

Herzlich willkommen!

Zum Thema Digitale Selbstverteidigung- Sicherheit im Internet

Referentin: Theresa Kuper

Gefördert vom:



Was ist der Digitale Engel?



Gefördert vom:



Bundesministerium
für Familie, Senioren, Frauen
und Jugend

Ein Projekt von:



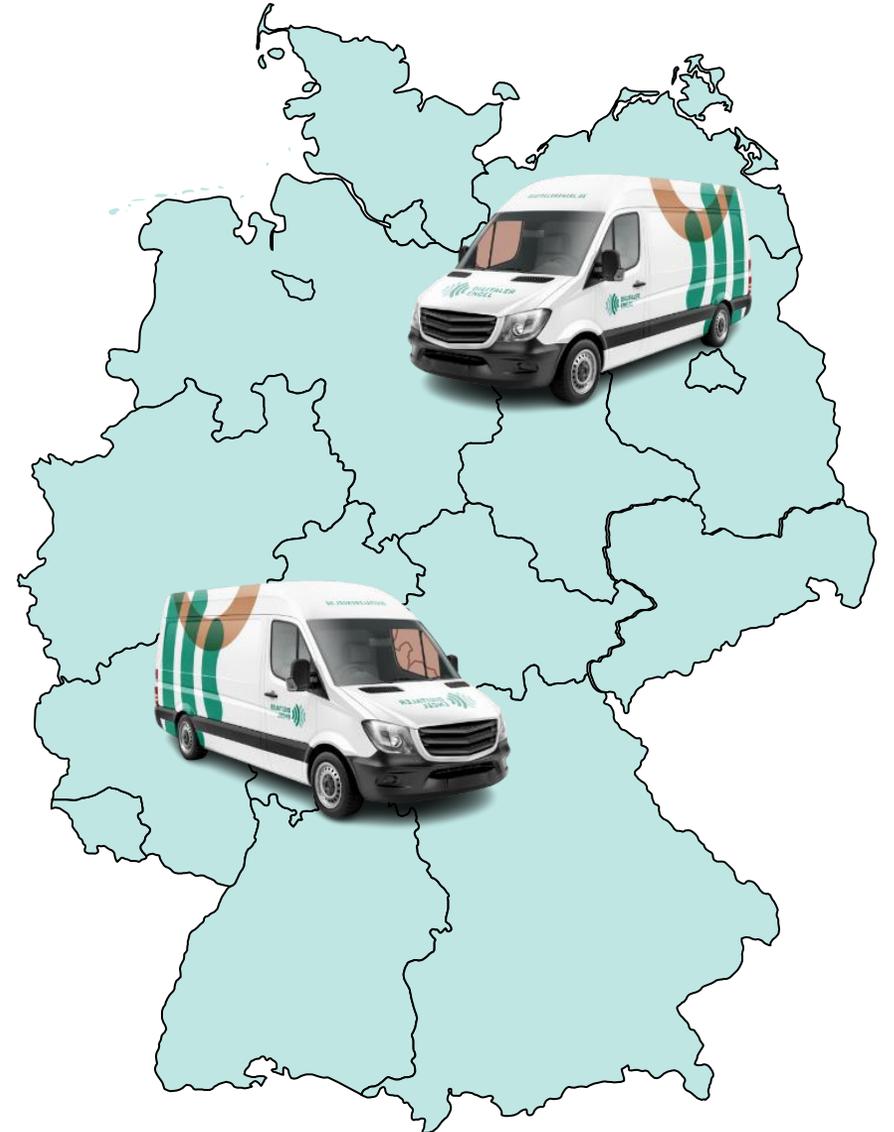
**Deutschland
sicher im Netz**

Was ist der Digitale Engel?

**praxisnahe Vermittlung digitaler
Anwendungen für ältere Menschen**

mit zwei Info-Mobilen quer durch Deutschland:

- Mehrgenerationenhäuser
- Seniorentreffs
- Kommunen
- Marktplätze
- Stadtfeste etc.



Was ist der Digitale Engel?

Weitere Angebote des Digitalen Engel



Online-Schulungen für Wissensvermittelnde

Menschen aus dem Umfeld Älterer werden befähigt, ihr Digitalwissen weiterzugeben und ein eigenes Angebot für Ältere zu gestalten.



Digitaler Engel vor Ort

Junge Freiwillige in Einrichtungen der Altenhilfe werden befähigt, ihr Digitalwissen weiterzugeben und älteren Menschen digitale Kompetenzen zu vermitteln.

Das Team vom Digitalen Engel



Petra Rollfing



Mobilreferentin

Katharina Kunze



Projektleiterin

Johannes Diller



Mobilreferent

Theresa Kuper



Referentin

Kerstin Schötschel



Sachbearbeiterin

Nora Bramati



Tourenplanung

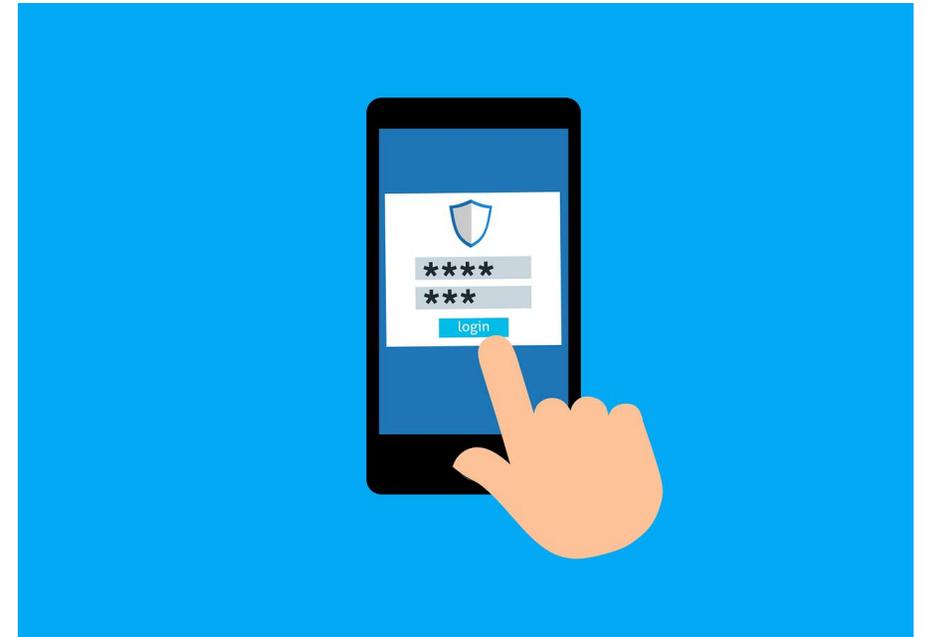
Can Felix Demirden



Öffentlichkeitsarbeit

Agenda

1. Sichere Passwörter
2. Cookies
3. Umgang mit Phishing
4. Weitere Tipps
5. Weiterführende Informationen



Bildquelle: www.pixabay.com

Überblick über die IT-Sicherheitslage in Deutschland

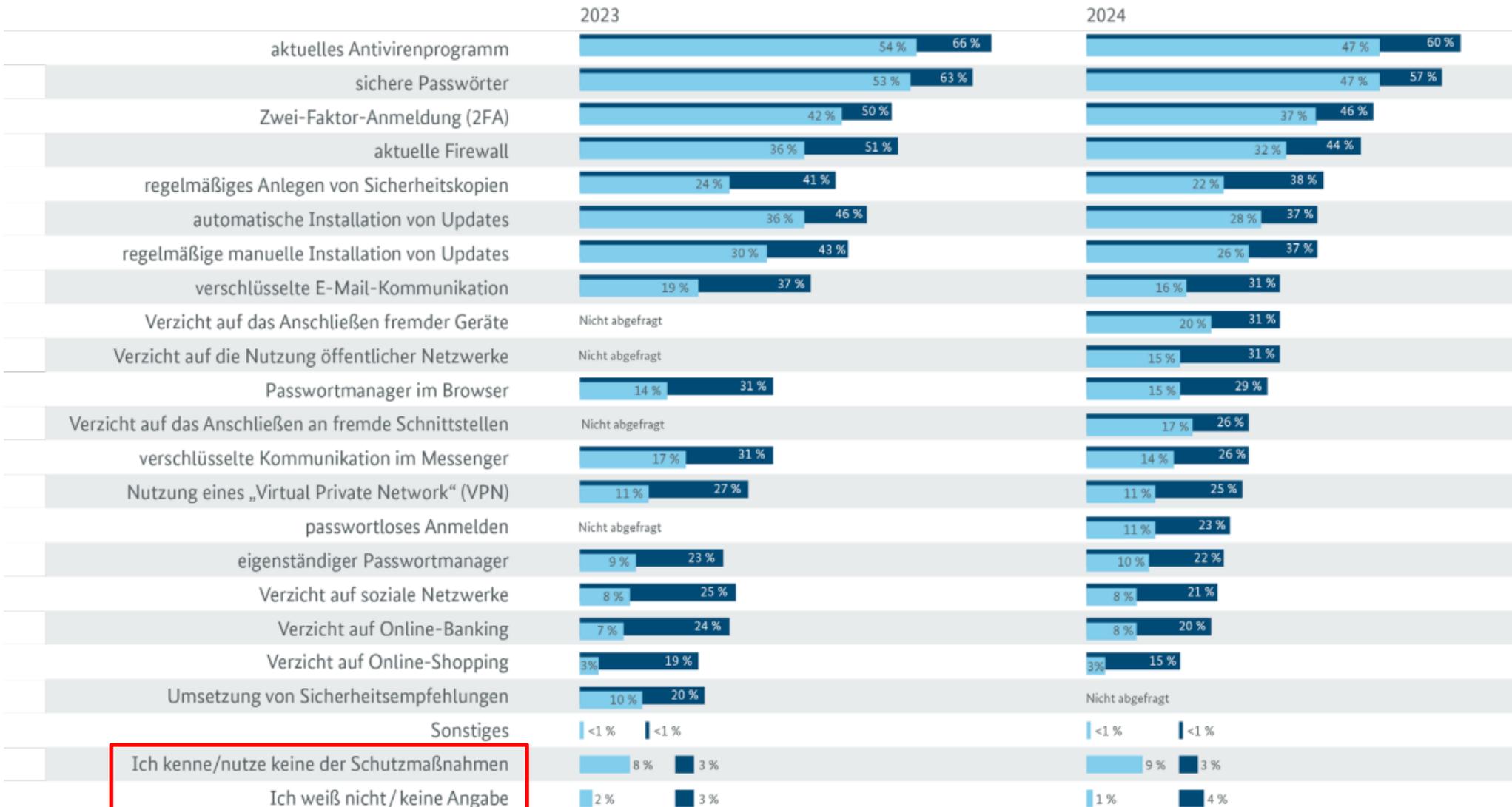
Sie haben angegeben, in den vergangenen 12 Monaten Opfer von Cyberkriminalität gewesen zu sein.

Um welche Art(en) von Straftat(en) handelte es sich dabei? ■ 2024 ■ 2023



Welche der folgenden Schutzmaßnahmen vor Gefahren im Internet kennen Sie?

Wie schützen Sie sich vor Gefahren im Internet? Ich schütze mich durch...



Sicherheit im Internet

Bildquelle: www.bsi.bund.de

1. Sichere Passwörter

1. Passwort

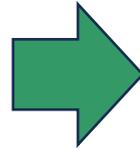
- Funktion eines Haustürschlüssels:
Kontrolle des Zugangs zu Daten und Systemen
- Erster Einsatz in den 1960ern durch den US-Computerwissenschaftler Fernando J. Corbató , um einzelne Dateien innerhalb eines Computersystems zu schützen.



