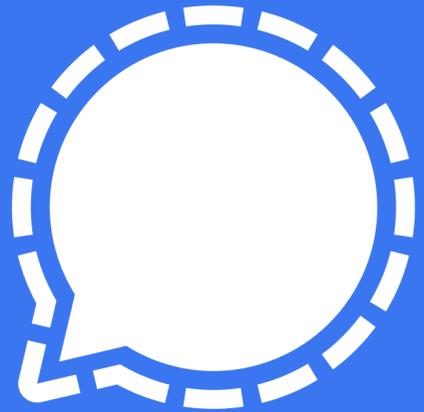


SIGNAL



LINE





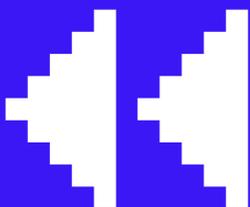
Beim Datenschutz und Anonymität schwächen die Apps WhatsApp und LINE und teilen persönliche Daten mit Dritten. Signal sammelt keine sensiblen Daten und schützt mit **Ende-zu-Ende-Verschlüsselung** Chats standardmäßig, diese müsst ihr bei WhatsApp und LINE selbst aktivieren. Damit schützt ihr eure Privatsphäre, denn nur Chat-Teilnehmer:innen können auf den Inhalt eurer Nachrichten zugreifen können.

**NÄCHSTE
FRAGE**



FALSCH ANTWORT

REW

NOCHMAL 

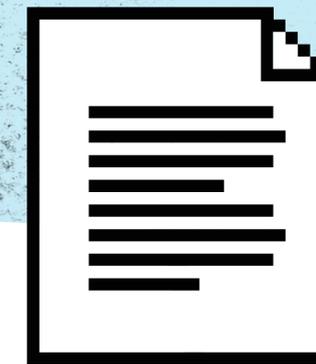
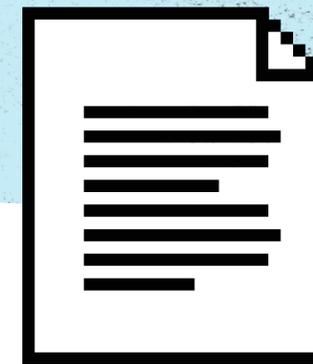
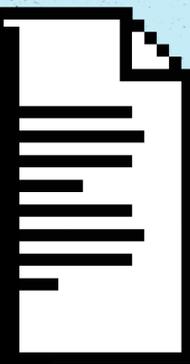
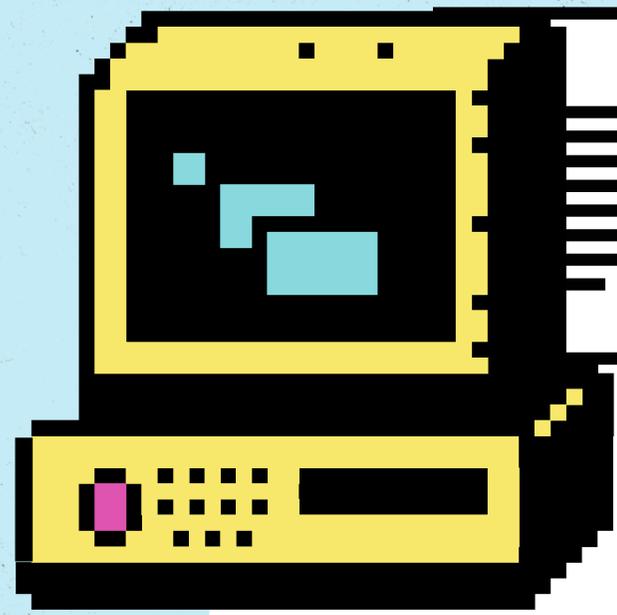
4. Wie viele Playstation-Accounts waren im April 2011 bei einer Hacking attacke betroffen?

