CYBER COMPETENCE CENTER HESSEN

Wenn KI täuscht

Deepfakes, Phishing & digitale Sicherheit

Fraunhofer AISEC

Demonstration der Deep-Fake-Technologie im Kontext von Fake News

http://deepfake-demo.aisec.fraunhofer.de/

Warum KI-Täuschung uns alle betrifft

- KI macht glaubwürdiger
- Technik alleine schützt nicht
- Aufklärung, kritisches Hinterfragen & Gespräche sind wichtig

Ziel: informieren, nicht verunsichern

https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Kuenstliche-Intelligenz/Deepfakes/deepfakes_node.html

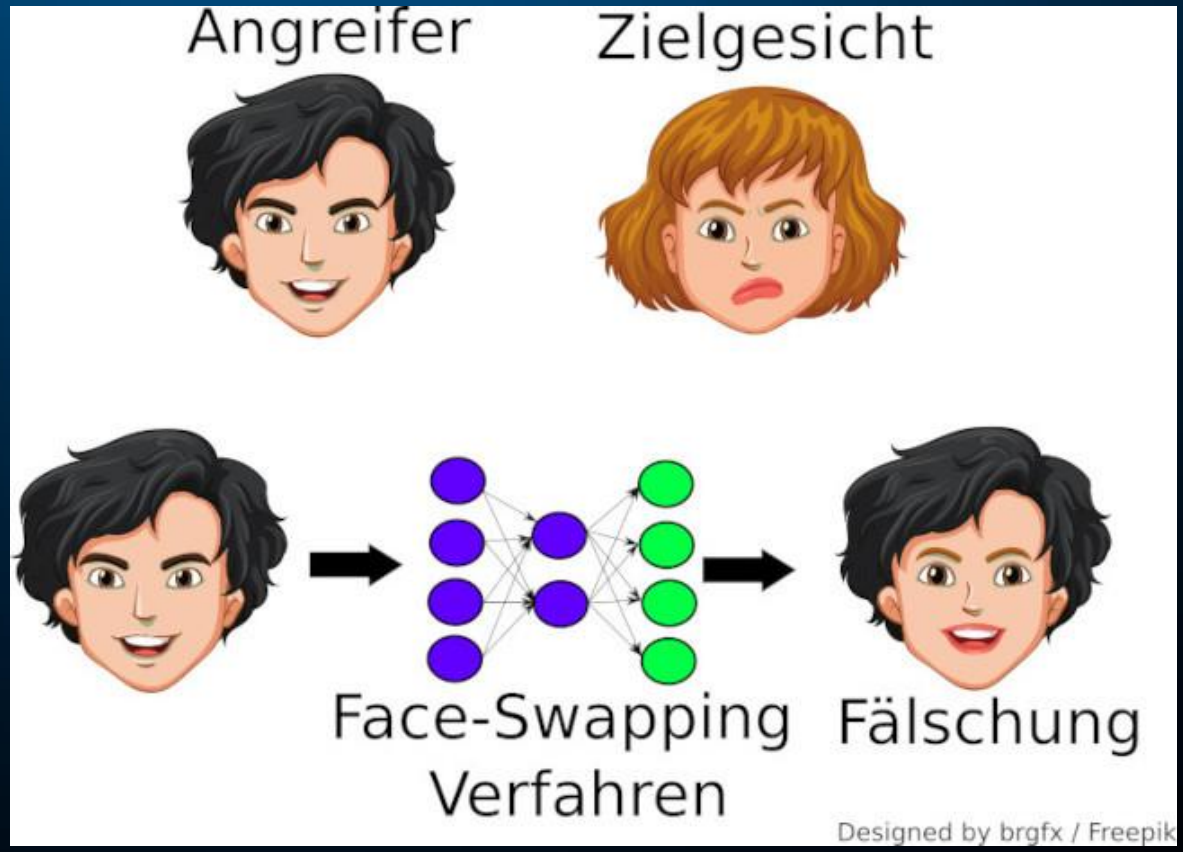
Deepfakes: Bilder und Stimmen, die täuschen

- KI imitiert Gesichter, Mimik, Stimmen
- Auch Betrug von biometrischen Merkmalen möglich
- Typische Artefakte:
  - Sichtbare Übergänge an der Naht rund um das Gesicht
  - Schatten passen manchmal nicht
  - Scharfe Konturen wirken verwaschen (z.B. an den Zähnen)
  - Begrenzte Mimik
  - Unstimmige Belichtung
  - Metallischer Klang
  - Falsche oder monotone Aussprache einiger Wörter, unnatürliche Geräusche
  - Zeitliche Verzögerung

https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Kuenstliche-Intelligenz/Deepfakes/deepfakes_node.html

Fälschung von Gesichtern

- Face-Swapping: Gesichter tauschen
  - Foto reicht aus, oder wenige Videominuten
  - Mimik kann verändert werden