Bildquelle: www.pixabay.com

1. Meistverwendete Passwörter

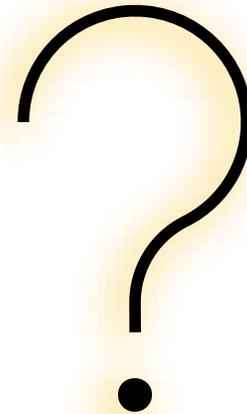
1. 123456
2. passwort
3. 12345
4. hallo
5. 123456789
6. qwertz
7. schatz
8. basteln
9. berlin
10. 12345678



Können in unter einer Sekunde von
Hackern entschlüsselt werden

1. Welches Beispiel ist am schwersten zu erraten?

- a) SmartPhone
- b) Smartphone
- c) Sp12!
- d) SmarT123!One



1. Ein sicheres Passwort ist

einmalig

Unterschiedliche Passwörter für unterschiedliche Konten

kreativ

Fantasiewörter oder Dialekte, die kein Wörterbuch kennt

lang

Mindestens 8 Zeichen lang

komplex

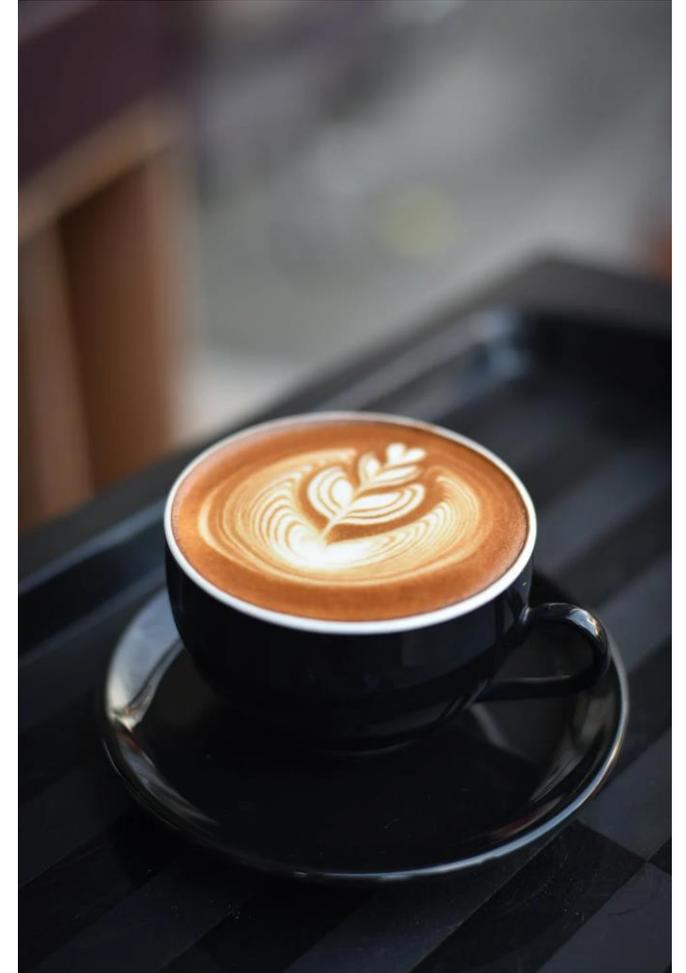
**verschiedene Klein- und Großbuchstaben, Sonderzeichen
und Zahlen**

1. Passwörter merken und erstellen: Merksatzmethode

Einen Satz auswählen, den Sie sich gut merken können und den 1. Buchstaben auswählen + App (Beispiel **K**leinzeigen)

Ich **t**rinke jeden **M**orgen eine **T**asse
Kaffee **p**lus einem **S**pritzer **M**ilch.

➤ ItjM1TK+1SMK.

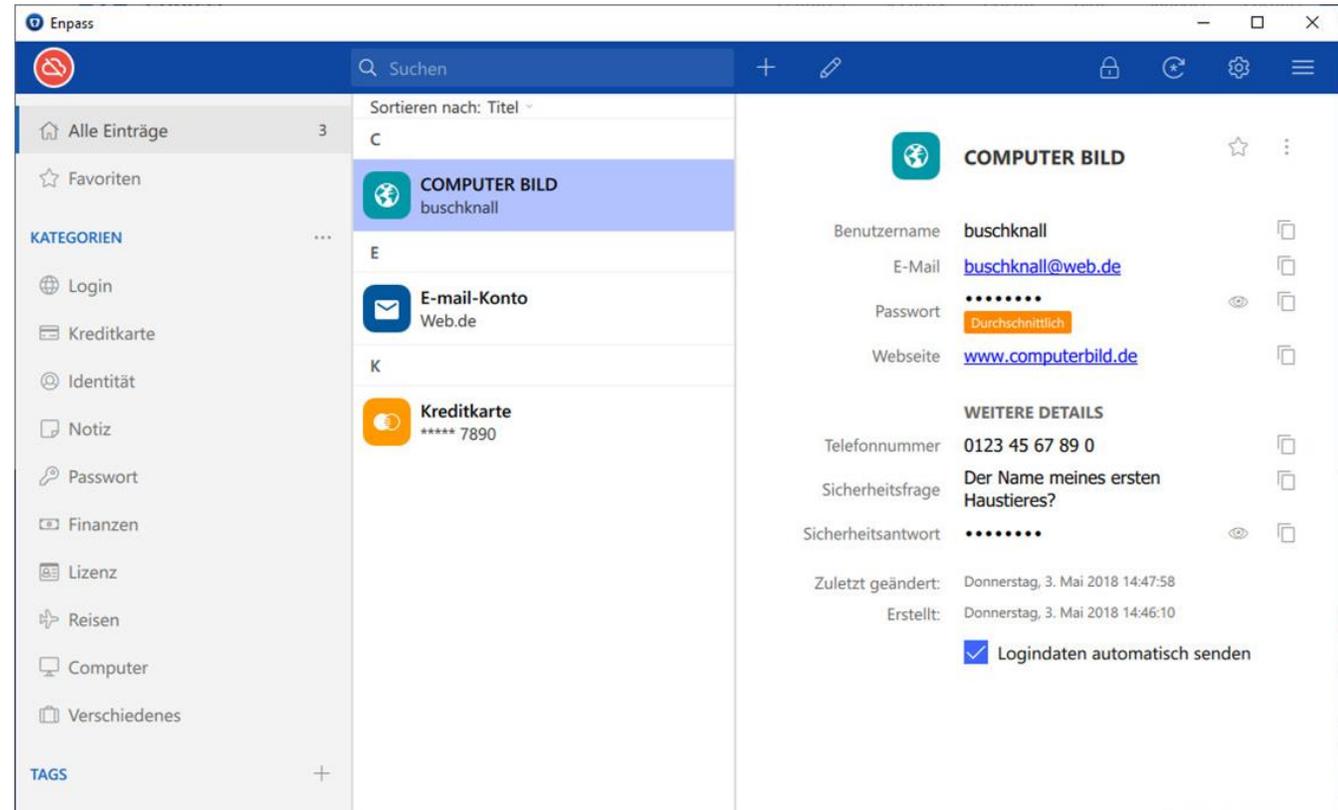


Bildquelle: www.pexels.com

1. Passwörter merken und erstellen mittels eines Passwort- Managers

1. Wie funktioniert ein Passwort-Manager?

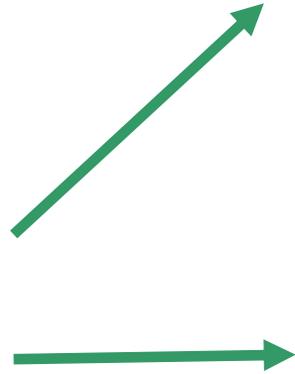
- Programme, die Benutzernamen und Passwörter verwalten
- Sichere Verwahrung von Passwörtern mittels Verschlüsselung und eines komplexen Masterpassworts
- Funktionsweise ähnlich wie ein Notizbuch, das in einer Schublade eingeschlossen ist



Bildquelle: www.computerbild.de

1. Beispiele für Passwort-Manager

- Enpass
- 1Password
- Keeper
- Dashlane
- LastPass
- NordPass

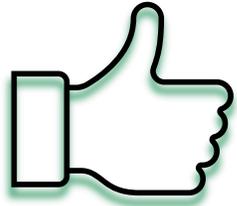


im Internet für Windows-PCs oder für Mac herunterladen und installieren

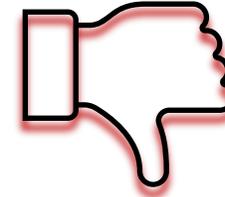
Als App im Google Play Store und im Apple Store

Apple-Geräte enthalten
Passwortmanager „Schlüsselbund“
→ in den Einstellungen zur iCloud

1. Vor- und Nachteile



- Nur ein Passwort merken
- Verwahren von Passwörtern und Benutzernamen: Erleichtert digitalen Nachlass
- Unterstützung bei der Passwortvergabe
- Warnung vor gefährdeten Websites und möglichen Phishing-Attacken
- Synchronisieren möglich



- Beim Vergessen des Masterpassworts sind im schlechtesten Fall alle Daten verloren → viel Arbeit wiederherzustellen
- Alle Passwörter können bei einem Cyber-Angriff auf einmal gestohlen werden

1. Auswahl des Passwort-Managers

Was sollten Sie bei der Auswahl eines Passwort-Managers beachten?

- A Sicherheitsmaßnahmen in Datenschutzerklärung durchlesen
- B Standort des Servers in Deutschland
- C Bewertungen im Internet durchlesen
- D Standort des Servers in Europa

1. Auswahl des Passwort-Managers

Was sollten Sie bei der Auswahl eines Passwort-Managers beachten?

A Sicherheitsmaßnahmen in Datenschutzerklärung durchlesen



B Standort des Servers in Deutschland

C Bewertungen im Internet durchlesen

D Standort des Servers in Europa



1. Zwei-Faktor-Authentifizierung (2FA)

Nach Aktivierung: Mehr als ein
Passwort wird benötigt, um Zugang
zum Account zu erhalten

Erster Faktor

- Passwort



Zweiter Faktor

- Besitz
- Biometrie



Bildquelle: www.pixabay.com

2. Cookies

2. Cookies

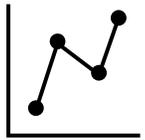


- kleine Textdateien, die über eine Webseite im Internetbrowser eines Nutzers gespeichert werden können

Bildquelle: www.unsplash.com

2. Kategorien von Cookies

✓ Notwendige/ Erforderliche/ Wesentliche Cookies



Leistungs-/Analyse-/Statistik-Cookies



Marketing-/ Werbe-/ Personalisierungs-Cookies

2. Cookies



Wir nutzen Technologien auf unserer Webseite, die personenbezogene Daten wie IP-Adressen verarbeiten. Details dazu und zu Ihren Rechten finden Sie in unserer Datenschutzerklärung sowie im Impressum. Ihre Einwilligung ist freiwillig und kann jederzeit unter Einstellungen oder im Footer der Webseite unter Datenschutzeinstellungen bearbeiten/widerrufen widerrufen werden.

Einige Dienste verarbeiten Daten in den USA, wo der Datenschutz als unzureichend gilt. Mit Ihrer Einwilligung stimmen Sie der Verarbeitung nach Art. 49 (1) lit. a DSGVO zu.