77 MILLIONEN

500.000 GENAU

KEINE





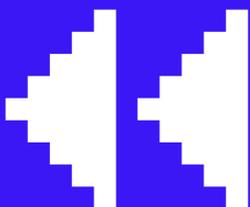
Auch Technik-Konzerne sind nicht 100% sicher: Im April 2011 hackten Unbekannte Sonys Playstation Netzwerk und stahlen rund 77 Millionen Datensätze von User:innen, darunter auch Kreditkartendaten. Um die Probleme zu lösen, musste Sony das Playstation-Network (PSN) für einen Monat abschalten und erlitt dadurch einen Schaden von rund 170 Millionen US-Dollar.

**NÄCHSTE
FRAGE**

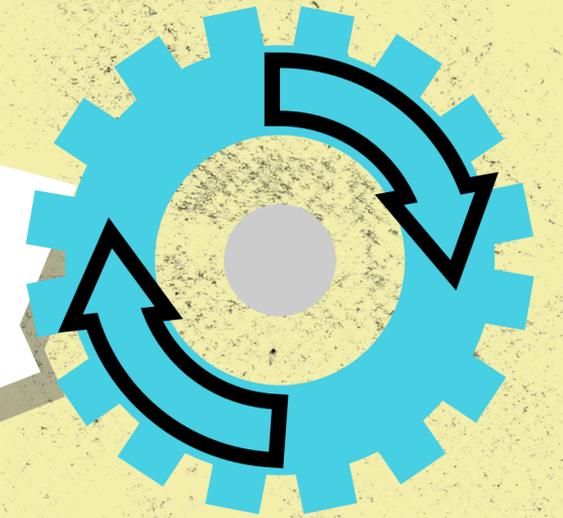


FALSCH ANTWORT

REW

NOCHMAL 

5. Wieso brauchen wir Patches und Updates?



PFLEGEN DIE HAUT UND WIRKEN ANTIBAKTERIELL



BEHEBEN FEHLER UND SICHERHEITSLÜCKEN
UND SCHÜTZEN VOR CYBER-ANGRIFFEN.



BRINGEN ÜBERHAUPT NICHTS!





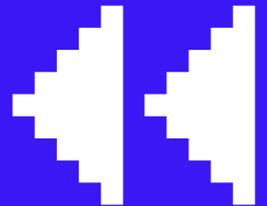
Updates und Game-Patches bremsen uns vielleicht zunächst oft aus, bieten aber Schutz vor Cyber-Angriffen. Die Software-Aktualisierungen schließen nämlich Sicherheitslücken. Und nebenbei wird auch häufig die Performance von Videospielen oder Betriebssystemen verbessert. Daher lohnt sich der Break!

**NÄCHSTE
FRAGE**



FALSCH ANTWORT

REW

NOCHMAL 

6. Was sind alles Computerviren? (Mehrfachnennung)

ILOVEYOU

EMOTET

MYDOOM

WANNACRY





So spaßig und kreativ wie sie klingen, alle vier sind bekannt-berüchtigte Computerviren. Loveletter wütete 2000 als Ketten-E-Mail mit dem Betreff „ILOVEYOU“ und **Schadcode** im Anhang. Der **Trojaner** „Emotet“ feierte erst Ende 2021 sein Comeback. „MyDoom“ terrorisierte uns 2004 mit **Datenmüll** und Spam. Die **Crypto-Ransomware** „Wannacry“ nahm 2017 Computer als digitale Geisel, um Lösegeld zu erpressen.