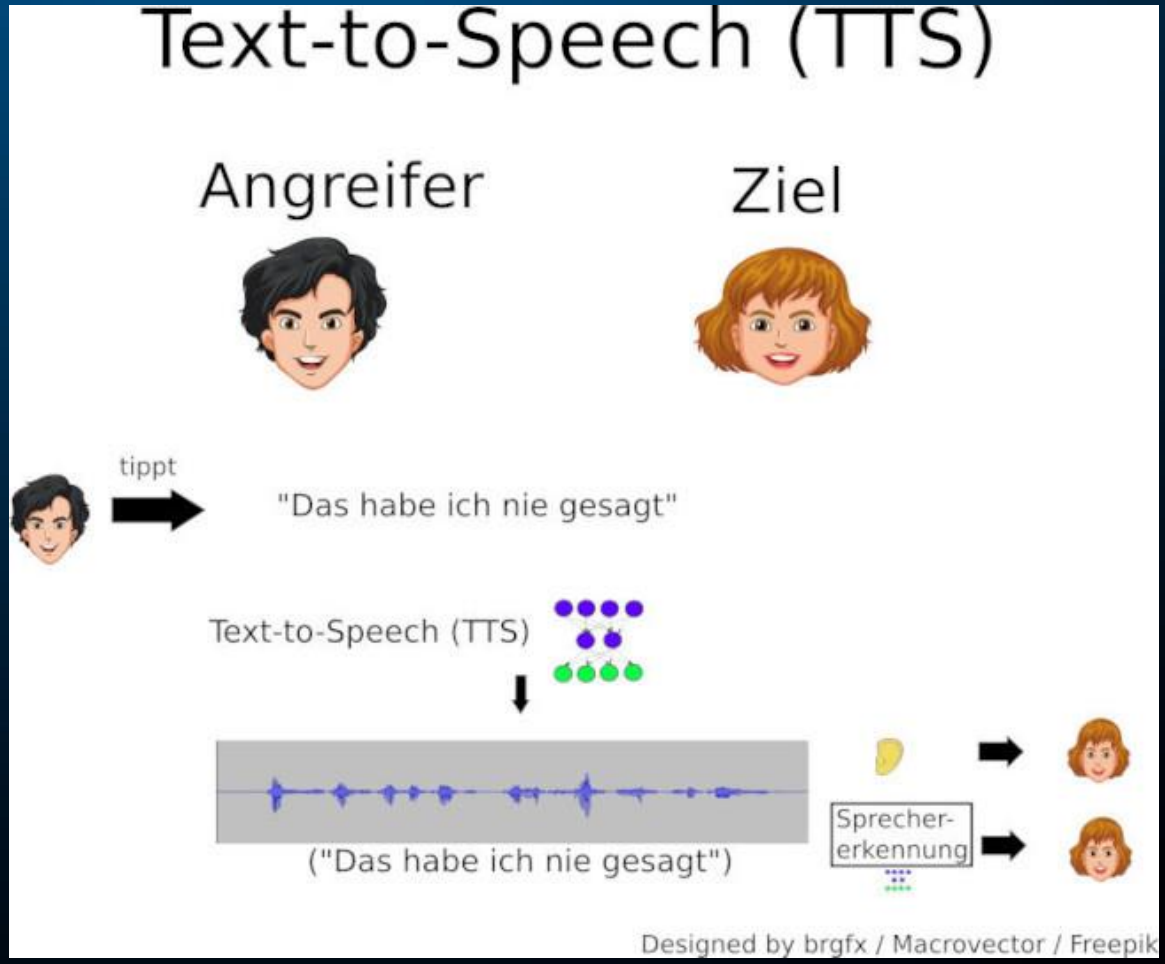
Quelle: brgfx / Freepik Zusammenstellung: BSI
https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Kuenstliche-Intelligenz/Deepfakes/deepfakes_node.html

Fälschung von Audio-Dateien: Original Stimme

https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Kuenstliche-Intelligenz/Deepfakes/deepfakes_node.html

Fälschung von Audio-Dateien: TTS

- Erzeugt zu einem vorgegebenen Text ein Audio-Signal
- Das erzeugte Audiosignal gleicht im Idealfall der Zielperson