Alle akzeptieren

**Nur essenzielle Cookies
akzeptieren**

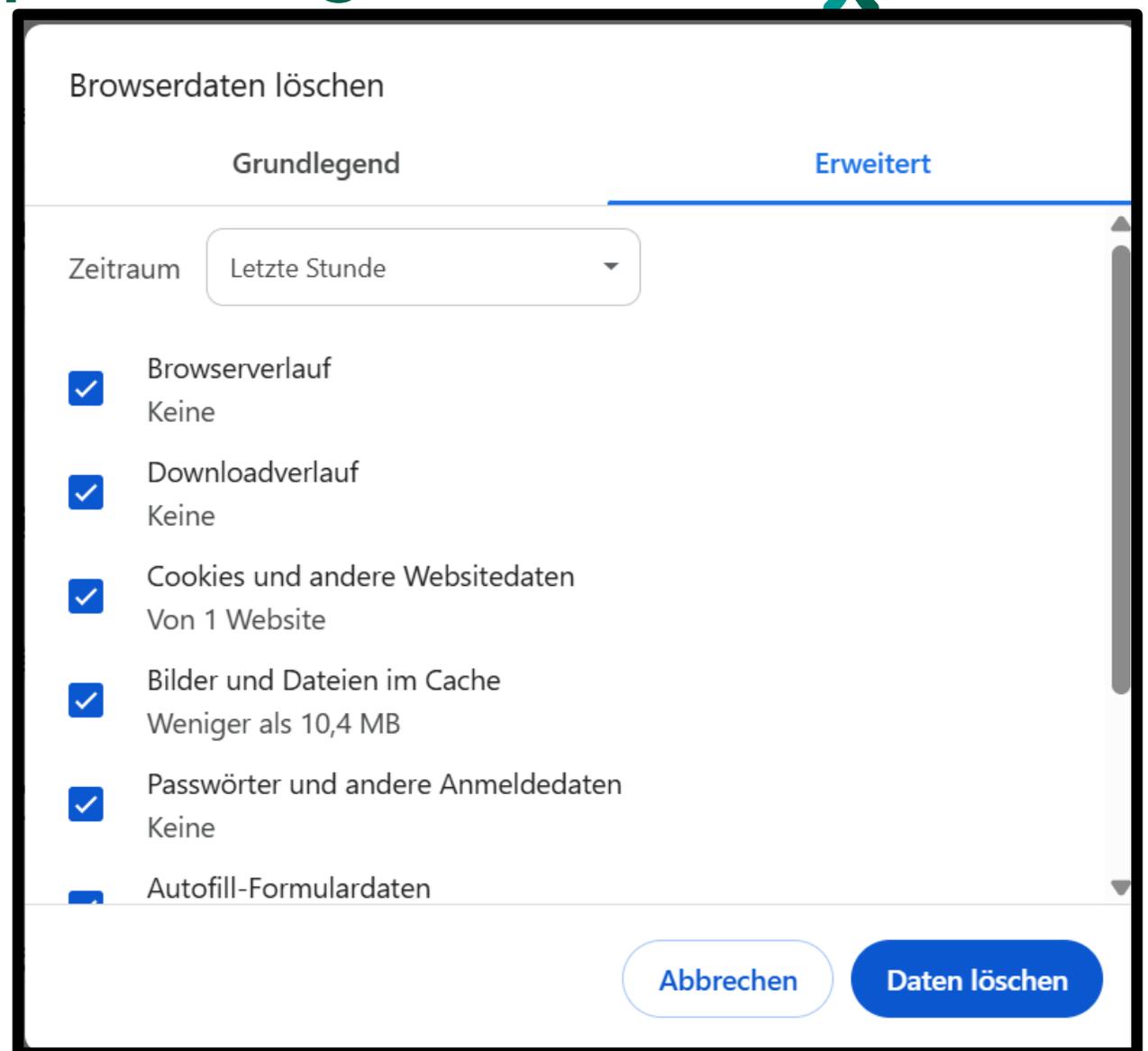
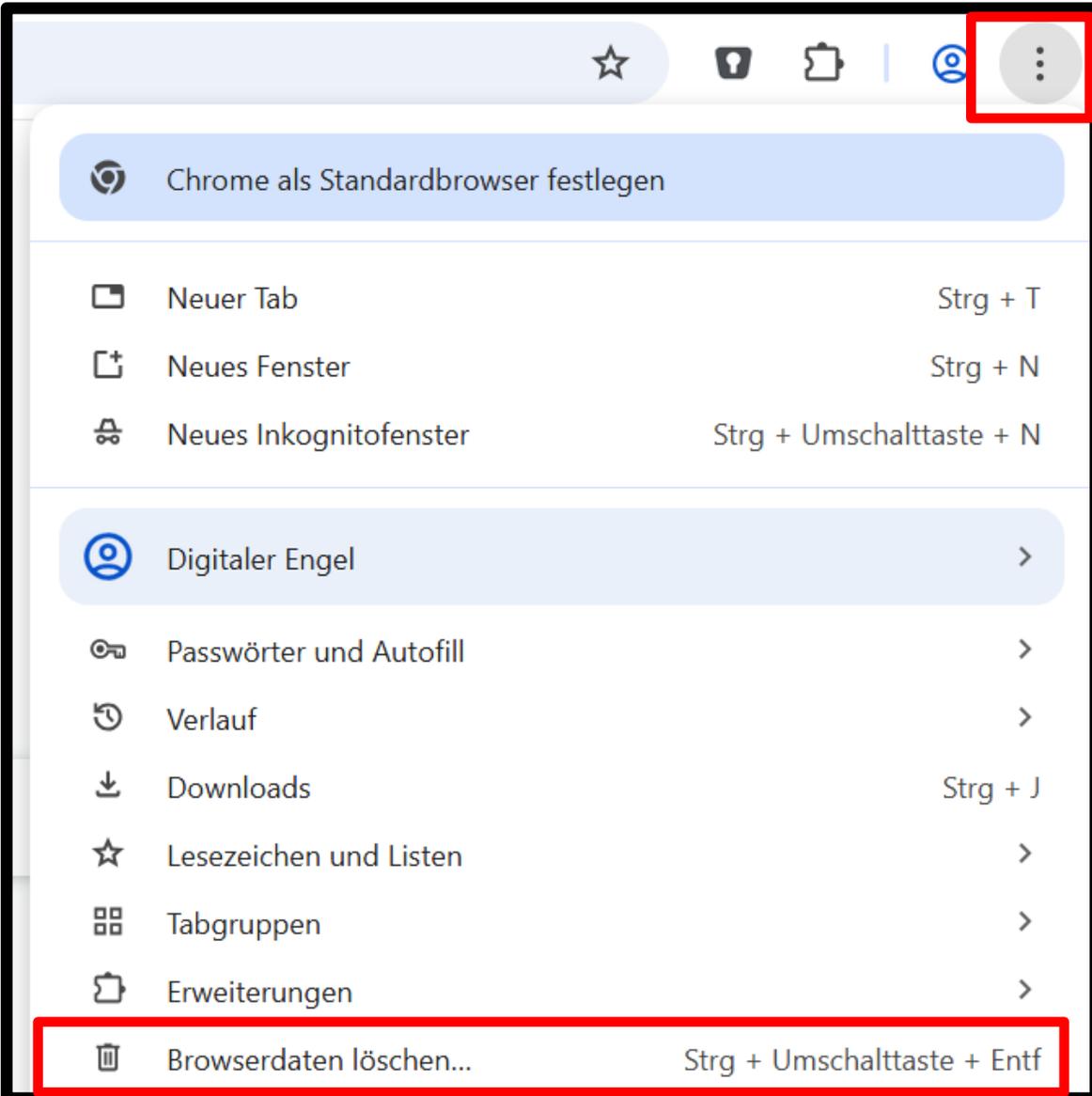
Individuelle Einstellungen

Cookie-Banner der Seite www.dsgvoschutzteam.com

2. Cookies

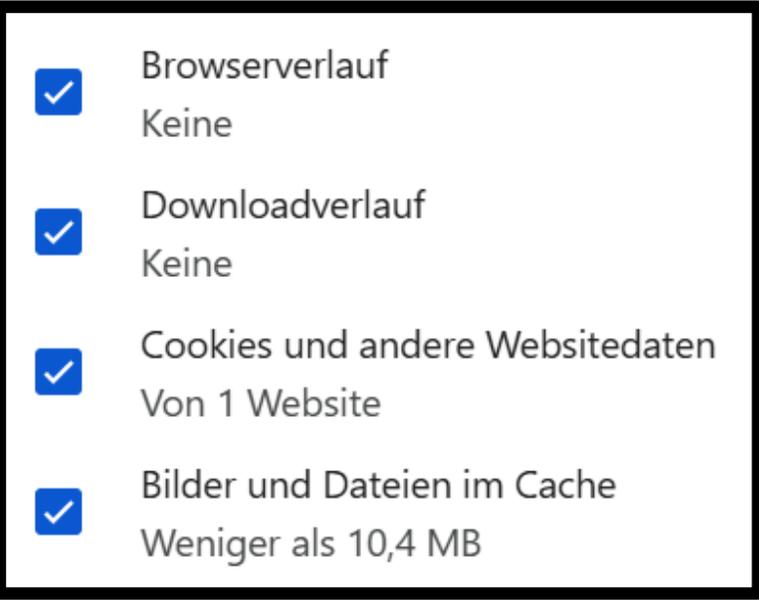
- Cookie-Banner = Vorschrift durch Europäischen Gerichtshof
- Nutzer:innen müssen **aktiv** der Verwendung von nicht notwendigen Cookies zustimmen

2. Cookies löschen am Beispiel Google Chrome



2. Cookies löschen am Beispiel Google Chrome

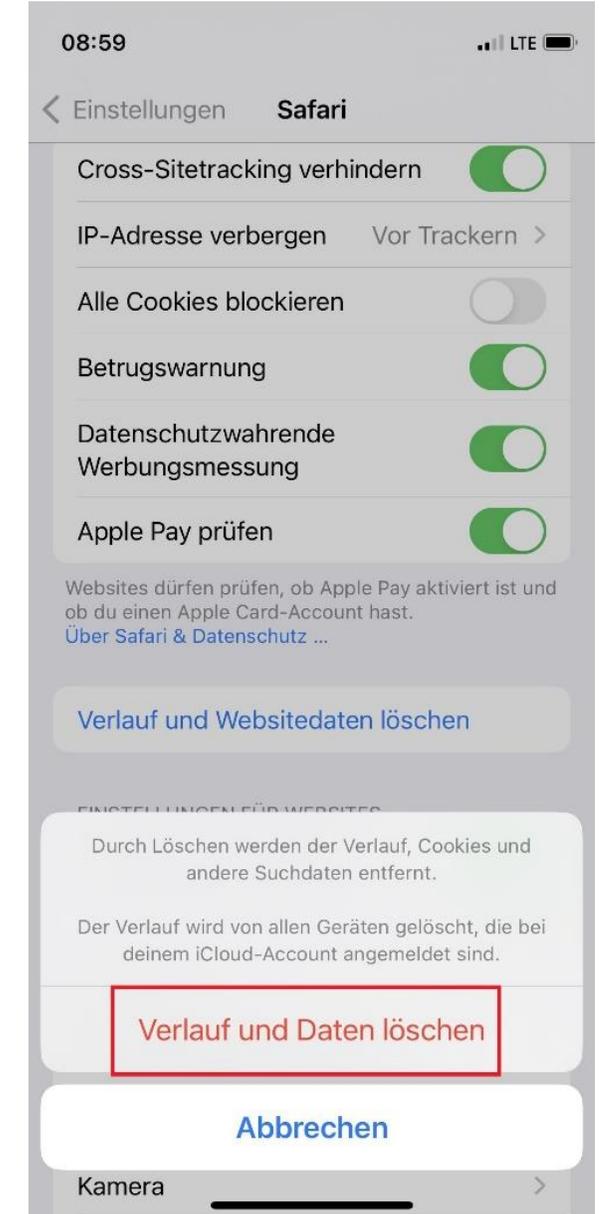
Cache

- 
- Browserverlauf
Keine
 - Downloadverlauf
Keine
 - Cookies und andere Websitedaten
Von 1 Website
 - Bilder und Dateien im Cache
Weniger als 10,4 MB

Eigener Screenshot aus Google Chrome

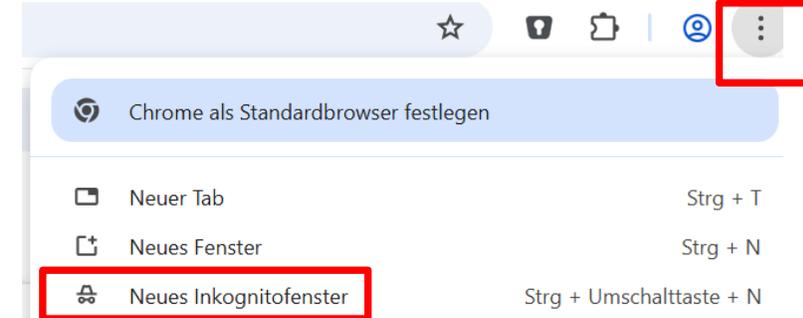
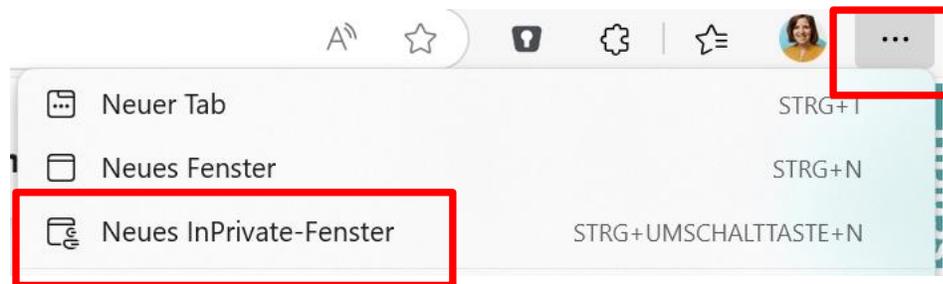
- Zwischenspeicher oder Puffer für Daten beim Surfen im Internet
- besuchte Seiten müssen so nicht erneut geladen werden müssen.
- Das Leeren vom Cache kann Speicherplatz freigeben und Probleme beim Laden von Webseiten beheben.