NÄCHSTE
FRAGE

7. Welche Daten solltest du Love-Scammer:innen definitiv nicht geben?



DEINE ZEIT UND AUFMERKSAMKEIT

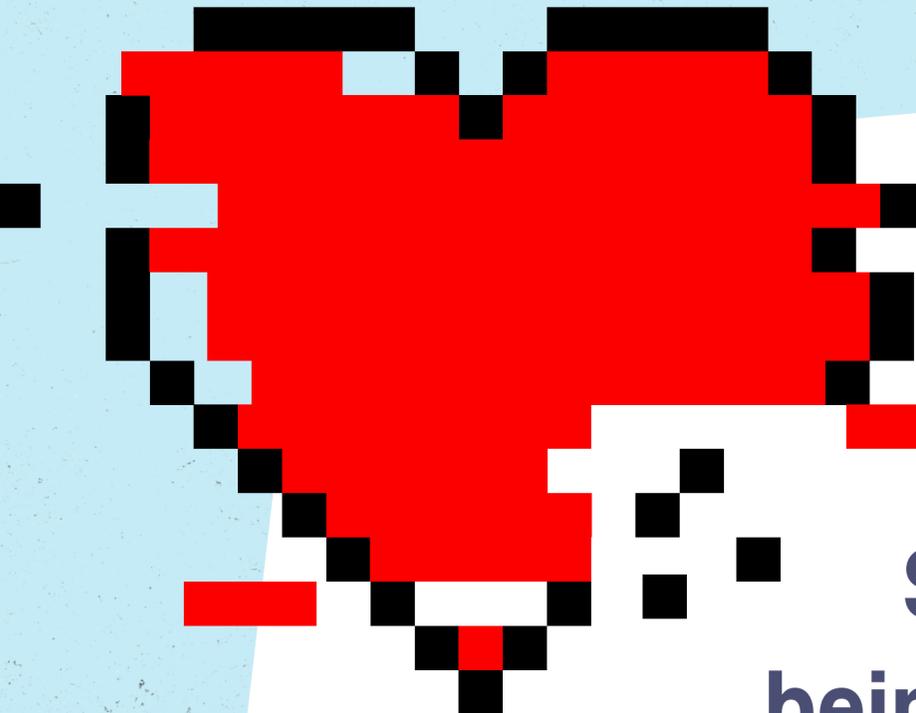


DEINE BESTEN GIFS UND MEMES



DEINE TELEFONNUMMER UND BANKVERBINDUNG





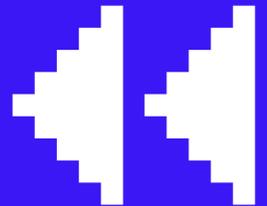
Liebevolle Flirts, große Erwartungen und noch größere Lügen! Was der Tinder-Schwindler kann, machen auch viele andere beim Love-Scamming. In sozialen Netzwerken wie Instagram und Snapchat sowie Dating-Plattformen täuschen die Scammer:innen **mit vermeintlich seriösen Profilen und Fake-Lebensläufen, um eure Daten und Geld zu kommen. Wie sagt man so schön: Vertrauen ist gut ... Zweifel aber noch besser!**

**NÄCHSTE
FRAGE**



FALSCH ANTWORT

REW

NOCHMAL 

8. Wie erkennst du Phishing-Nachrichten in deinem Messenger?



ALS PROFILBILD HAT DER ODER DIE USER:IN EINEN FISCH ALS KOPF.



DU WIRST AUFGEFORDERT EINEN SELTSAMEN LINK ANZUKLICKEN.



EIN FREUND FRAGT DICH, OB DIR DAS GEMEINSAME KONZERT GESTERN GUT GEFIEL.



Enter your email

Password

Next



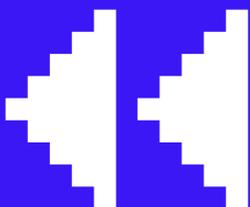
„Das hab ich dir nie geschrieben!“ Habt ihr so schonmal verwirrt über eine dubiose Nachricht gesprochen? Beim Phishing werden wir wie der Fisch an der Angel aus einem Social-Media-Netzwerk mit einem Link rausgelockt und auf einer Website aufgefordert, unseren Namen und Passwörter einzugeben – diese sehen unseren bekannten Plattformen wie Instagram sehr ähnlich. Gesteigert wird der Betrug, wenn wir von vermeintlichen Freund:innen aufgefordert werden einen Link anzuklicken. Die Kontakte sind aber nur Fake. Ziel von Phishing-Nachrichten: unsere persönlichen Daten bekommen.