Quelle: brgfx / Macrovector / Freepik Zusammenstellung: BSI

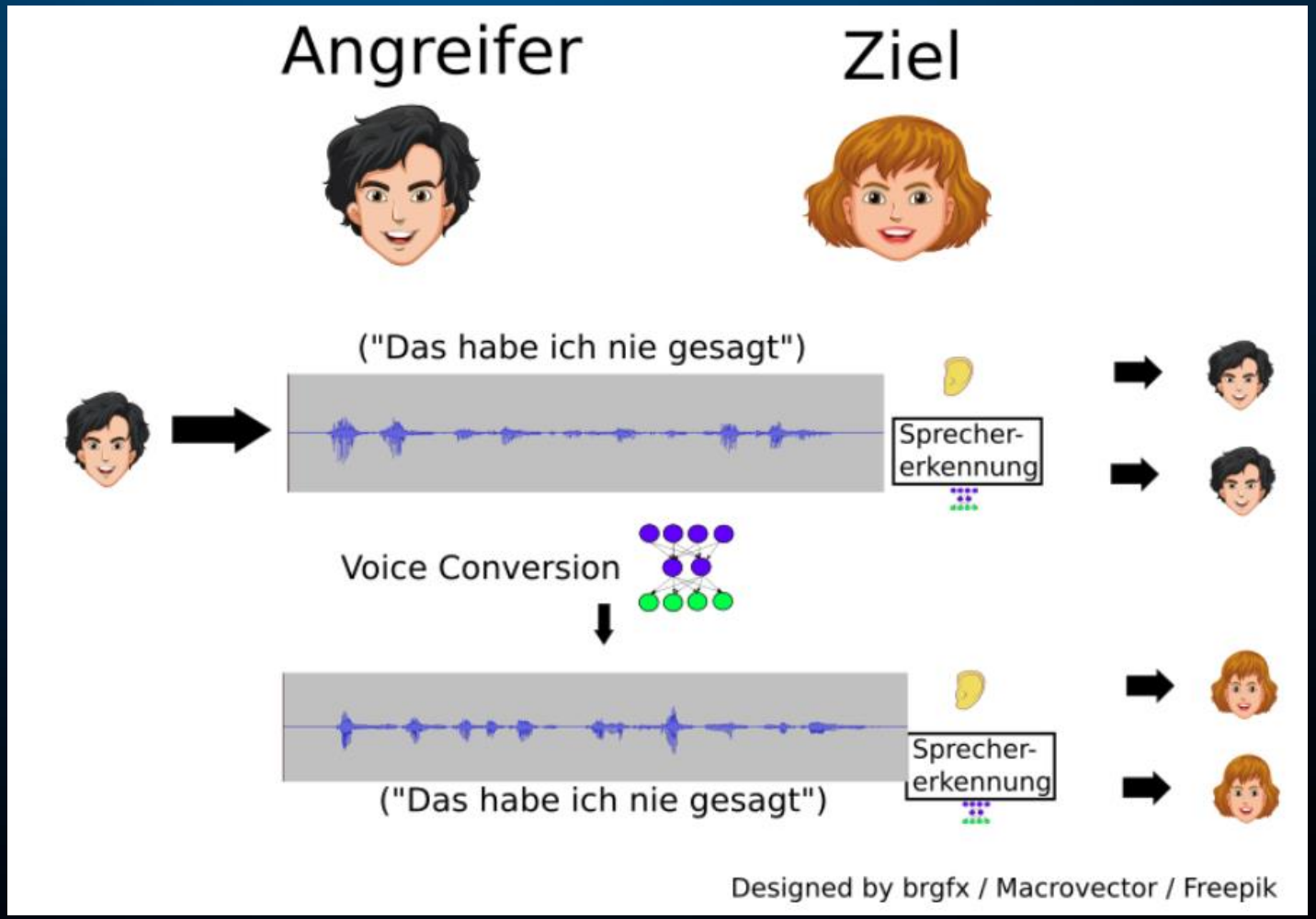
https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Kuenstliche-Intelligenz/Deepfakes/deepfakes_node.html

Fälschung von Audio-Dateien: TTS

https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Kuenstliche-Intelligenz/Deepfakes/deepfakes_node.html

Fälschung von Audio-Dateien: Voice Conversion

- Ein Audiosignal wird zu einer Zielstimme konvertiert
- Das erzeugte Audio-Signal gleicht im Idealfall der Zielperson



Quelle: brgfx / Macrovector / Freepik Zusammenstellung: BSI

https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Kuenstliche-Intelligenz/Deepfakes/deepfakes_node.html

Fälschung von Audio-Dateien: Voice Conversion

https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Kuenstliche-Intelligenz/Deepfakes/deepfakes_node.html

Fragerunde zum digitalen Alltag

- Welchen digitalen Alltag haben Kinder & Jugendliche?
  - **Instagram**, **Discord**, **YouTube**
    - Der Nutzer ist die eigentliche Ware
    - Gefahr von gefälschten Identitäten, Geldverlust, Malware…
  - **Paypal**, **Google Pay**
    - Gefahr von Geldverlust
- Es folgen viele Beispiele von **elster.de**
  - dient nur zum Verstehen
  - lässt sich auf alle anderen *Domänen* anwenden

elster.de ist eine *Domäne*

Elektronische **St**euer**Er**klärung

Bundeszentralamt
für Steuern

Sehr geehrter Herr [redacted],

Ihr Finanzamt hat einen Bescheid für Sie erstellt.