2. Cookies bei iOS löschen



2. Cookies: Weitere Tipps

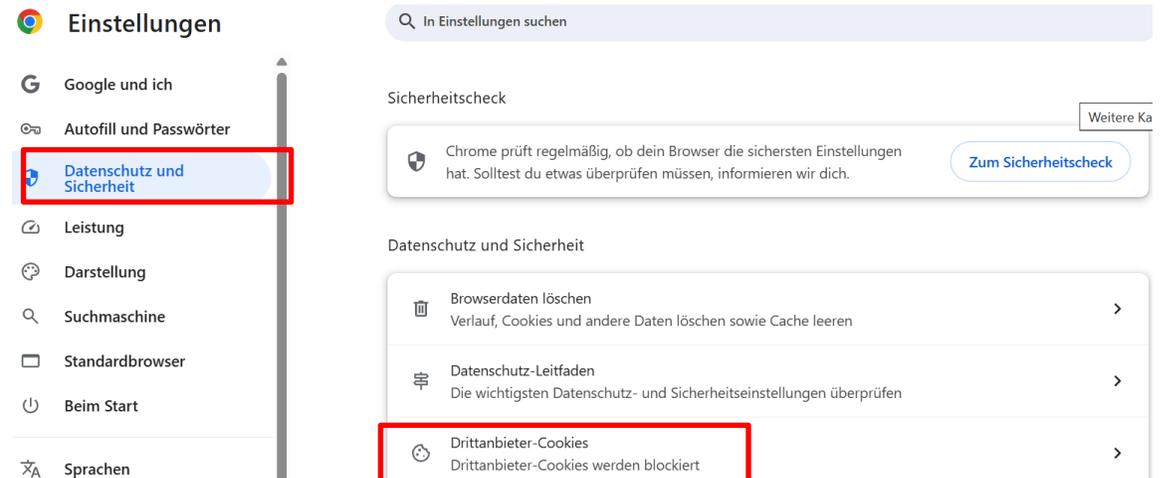
- Inkognito oder anonymen Modus nutzen



- Anti-Tracking-Software nutzen

- Drittanbieter-Cookies blockieren

Eigene Screenshots Google Chrome und Microsoft Edge



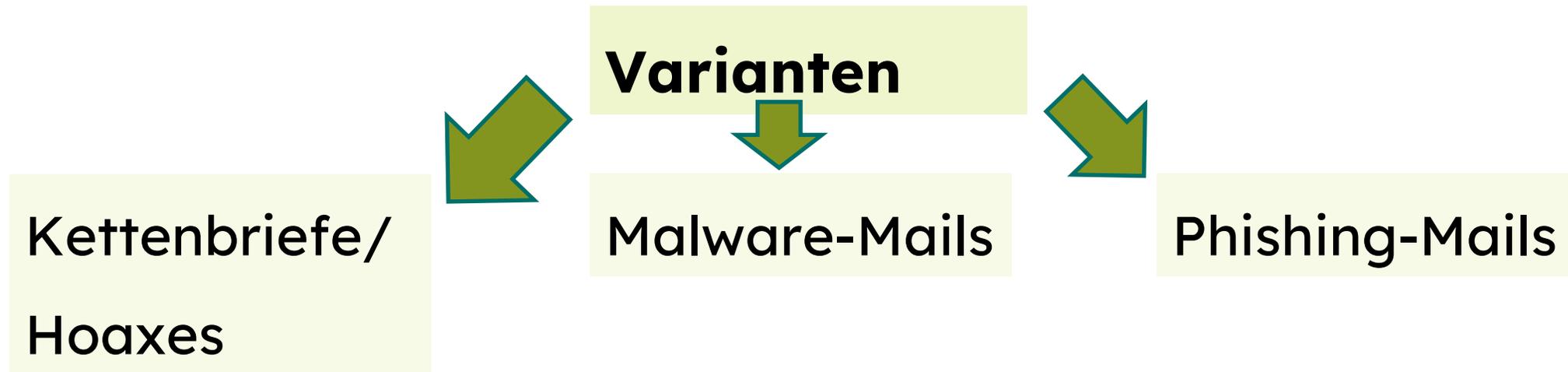
3. Umgang mit Phishing

3. Spam

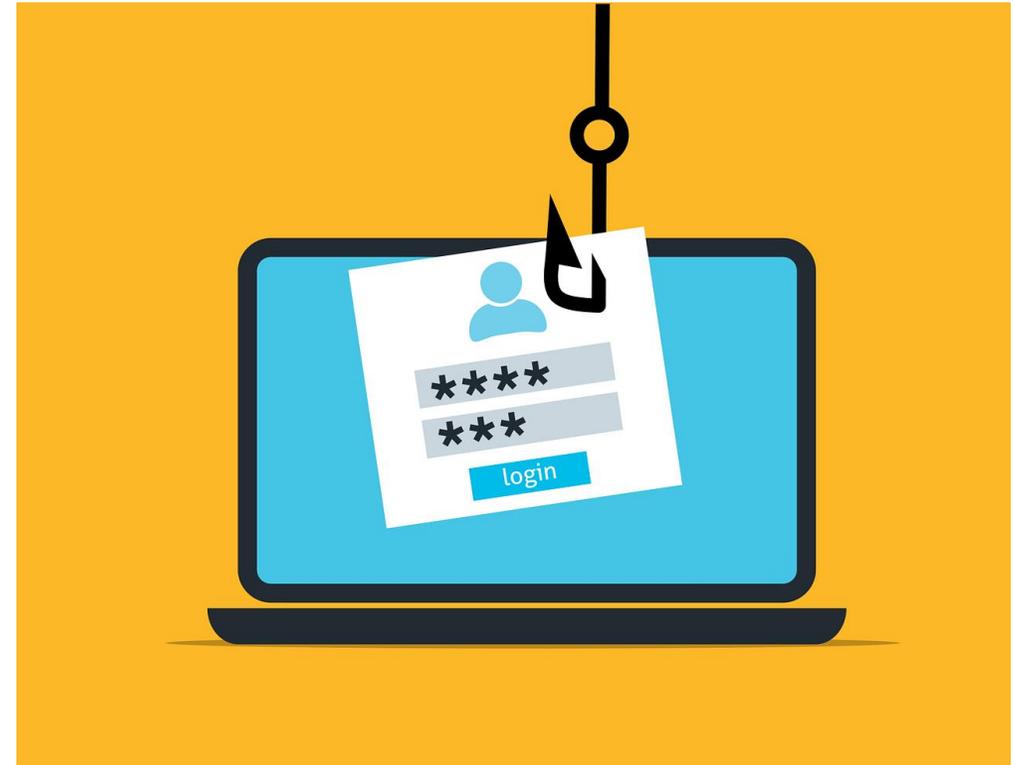
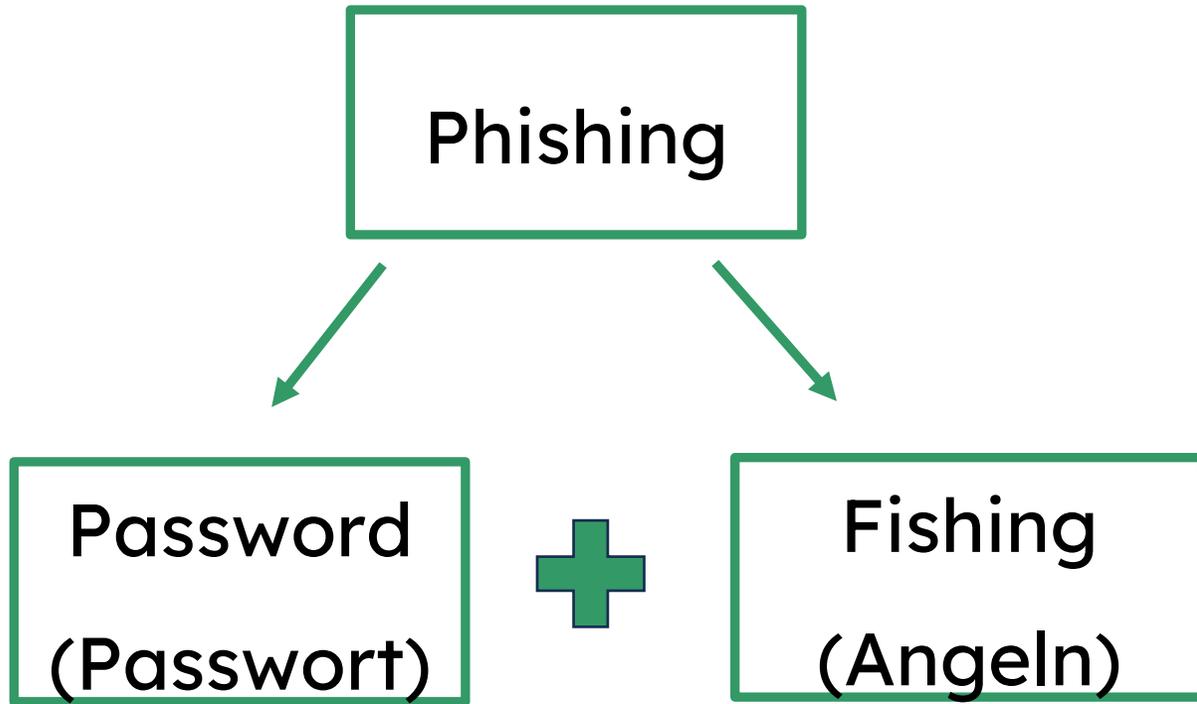
- Spam/Junk-Mail = unerwünschte Werbung, die ungewollt in das E-Mail-Postfach zugestellt wird
- 60-90% aller Mails bestehen aus Spam-Mails



Bildquelle:
www.askleo.askleomedia.com



3. Phishing



Bildquelle: www.pixabay.com

3. Gefahr von Social Engineering

Social Engineering = Soziale Manipulation



Beispiele:

- Ein netter Anruf einer Ihnen nicht bekannten Bankmitarbeiterin, mit der Bitte, ihr Ihre Zugangsdaten zu geben
- Enkeltrick
- E-Mail mit dubiosem Anhang

➤ **Bekannte Online-Form = Phishing**

3. Phishing erkennen

Die vorliegenden
Beispiele stammen aus
dem Google Phishingtest



Google Phishingtest Entwickelt von JIGSAW



Erkennen Sie Phishing?

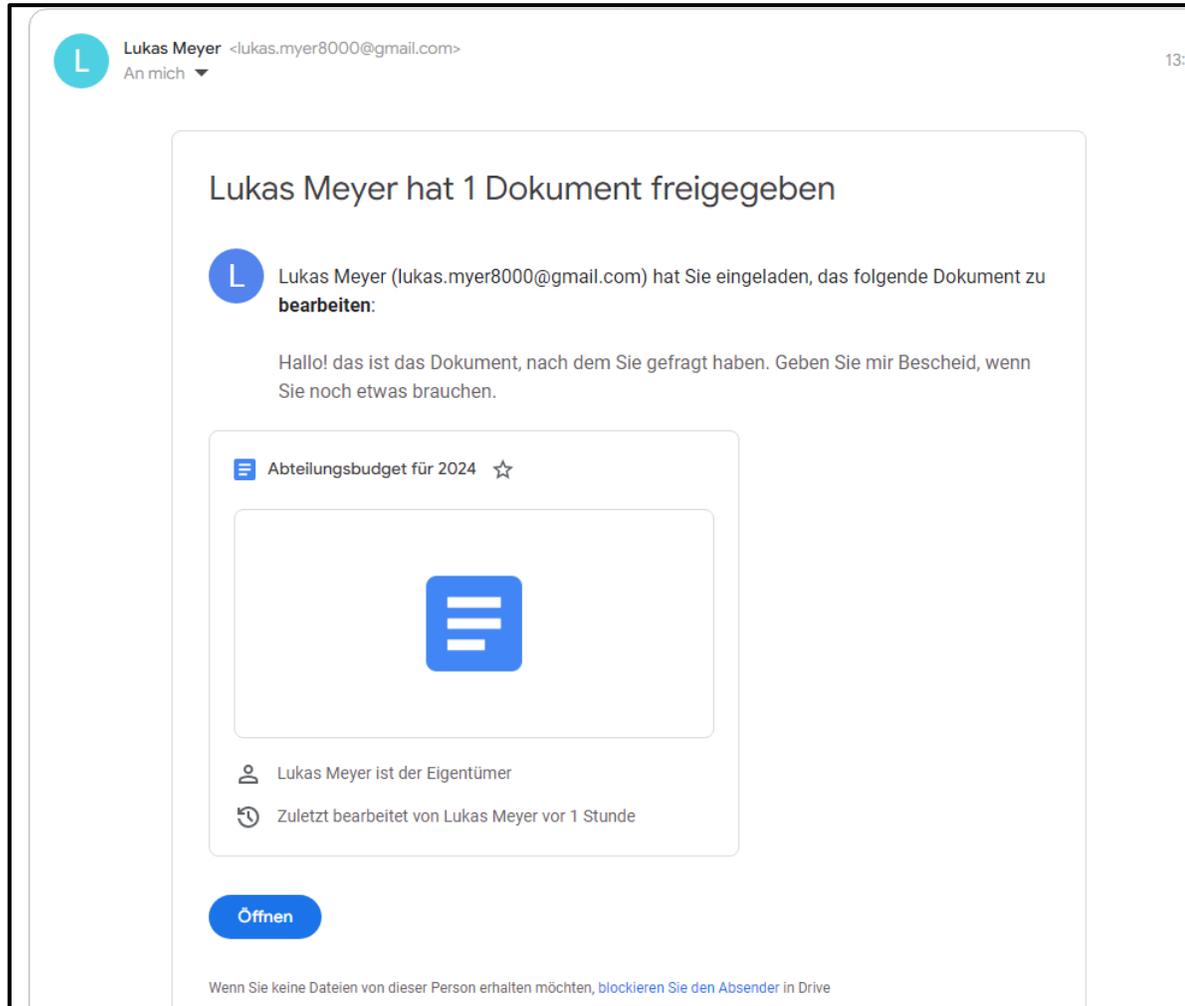
Bei Phishing-Angriffen werden ahnungslose Nutzer dazu verleitet, personenbezogene oder finanzielle Informationen preiszugeben. Häufig werden dabei Inhalte bekannter, vertrauenswürdiger Unternehmen nachgeahmt.