**NÄCHSTE
FRAGE**



FALSCH ANTWORT

REW

NOCHMAL 

9. Welche Gefahren können durch Deep Fakes entstehen?



EIN VULKAN BRICHT AUS.

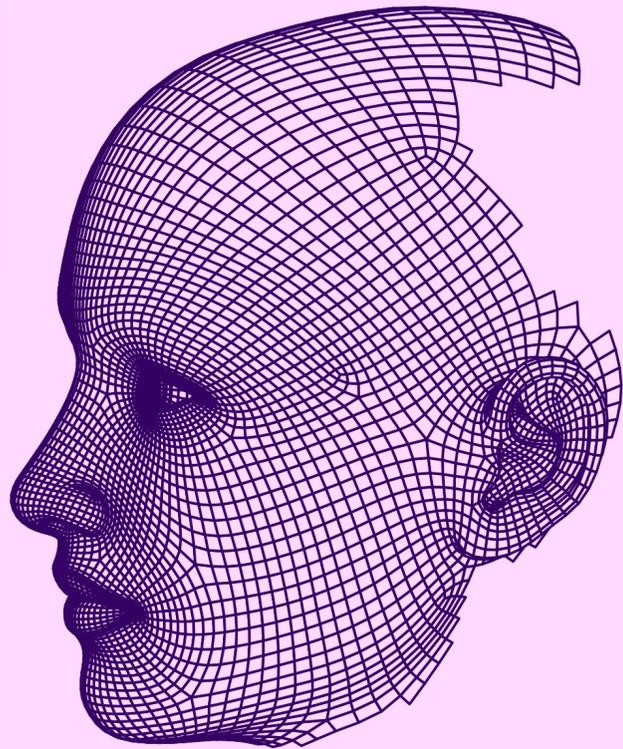


FALSCH INFORMATIONEN WERDEN VERBREITET



DER RUF VON PERSONEN WIRD GESCHÄDIGT

FAKE



„Was?! Das bist gar nicht du?“

Identitäten können durch Künstliche Intelligenz mit wenig Aufwand und überraschend überzeugenden Ergebnis gefaked werden. **Durch Face-**

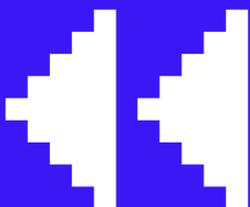
Swapping sehen manche Leute ganz wie andere aus und das in hoher Bild- und Videoqualität. Weil die Ergebnisse von der Wirklichkeit nur schwer zu unterscheiden sind, können leicht falsche Informationen verbreitet und/oder der Ruf von Personen geschädigt werden.

**NÄCHSTE
FRAGE**



FALSCH ANTWORT

REW

NOCHMAL 

10. Seit wann gibt es das Cyber Defense Center?

1989

2014

2022





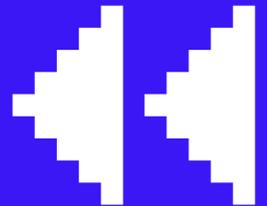
Informationen und Daten sind Macht und müssen geschützt werden. Die Bedeutung von IT-Sicherheit nimmt bei zunehmenden Gefahren zu, weswegen die Telekom 2014 das Cyber Defense Center in Bonn eröffnet hat. Spezialist:innen überwachen dort kontinuierlich IT-Systeme und Websites, um bei Cyber-Attacken zu reagieren.

ENDE



FALSCH ANTWORT

REW

NOCHMAL 

Noch mehr Fakten über Cyber-Sicherheit, soziale Medien und digitale Trends findest du im reif-Onlinemagazin oder auf Instagram.



reif

@reifmagazin

www.reif-magazin.de

powered bei Deutsche Telekom



Erleben, was verbindet.

MacBook