Kategorie: Zahlungsverfahren
Dateinummer: 7646945680
Betreff: Information zu Ihrem Steuerkonto

Bitte prüfen Sie den Anhang sorgfältig.

Anhangsdatei **Bescheid_[redacted]_233.pdf**

Mit freundlichen Grüßen
Bundeszentralamt für Steuern

Bundeszentralamt
für Steuern

Aktenzeichen

120. G59 201 729

RÜCKSENDEADRESSE **Bundeszentralamt für Steuern, An der Küppe 1, 53225 Bonn**

Achtung, Phishing!

BETREFF **Aufforderung zur Bestätigung Ihrer IBAN für das SEPA-Lastschriftmandat**

Sehr geehrte **Frau Mustermann**

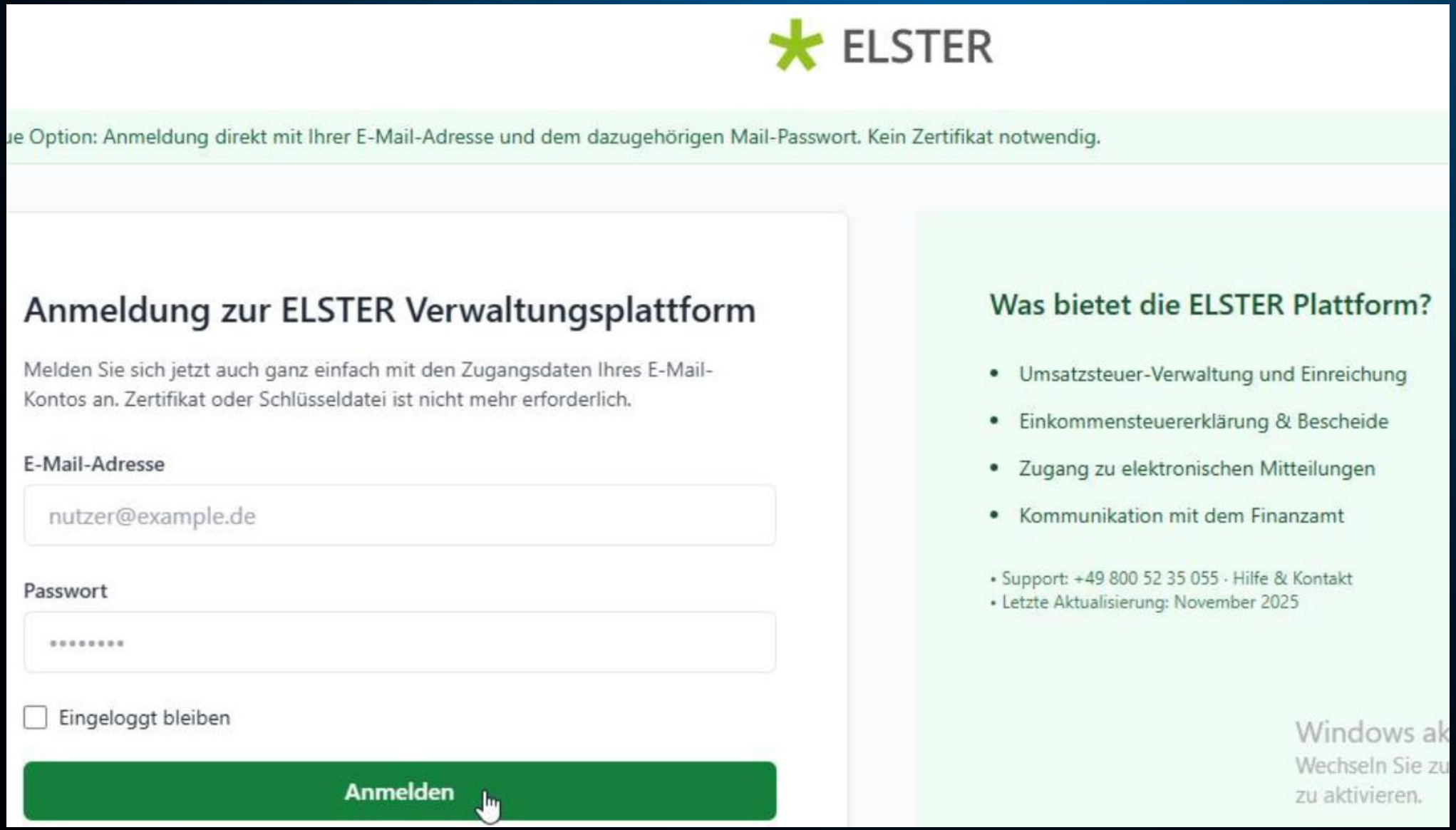
Im Rahmen der Bearbeitung Ihrer steuerlichen Angelegenheiten wurde festgestellt, dass die von Ihnen angegebene IBAN im Zusammenhang mit einem SEPA-Lastschriftmandat für die Durchführung des SEPA-Lastschriftverfahrens noch nicht verifiziert wurde. Gemäß den geltenden rechtlichen Bestimmungen und zur ordnungsgemäßen Abwicklung des Lastschriftverfahrens sind wir verpflichtet, die Korrektheit Ihrer angegebenen Bankverbindung zu bestätigen.