Durch KI werden Phishing-Angriffe immer raffinierter, personalisierter und häufiger.

Sie glauben, Sie können erkennen, was echt und was gefälscht ist?

[Quiz starten](#)

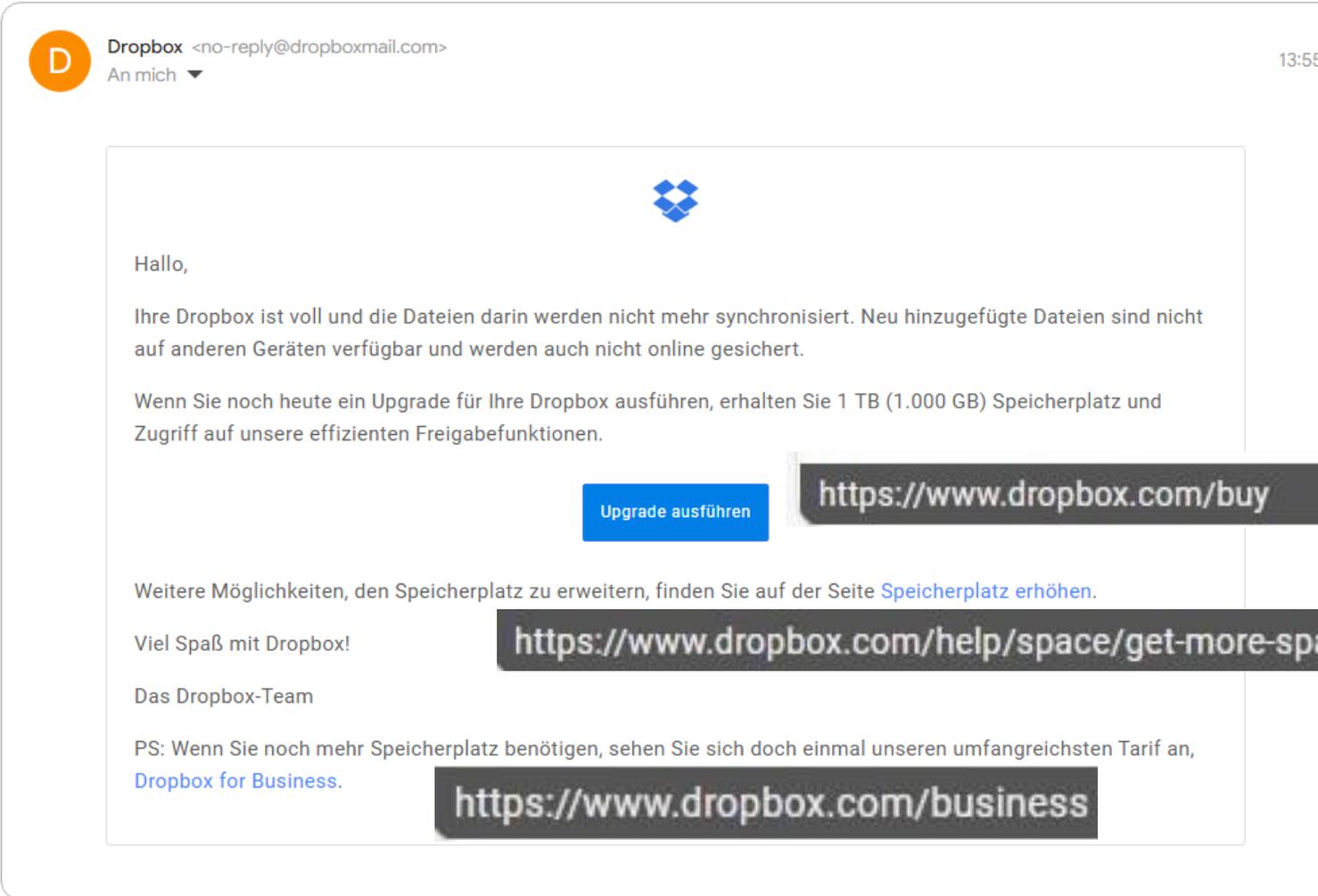
3. Phishing oder echt?



Phishing

Durch Bewegung des Mauszeigers auf Öffnen wird die unsichere URL angezeigt

3. Phishing oder echt?



Echt

- Ungewöhnliche, aber authentische Absenderadresse dropboxmail.com
- URL ist ein sicherer Link (https)

(WARNUNG) : Ihr PayPal-Konto wurde vorübergehend gesperrt [#CaseID : 65GVY79EV3VY5NY26SHY]

 **service@paypal.de** <ekfngyssnsermhgvlcciae3serihjnyserjkytr79ev3vy5ny5dw57o-245.254.15.76@kfnms.xycpnhjvbrvvoqkfhkyjrhrh.owilksnba.com>
An: petra @yahoo.de



Ihr PayPal-Konto wurde vorübergehend gesperrt

Sehr geehrter Kunde

Ihr PayPal Konto wurde vorübergehend gesperrt. Wir haben verdächtige Aktivitäten auf Kreditkarten gefunden, die mit Ihrem PayPal Konto verknüpft sind. Sie müssen Ihre Identität bestätigen, um zu bestätigen, dass Sie die Kreditkarte besitzen.

Um die Kontosicherheit aufrechtzuerhalten, geben Sie dokumente an, die Ihre Identität bestätigen.

[PayPal Kontoüberprüfung](#)

<https://linkedin.com/slink?code=gKi5MTD?id=serihjny>

Wer ist Absender?

Ist eine persönliche Anrede vorhanden?

Gibt es sprachliche Auffälligkeiten?

Enthält die E-Mail eine Dringlichkeit?

Wohin führt der Link?

3. Tipp zur Erkennung von Phishing

Inhaltsverzeichnis

29. November 2024: Kundschaft der Deutschen Bank mit vorübergehender photoTAN-Sperrung konfrontiert

28. November 2024: Sparkasse droht mit Kontoeinschränkungen

27. November 2024: DKB-Kundschaft zur Datenaktualisierung innerhalb von 48 Stunden aufgefordert

26. November 2024: Zahlungsaufruf zu unbezahlten Zollgebühren im Namen von DHL

25. November 2024: Aufforderung zur Kontoaktualisierung bei Disney+-Kundschaft

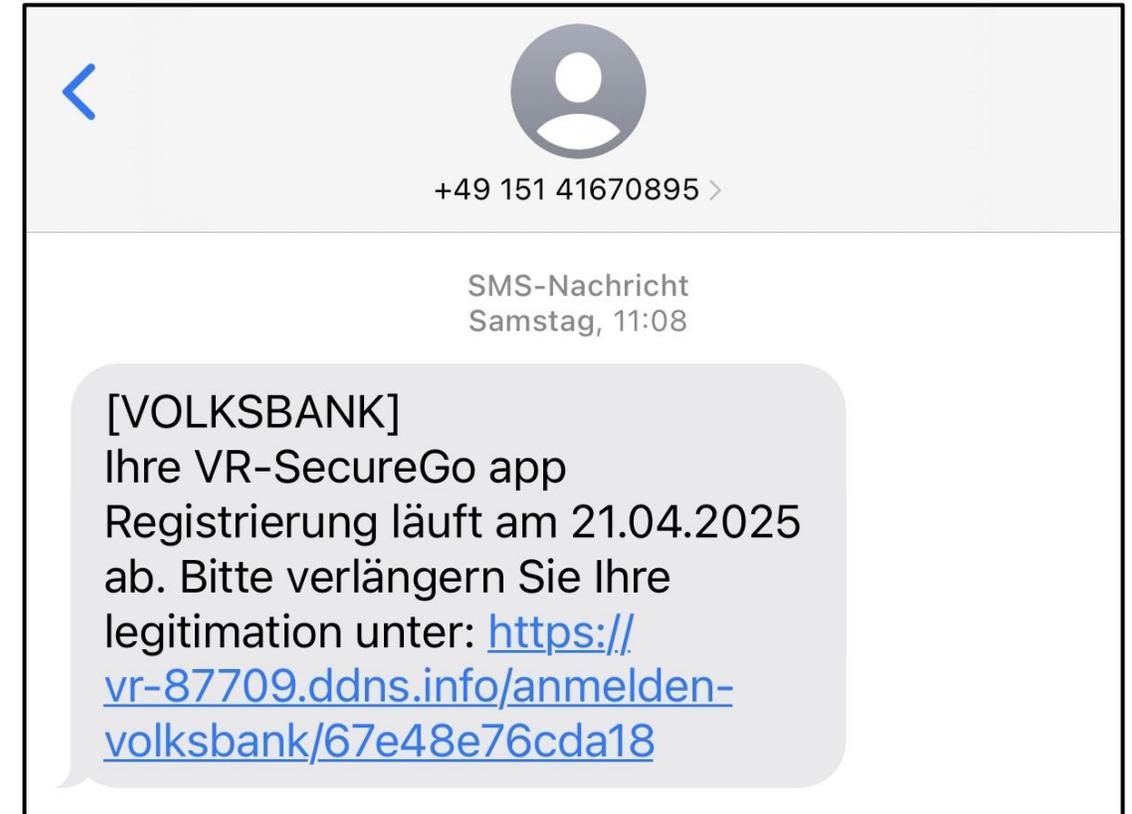
22. November 2024: Angeblicher Kontozugriff aus den Niederlanden bei Amazon-Kundschaft

Ältere Beiträge

Bildquelle und Link zum
Phishing-Radar der
Verbraucherzentrale NRW



3. Smishing Beispiele



Bildquelle: Eigene Screenshots

3. Quishing



- Betrügerische Codes per Briefpost, an Ladesäulen für E-Autos, Parkscheinautomaten, auf gefälschten Strafzetteln sowie in Bussen und Bahnen.
- QR-Code nur scannen, wenn Sie sich über dessen Echtheit sicher sind und vorher prüfen können, wo er hinführt

3. Quishing



COMMERZBANK 
Die Bank an Ihrer Seite

1885 - POSTFACH 1464 - 39004 Magdeburg
P 31 42C4 1B0F 61 E001 1F81
DV 08.24 0,85 Deutsche Post  *K4 000*

Aktualisierung Ihres photoTAN-Verfahrens zur Sicherheit Ihrer Bankgeschäfte 21. August 2024

Sehr geehrte Kontoinhaberin, sehr geehrter Kontoinhaber,

mit diesem Schreiben möchten wir Sie über eine wesentliche Sicherheitsmaßnahme informieren, die Ihre finanziellen Transaktionen betrifft. Aufgrund bedauerlicher Vorfälle von Betrug in Verbindung mit dem photoTAN-Verfahren sehen wir uns gezwungen, ab sofort eine regelmäßige Erneuerung dieses Sicherheitsverfahrens einzuführen.

Die Sicherheit Ihrer Bankgeschäfte hat für uns oberste Priorität. Daher ist es unerlässlich, dass Sie Ihr photoTAN-Verfahren in regelmäßigen Abständen aktualisieren. Diese Maßnahme stellt sicher, dass nur Sie persönlich und autorisiert Überweisungen und andere Bankgeschäfte durchführen können. Wir bitten Sie daher, Ihr photoTAN-Verfahren umgehend zu aktualisieren. Scannen Sie dazu einfach den beigefügten QR-Code, der Sie direkt zur Reaktivierung führt.