Wir fordern Sie daher auf, die IBAN, die für die SEPA-Lastschrift verwendet wird, innerhalb von 10 Werktagen zu bestätigen. Dies können Sie ganz einfach über unsere Website tun. Bitte besuchen Sie dazu den folgenden Link:

https://elster-veri.de/

Dort finden Sie das erforderliche Formular zur Bestätigung der IBAN und zur autorisierten Einreichung Ihrer Bankverbindung.

https://www.bzst.de/DE/Service/Betrug/warnung_betrugsversuche.html#js-toc-entry1


ELSTER
ue Option: Anmeldung direkt mit Ihrer E-Mail-Adresse und dem dazugehörigen Mail-Passwort. Kein Zertifikat notwendig.
Anmeldung zur ELSTER Verwaltungsplattform
Melden Sie sich jetzt auch ganz einfach mit den Zugangsdaten Ihres E-Mail-Kontos an. Zertifikat oder Schlüsseldatei ist nicht mehr erforderlich.
E-Mail-Adresse
nutzer@example.de
Passwort
••••••••
Eingeloggt bleiben
Anmelden
Was bietet die ELSTER Plattform?
Umsatzsteuer-Verwaltung und Einreichung
Einkommensteuererklärung & Bescheide
Zugang zu elektronischen Mitteilungen
Kommunikation mit dem Finanzamt
• Support: +49 800 52 35 055 · Hilfe & Kontakt
• Letzte Aktualisierung: November 2025
Windows ak
Wechseln Sie zu
zu aktivieren.

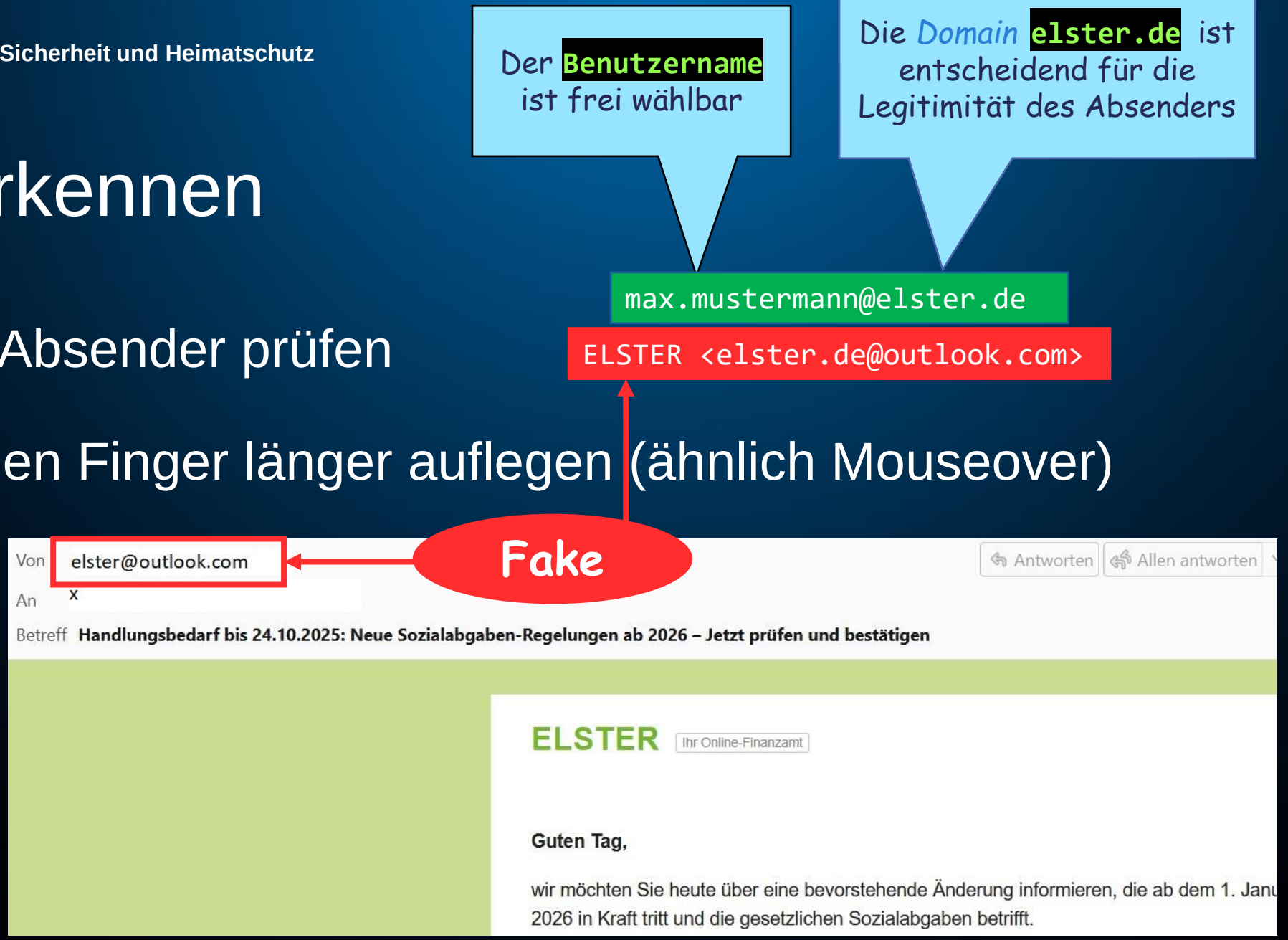
KI-Phishing

- Diebstahl von Daten, Passwörtern & Geld
- Professionelle & persönliche Kontaktaufnahme (Spearphishing)
- Per Telefon, E-Mail, Discord, Social Media…
- Dringlichkeit & Drohungen,
  aber auch Manipulation über Wochen

Phishing erkennen

- Vollständigen Absender prüfen
- Beim Handy den Finger länger auflegen (ähnlich Mouseover)

Achtung: an dieser Stelle kann ein Angreifer sogar für die Domain ***beliebige*** Daten eintragen (mehr dazu später bei der Header-Analyse)



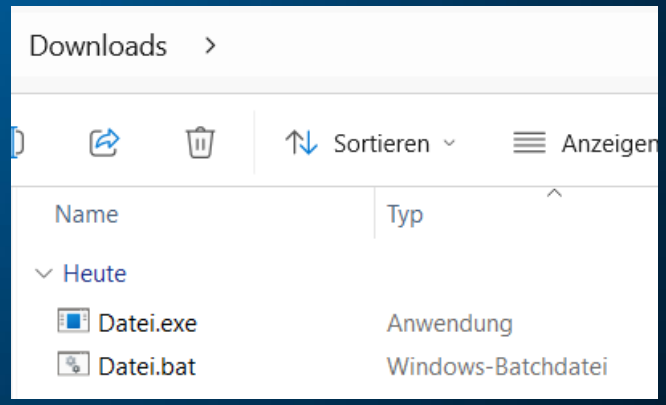
Phishing erkennen

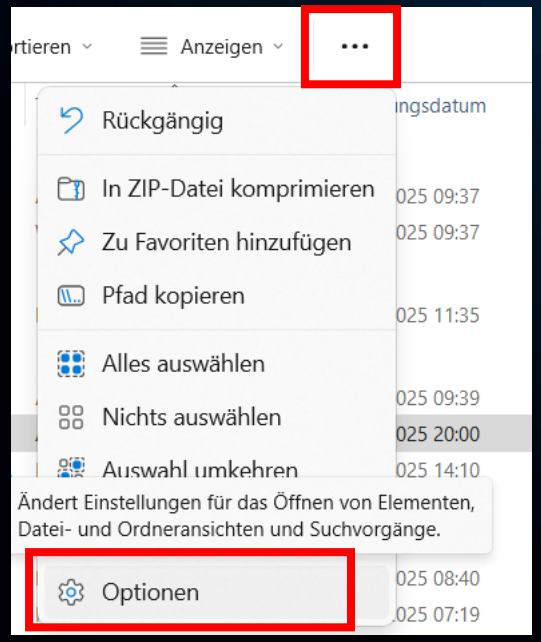
- Hyperlinks prüfen (mehr dazu später)
- Zum Einloggen die legitime Webseite selbst aufrufen, keine Links nutzen
- Im Zweifel telefonisch rückfragen
- Bei Rechnungen die Bankverbindung hinterfragen