319671
005424
1 1
00000000
GT

Bitte beachten Sie, dass diese Aktualisierung für alle Kunden verpflichtend ist, um die Integrität Ihres Kontos und die Sicherheit Ihrer Finanztransaktionen zu gewährleisten. Für den Prozess wird der separat versandte Aktivierungsbrief benötigt, der zur Aktivierung des photoTAN-Verfahrens verwendet wurde.

Vielen Dank für Ihr Verständnis und Ihre sofortige Kooperation in dieser Angelegenheit.

Mit freundlichen Grüßen,
Commerzbank


Arno Walter

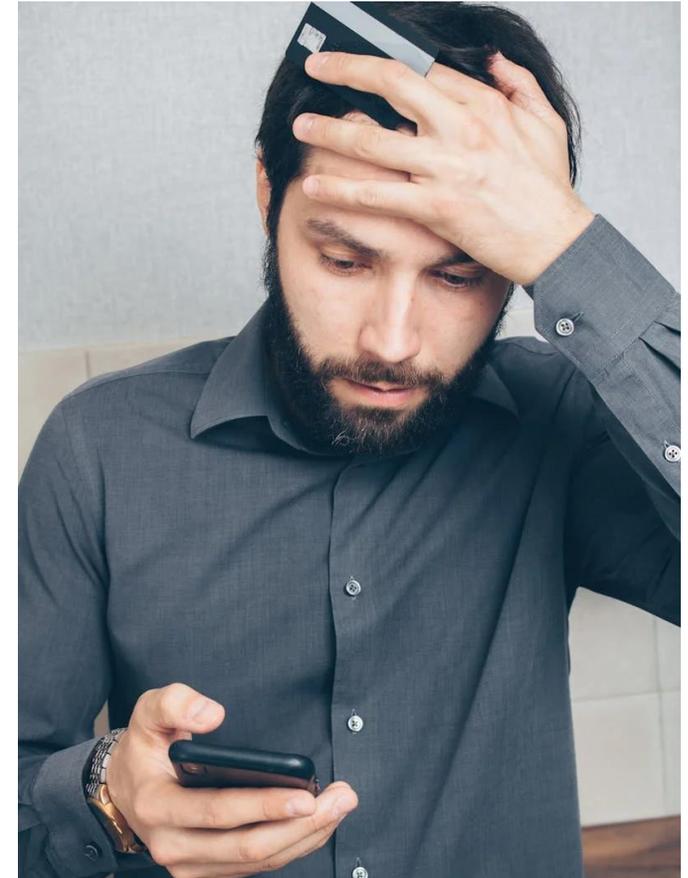

Aydin Sahin

Vorsitzender des Aufsichtsrats: N.N.
Vorstand: Manfred Kriof (Vorsitzender),
Marcus Chronik, Jörg Hessemmüller,
Michael Kolzbauer, Bettina Orloff, Sabine Schmittroch

Commerzbank Aktiengesellschaft, Frankfurt am Main
Handelsregister: Amtsgericht Frankfurt am Main, HRB 52000
USt-IdNR: DE 114 103 514

3. Identitätsdiebstahl

- Betrüger:innen geben sich im Internet für andere Personen aus
- Nutzung von persönlichen Daten, die online gefunden wurden zum Beispiel zur Erstellung von Nutzerkonten oder Bestellen von Waren oder Dienstleistungen



Bildquelle: www.pexels.com

3. Identity Leak Checker des Hasso-Plattner-Instituts



Wurden Ihre persönlichen Identitätsdaten im Rahmen eines bekannten Hacks oder Datenleck entwendet?

Wurden Ihre Identitätsdaten ausspioniert?

Täglich werden persönliche Identitätsdaten durch kriminelle Cyberangriffe erbeutet. Ein Großteil der gestohlenen Angaben wird anschließend in Internet-Datenbanken veröffentlicht und dient als Grundlage für weitere illegale Handlungen.

Mit dem HPI Identity Leak Checker können Sie mithilfe Ihrer E-Mailadresse prüfen, ob Ihre persönlichen Identitätsdaten bereits im Internet veröffentlicht wurden. Per Datenabgleich wird kontrolliert, ob Ihre E-Mailadresse in Verbindung mit anderen persönlichen Daten (z.B. Telefonnummer, Geburtsdatum oder Adresse) im Internet offengelegt wurde und missbraucht werden könnte.

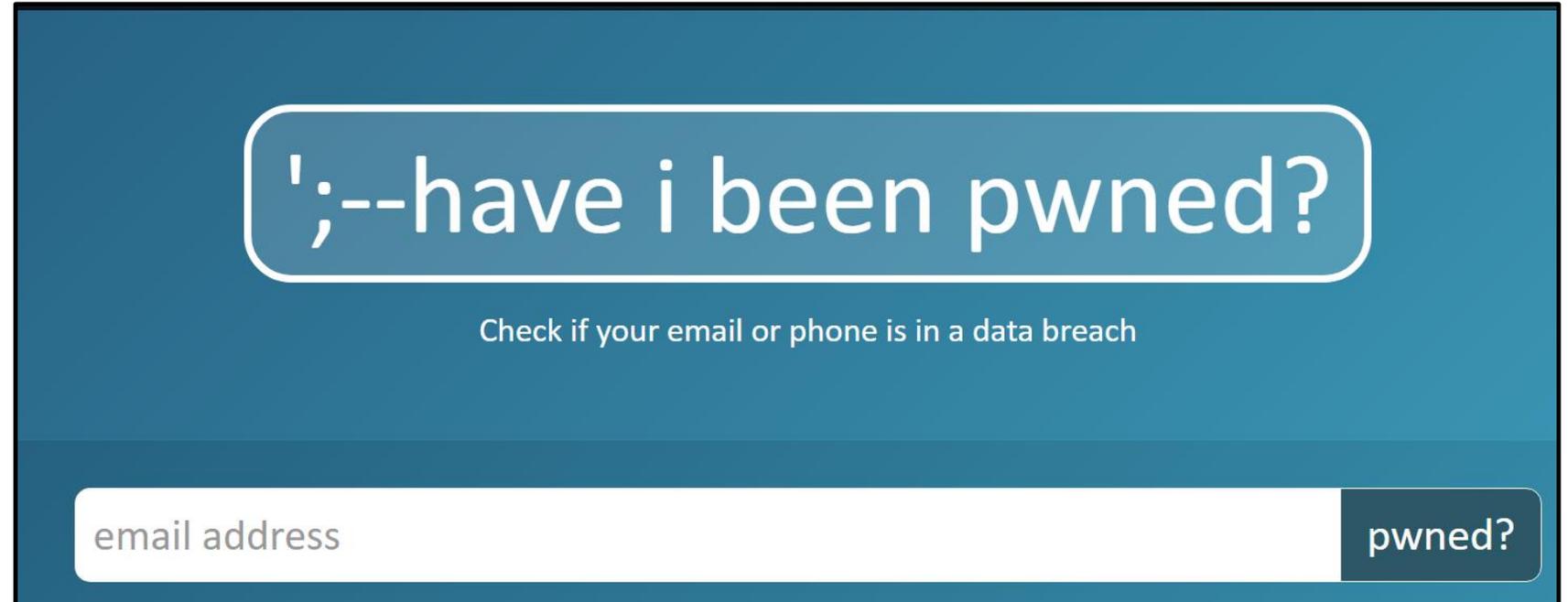
Die von Ihnen eingegebene E-Mail-Adresse wird lediglich zur Suche in unserer Datenbank und das anschließende Versenden einer Benachrichtigungs-E-Mail benutzt. Sie wird von uns in verschleierter Form gespeichert, um Sie vor E-Mail-Spam zu schützen. Die Weitergabe an Dritte ist dabei ausgeschlossen.

E-Mail-Adresse prüfen!

Quelle: <https://sec.hpi.de/ilc/search>

3. Have I Been Pwned (HIBP)

Wurden Ihre
persönlichen
Identitätsdaten im
Rahmen eines
bekannten Hacks
oder Datenleck
entwendet?



';--have i been pwned?

Check if your email or phone is in a data breach

email address

pwned?

3. Scam

- Betrug
- Mit dubiosen Versprechungen/ Gewinnen/ Geschichten versuchen Betrüger:innen ans Geld zu kommen

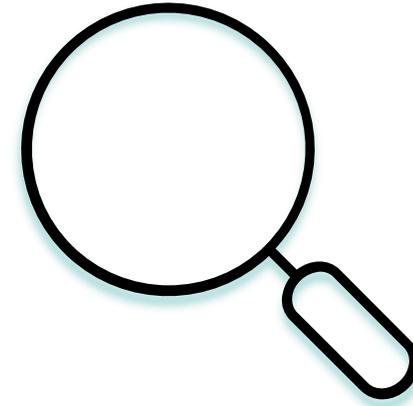
Arten

- Romance-Scam
- Wohnungs-Scam
- Job-Scam



Bildquelle: www.pixabay.com

3. Scam erkennen



- Kontaktaufnahme: Einladung zum Chat
- Sprache: meistens gutes Englisch
- Bilder: Frauen oft leicht bekleidet, Männer mit Fotos in Uniform
- Am Inhalt der Mails: Bitten um Geld / Visum / Päckchen- oder Briefversand / gemeinsames Konto
- Männer aus Westafrika/Russland/ Südostasien, Frauen aus osteuropäischen / südostasiatischen / südamerikanischen Ländern.

3. Scam-Betrug: Was tun?

- Ignorieren: Kein Geld überweisen
- Beweise sichern
- Hilfe holen: Anzeige erstatten
- Jeglichen Kontakt abbrechen

Weitere Informationen: www.polizei-beratung.de



Bildquelle: www.pixabay.com

3. Informationsblatt zu Scamming

SCAMMING – BETRUG MIT VORAUSZAHLUNGEN

Immer wieder erfinden Betrügerinnen und Betrüger (Scammer) Geschichten, um ahnungslose Menschen dazu zu bringen, ihnen Geld zu überweisen. Diese unter dem Namen Nigeria Connection bekannt gewordene Betrugsmasche tritt mittlerweile in vielfältiger Form auf.

Betrug mit falschen Geldversprechen

Zu einem der ältesten Tricks der Nigeria Connection gehören E-Mails (vormals Briefe oder Faxe), in denen Empfängerinnen und Empfängern eine Menge Geld versprochen wird, z. B. aus einer Erbschaft. Um an das Geld zu kommen, müssen die Angeschriebenen allerdings zunächst viele tausend Euro für Gebühren, Notarkosten oder Steuern zahlen. Hat das Opfer gezahlt, bricht die Gegenseite den Kontakt ab und das Geld ist unwiederbringlich verloren.

Betrug mit vorgetäuschter Liebe

Bei dieser Betrugsmasche suchen sich die Scammer ihre Opfer in Online-Partnerbörsen oder sozialen Netzwerken. Sie flirten und umgarnen ihre Opfer, bis diese sich in ihr virtuelles Gegenüber verlieben. Dann kommt die Frage nach dem Geld, z. B. für eine dringende Operation oder eine andere angebliche Notlage, für die die Opfer Geld überweisen sollen. Viele tun dies dann auch, da sie zu diesem Zeitpunkt schon von ihrer Internet-Bekanntheit emotional abhängig sind.

Betrug mit Wohnungsangeboten

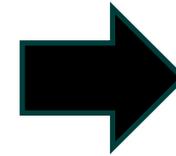
Eine tolle Wohnung zu einem Schnäppchenpreis. Der Haken: Der Eigentümer oder die Eigentümerin ist im Ausland, eine Besichtigung unmöglich. Deshalb wird angeboten, den Schlüssel gegen eine Vorauszahlung der ersten Miete und Kautions zu schicken. Sollte die Wohnung nicht gefallen, werde das Geld erstattet. Doch oft existiert die Wohnung gar nicht oder gehört einem Ahnungslosen. Das Geld ist weg.

Betrug mit gefälschten Schecks

Über Verkaufsanzeigen in Zeitungen oder im Internet nehmen die Betrügerinnen und Betrüger Kontakt zu Privatpersonen auf, die beispielsweise ein gebrauchtes Auto verkaufen. Sie bieten ihnen einen Scheck an, der auf einen höheren als den tatsächlichen Kaufpreis ausgestellt ist. Es wird vereinbart, dass das Opfer den Differenzbetrag beim Einreichen des Schecks bei der Bank per Bargeldtransfer an die Betrügerinnen und Betrüger überweist. Da selbst Bankangestellte einen gefälschten Scheck selten erkennen, stellt sich erst nach einigen Tagen heraus, dass der Scheck gefälscht war. Das bereits überwiesene Geld ist dann schon weg. Hinzu kommt, dass die Bank wegen Betrugs strafrechtliche Schritte gegen das Opfer einleiten kann.



Wenden Sie sich bei Problemen oder Fragen an die Polizei.



4. Weitere Tipps

Wie nutze ich das Internet sicher?

Dabei sein!
Online im Alter.



Sicheres Gerät

- Apps aus sicheren Quellen laden
- Betriebssystem und Apps aktualisieren
- Virenschutz installieren



Sichere Internetverbindung

- WLAN mit einem sicheren Passwort schützen
- WLAN ausschalten, wenn nicht in Benutzung
- Im öffentlichen Hotspot keine persönlichen Daten eingeben



Sichere Internetseiten

- Auf SSL Verschlüsselung achten
- Datenschutzerklärung und Impressum müssen vorhanden sein

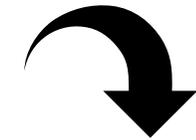


Schaubild:
Digitaler Engel



Drei Tipps für noch mehr Sicherheit

1. Verwenden Sie sichere Passwörter
2. Gehen Sie sparsam mit persönlichen Daten im Internet um
3. Aktivieren Sie die Drittanbietersperre bei Ihrem Mobilfunkanbieter

Ein Projekt von:

Gefördert von:

4. Sicheres Gerät

4. Apps aus sicheren Quellen laden



Google Play Store
(Android)



App Store
(iPhone)



AppGallery
(Huawei)

Die Apps werden dort auf Sicherheit geprüft.

4. Updates

- Begriff kommt aus dem Englischen
- Bedeutet auf Deutsch: **Aktualisierung**
- „up to date“ sein = auf den neusten Stand sein

4. Beispielfrage aus dem DiFü

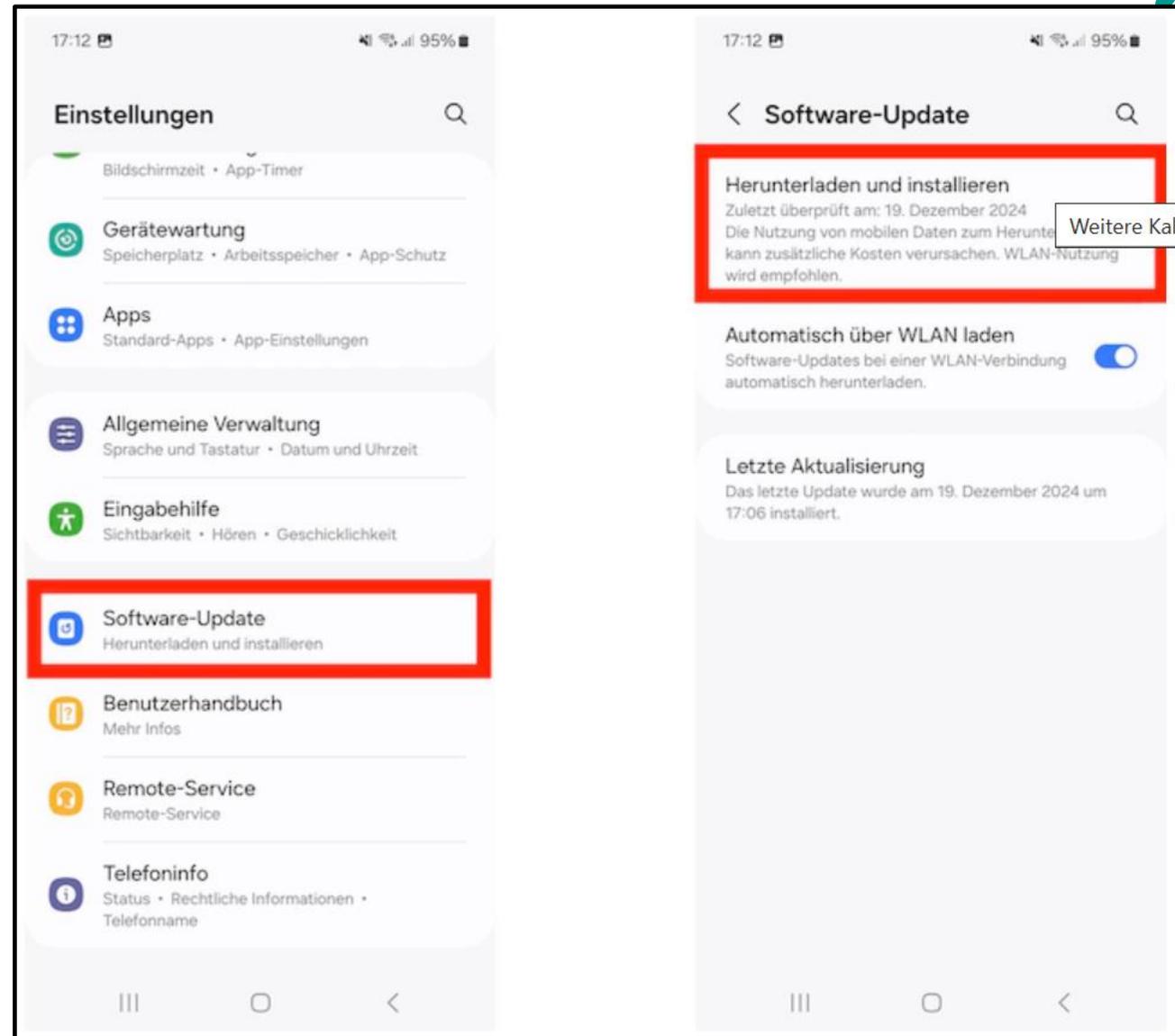


Warum sind Updates wichtig?

- A** Sie reinigen den Rechner von gefährlichen Dateien aus dem Internet.
- B** Sie schließen Sicherheitslücken und schützen damit persönliche Daten.
- C** Sie sorgen für eine stabile und schnellere Internetverbindung.

4. Updates

Aktualisierung des
Betriebssystems
(„Software“)



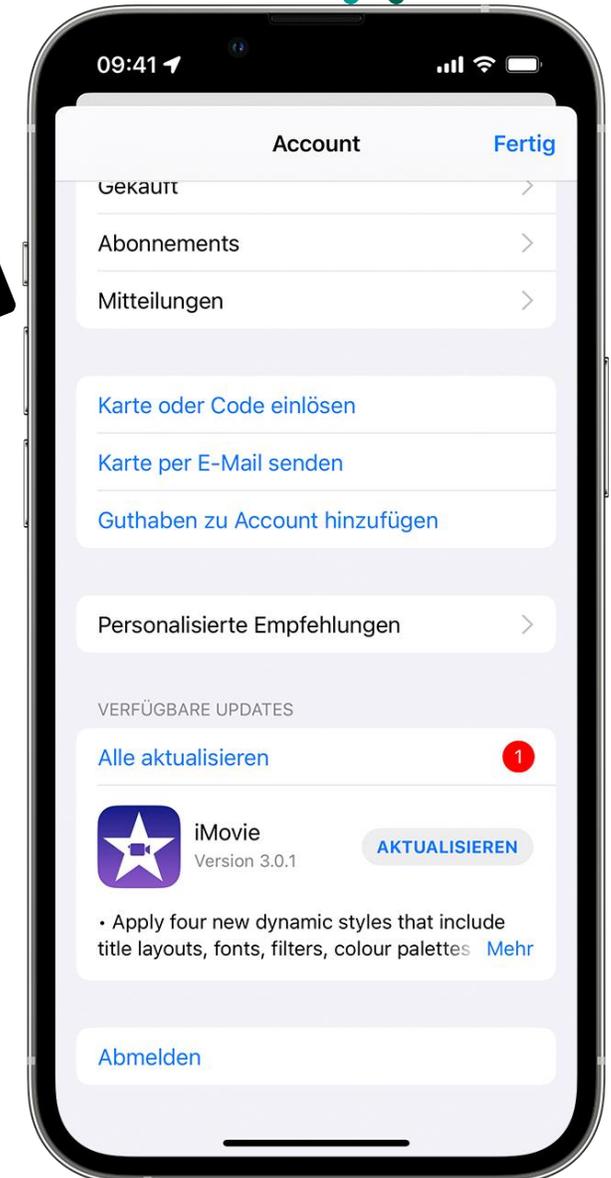
4. Updates

Aktualisierung von Apps

Im Google Play Store

1. Auf Ihr Profilkürzel tippen
2. „Meine Apps und Spiele“ auswählen
3. Alle aktualisieren oder Details ansehen

Im App Store



4. Virenschutz

- Android-Geräte: eingebauter Virens Scanner („Google Play Protect“) im Play Store
- Windows-Geräte: vorinstallierter Virens Scanner („Windows Defender“)
- Betriebssysteme von Apple-Geräten grundsätzlich sehr gut vor Viren geschützt

4. Smartphone sicher sperren

Muster



PIN



Passwort



Fingerabdruck



Iris-Scan



Gesichtserkennung



4. Smartphonesperre einrichten

Bei Android



1. Einstellungen
2. Sperrbildschirm
3. Sperrbildschirmtyp

Bei iOS



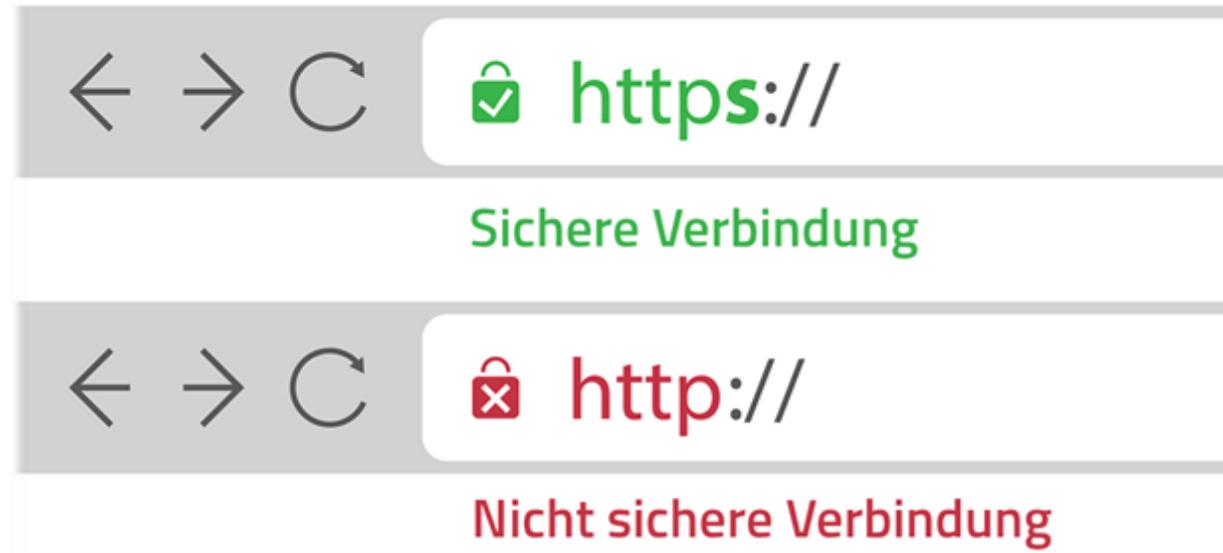
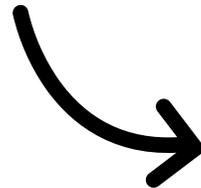
1. Einstellungen
2. Face ID & Code oder
Touch ID & Code