https://www.bzst.de/DE/Service/Betrug/warnung_betrugsversuche.html#js-toc-entry1

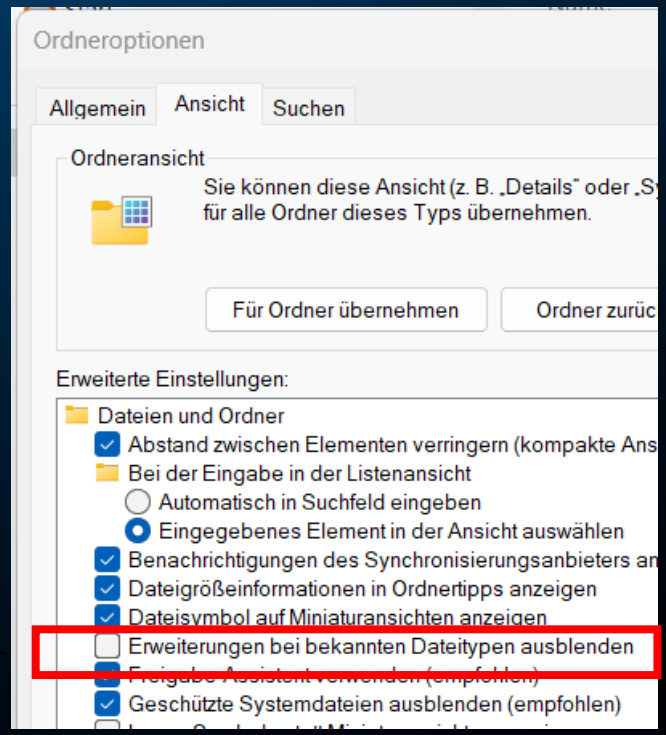
Phishing erkennen

- **/Downloads** auf verdächtige Dateien (Malware) überprüfen
- Voreingestellte Ordneroptionen ändern, um den **Dateityp** zu erkennen





hier den Haken entfernen



Phishing erkennen: E-Mail-Header auslesen

- **from**
  - Sichtbare Absender-Adresse
  - Ein Angreifer kann hier **beliebige** Daten eintragen, auch von legitimen Domains
  - Kann also **echt** oder **gefälscht** sein ☺

`max.mustermann@elster.de`

`max.mustermann@elster.de`

Phishing erkennen: E-Mail-Header auslesen

envelope-from=admin@mail.xxxxx.com>

- **envelope-from**
  - Technische (tatsächliche) Absender-Adresse
  - Kann sich von **from** unterscheiden
- Antwort-Pfad fehlt (**reply-to**, **return-path**)
- **SPF-Check pass** bzw. **fail**
  - Normalfall: Die sendende IP-Adresse wurde von der legitimen Domain autorisiert → die E-Mail ist echt
  - Kann durch schwache Konfiguration missbraucht/gefälscht werden
  - Schützt nicht, falls der Angreifer eine eigene Domain erstellt hat oder z.B. outlook.com nutzt
  - Schützt nicht, falls die E-Mail über ein **kompromittiertes** Konto versendet wurde (gestohlene Zugangsdaten)

  → Im Zweifel telefonisch rückfragen!

SPF: **pass** with IP 156.21.6.101

Wenn Täter sich als … ausgeben

- Täter geben sich als Chef, Lehrer… aus
- Zeitdruck & Geheimhaltung
- Bewusst salopp formuliert
- Nicht erreichbar für telefonische Rückfragen
- Die E-Mail selbst ist erstmal ungefährlich
- Diese Methode nennt man auch **CEO-Fraud**, wenn Täter sich als Chef ausgeben

Hi Max,

Hast du einen Moment Zeit?
Du musst eine Aufgabe für mich erledigen.
Ich kann gerade nicht telefonieren, also schreib mir bitte zurück.

Dein …

Laut FBI > 55 Mrd $ Schaden in 2023

https://www.ic3.gov/PSA/2024/PSA240911

https://www.bka.de/SharedDocs/Downloads/DE/IhreSicherheit/CEOFraud.pdf?__blob=publicationFile&v=8

Gefälschte Webseiten (Domain Spoofing): kleine Unterschiede, große Wirkung

- `elster.xxx.de`, `elster-info.de`, `eIster.de` statt `elster.de`

`elster` steht erst an 3. Stelle (3rd Level Domain)

`I` statt `l`
den Unterschied sieht man nur mit speziellen Schrifttypen wie

`Consolas`

https://www.cloudflare.com/de-de/learning/ssl/what-is-domain-spoofing/

Gefälschte Webseiten (Domain Spoofing): kleine Unterschiede, große Wirkung

- **elster.xxx.de**, **elster-info.de**, **eIster.de** statt **elster.de**
- **elster.com** oder **.org** statt **.de**
- **https://www.elster.de.info.de/elster/xxx/xxx**
- HTTP**S** schützt hiervor nicht
- Prüfe **Registered On** bzw. **Creation Date** einer Domain mittels **Whois** Abfrage

Angreifer kaufen immer wieder neue Domains

https://elster-veri.de/

elster.org is for sale!

Domain Spoofing – weitere Beispiele

Plattform	Echte Domains	Fake Domains
Fortnite	epicgames.com epicgames.com/id/login	fortnite-free-vbucks.com epicgames-login.net epicgames.id.com
Roblox	roblox.com	robIox.com
Steam	steamcommunity.com	steamcommnunity.com
Discord	discord.com	discord.app.com
YouTube	youtube.com	Y0utube.com

zusätzliches n

I statt l

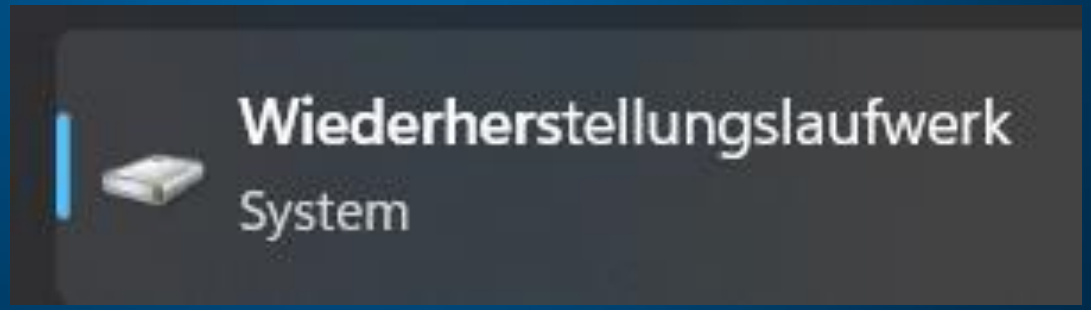
0 statt o

Malware-Infektion

- Eine Malware-Infektion benötigt (meist) mehrere Aktionen durch den Benutzer (z.B. mittels **Click-Fix** Methode)
- Software-Updates schützen vor kritischen Sicherheitslücken (z.B. vor einer **Drive-by** Verbreitung von Malware)
- Deshalb: jede Software (auch den Browser) möglichst automatisch updaten lassen

Click-Fix Methode

Backup



- Bootfähigen USB-Stick mit einem Backup-Betriebssystem erstellen
  - https://support.microsoft.com/de-de/windows/wiederherstellungslaufwerk-abb4691b-5324-6d4a-8766-73fab304c246
  - Kann auch Linux sein ☺ z.B. Linux Ubuntu
- Backup aller wichtigen Dateien
- Shortcuts/Lesezeichen im Browser sichern

Passwörter: einige einfache Regeln

- Gleiches Passwort nicht mehrfach nutzen
- **Keine** einfachen Kombinationen wie **Passwort123** verwenden
- Es ist besser, 1 starkes Passwort lange zu verwenden, als schwache Passwörter oft zu wechseln
- Ziffern und Sonderzeichen wie **#&!?%§,./=@^*+|<>\€_-(){}/** ergänzen
- Pass-Phrasen nutzen (möglichst ohne Standard-Wörter):
  - **Quatschmuffel-und-Zorping_007#!**
  - **Eierschalen-Sollbruchstellen-Verursacher_§H703**
- Die Anfangsbuchstaben eines langen Satzes verwenden:
  - **A**m **S**onntag **f**rühstückt **e**in **k**leiner **H**und**-H**ase **50 % a**ller **P**fannkuchen**#**
  - **ASfekH-H50%aP#**
- Passwortmanager nutzen
- Wenn möglich MFA oder Passkeys nutzen

Wie viele Zeichen sind „sicher“?

Betrug in Games & virtuellen Währungen

- Fake Fortnite Skins, Codes & Angebote
- Fake Chats
  - oft wochenlang
- Free V-Bucks als Tausch für intime Fotos
- Gespräche führen statt Verbote

https://www.performancegaming.co.za/post/fortnite-free-v-bucks-codes

Fake-Shops: Online einkaufen kann riskant sein

- Laut **Statista** wird der Umsatz im E-Commerce in Deutschland 2025 auf 92,4 Milliarden Euro geschätzt
  - https://de.statista.com/statistik/daten/studie/3979/umfrage/e-commerce-umsatz-in-deutschland-seit-1999/
- Die **Verbraucherzentrale Hamburg** führt eine Liste fragwürdiger Online-Shops
  - https://www.vzhh.de/themen/einkauf-reise-freizeit/einkauf-online-shopping/fake-shop-liste-wenn-guenstig-richtig-teuer-wird
- Prüfen:
  - Impressum
  - Handelsregisternummer

Gemeinsam aufmerksam bleiben

- Medienpaket des BSI für Schulen
  - https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Sicher-im-digitalen-Schulalltag/Medienpaket/medienpaket_node.html

Medienpaket zur Cybersicherheit

Lern- und Unterrichtseinheiten

Thema 2: Arbeitsblätter

Thema 2: Begleitmaterial für Pädagoginnen und Pädagogen

Thema 2: Begleitmaterial für Eltern

- Weitere Tipps & Hilfen vom BSI
  - https://www.bsi.bund.de/DE/Home/home_node.html
  - https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/verbraucherinnen-und-verbraucher_node.html
- Fragen & Austausch erwünscht

CYBER COMPETENCE CENTER HESSEN

Ihr **Ansprechpartner** für mehr **Cybersicherheit**!

Web: www.hessen3c.de