4. Sichere Internetseiten

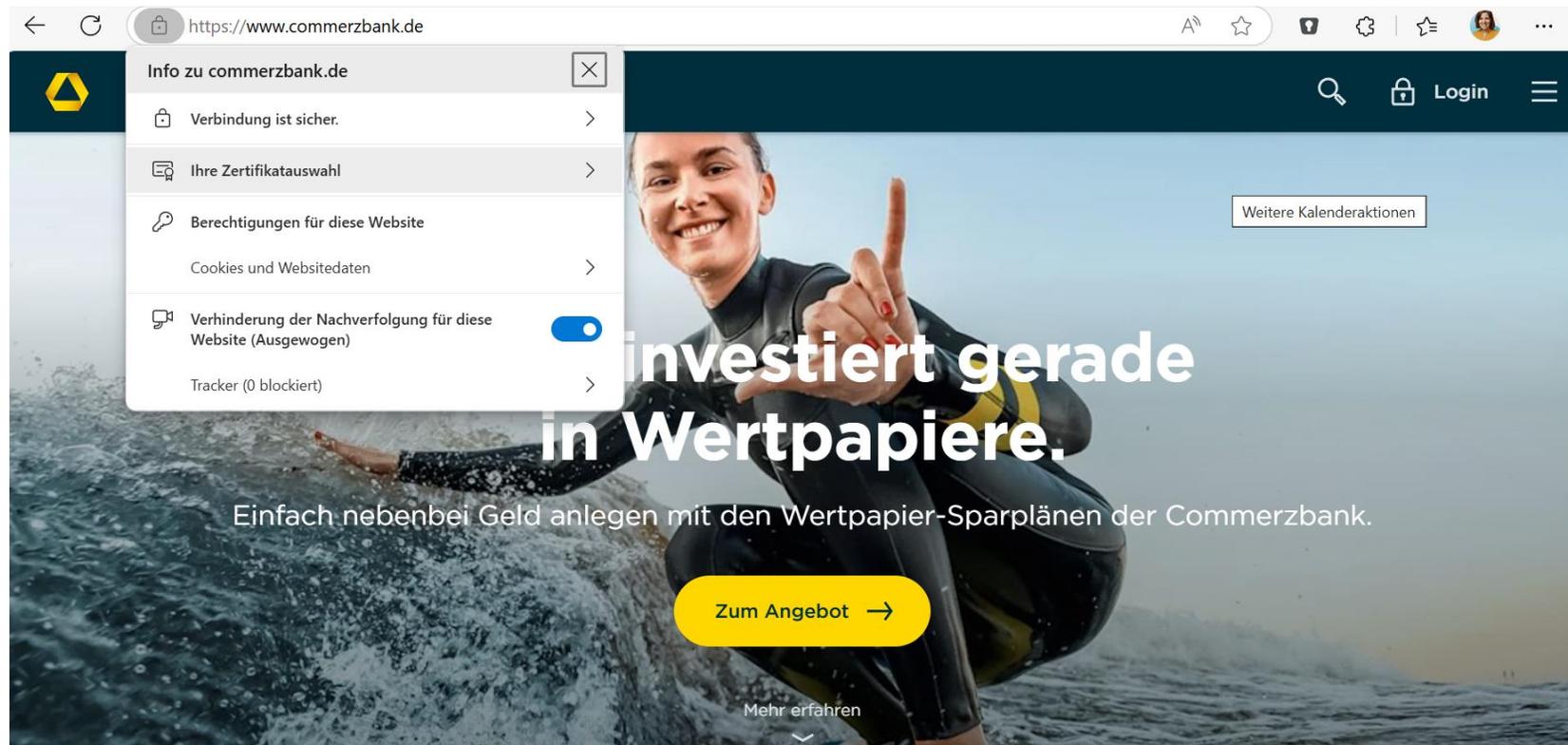
4. Sichere Internetseiten

1. Impressum und Datenschutzerklärung müssen vorhanden sein

2. auf SSL-Verschlüsselung achten



4. Sichere Internetseiten erkennen



Eigene Screenshots von
www.commerzbank.de



4. Fake-Shops erkennen

Was sind mögliche Anzeichen für Fake Shops, für Online-Shops, hinter denen möglicherweise Betrüger stecken? (Mehrere Antworten möglich)

- A** Es gibt kein Impressum und keine Datenschutzerklärung auf der Webseite.
- B** Es gibt keine Gütesiegel auf der Webseite.
- C** Der Sitz des Online-Shops ist nicht Deutschland.
- D** Der Online-Shop behauptet, er biete die Zahlung auf Rechnung oder Nachnahme an, im Bezahlvorgang kann man aber nur Kreditkartenzahlung oder Vorab-Überweisung auswählen.



Was sind mögliche Anzeichen für Fake Shops, für Online-Shops, hinter denen möglicherweise Betrüger stecken? (Mehrere Antworten möglich)

A Es gibt kein Impressum und keine Datenschutzerklärung auf der Webseite.



B Es gibt keine Gütesiegel auf der Webseite.



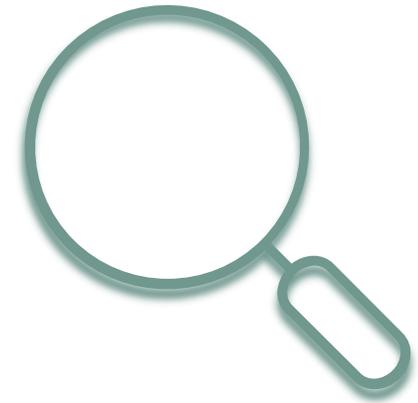
C Der Sitz des Online-Shops ist nicht Deutschland.

D Der Online-Shop behauptet, er biete die Zahlung auf Rechnung oder Nachnahme an, im Bezahlvorgang kann man aber nur Kreditkartenzahlung oder Vorab-Überweisung auswählen.



4. Weitere Merkmale von Fakeshops

- Mindestens eine kostenlose Bezahlungsmöglichkeit?
- **Sprachliche Mängel?**
- Ungewöhnlich viel **Werbung?**



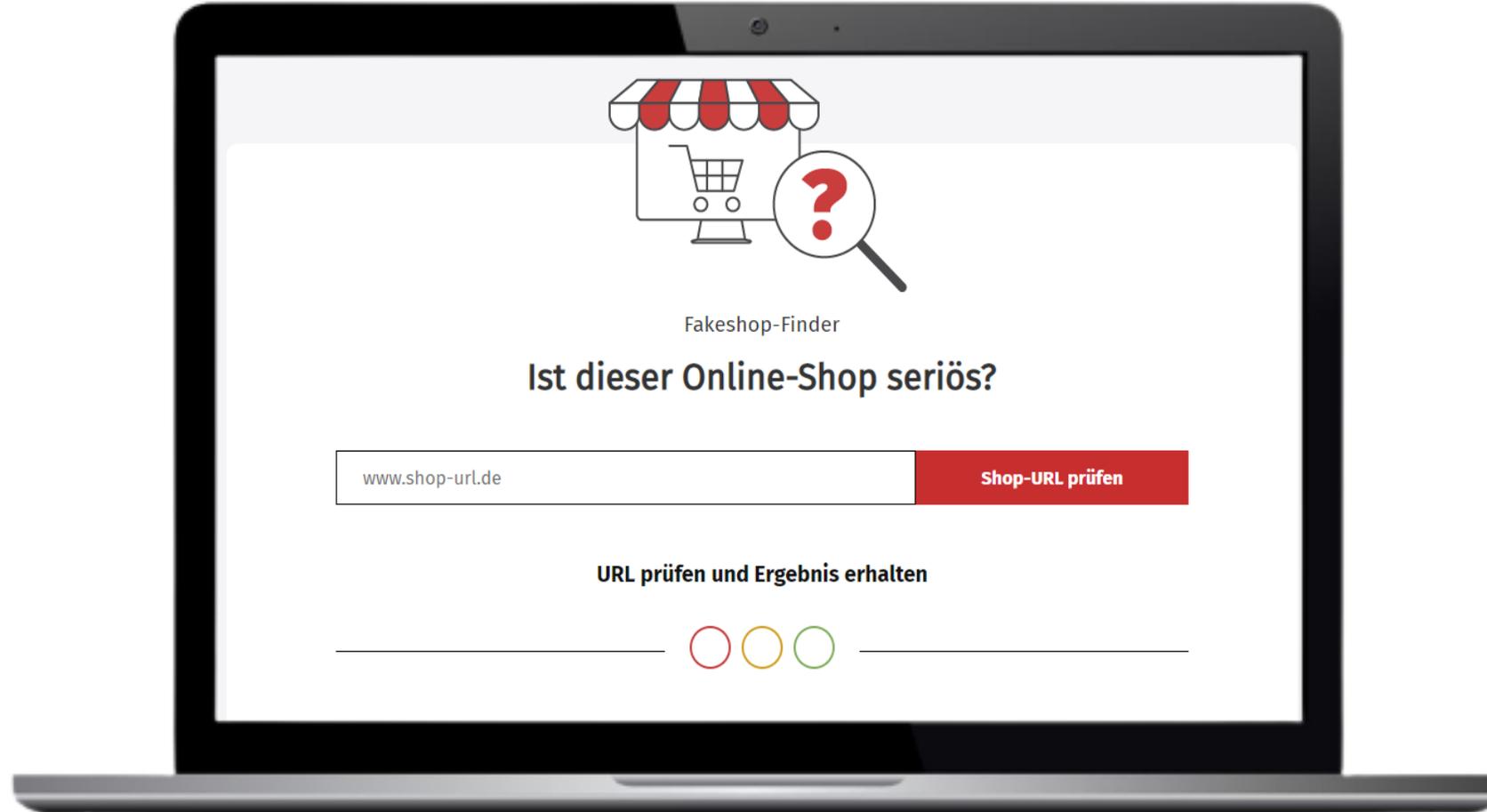
4. Gütesiegel

Gütesiegel geben (mehr) Sicherheit:



Wichtig: Logos müssen mit den Siegel-Anbieter verlinkt sein!

4. Fakeshops erkennen: „Fakeshop-Finder“



www.verbraucherzentrale.de/fakeshopfinder



5. Weiterführende Angebote

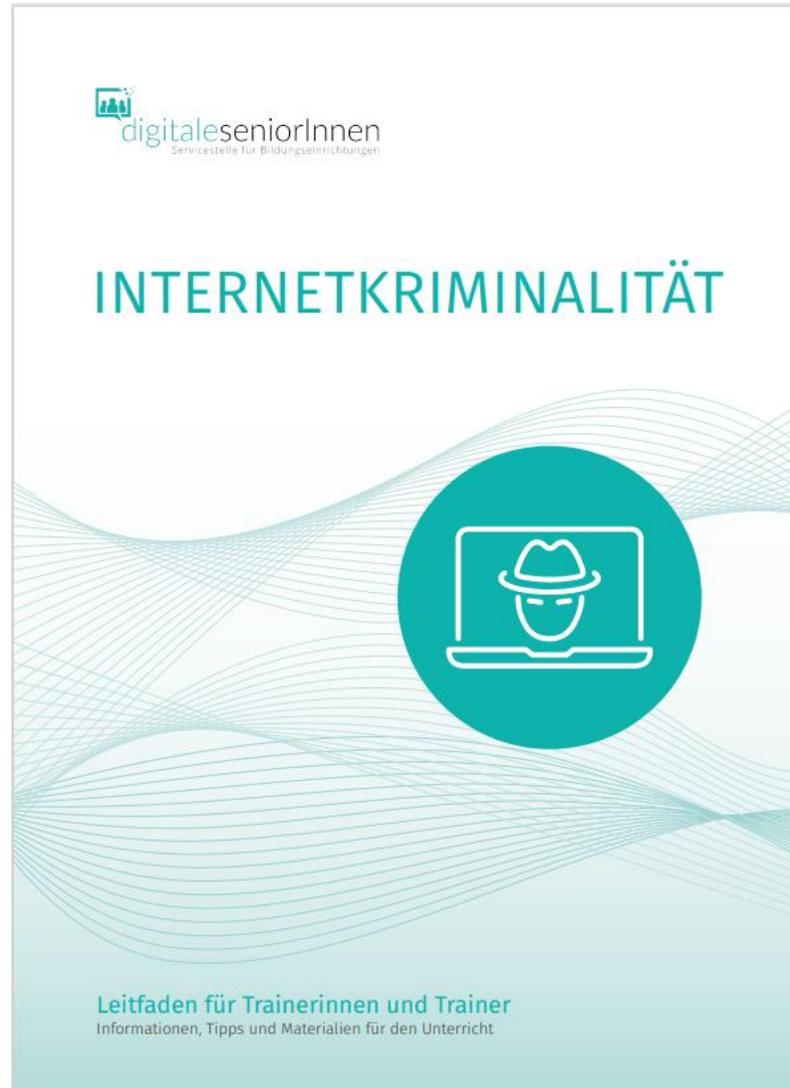
5. Wissen üben und erweitern



5. Weiterführende Informationen



5. Weiterführende Informationen



Österreichisches Institut für angewandte
Telekommunikation (ÖIAT) 2020



Hilfreiche Materialien



- kurzweilige Erklärvideos
- Antworten auf die häufigsten Digitalisierungsfragen älterer Menschen.
- Der Digitale Engel jederzeit und überall verfügbar!
- **Zu finden unter:**
 - www.digitaler-engel.org oder
 - YouTube: „Digitaler Engel“



Online-Schulungen für Wissensvermittelnde



ePA

 20.05.2025, 15:00-16:30 Uhr

Schulungsangebote zur KI

 22.05.2025, 10:00-11:30 Uhr

Online-Personalausweis

 26.05.2025, 10:00-11:30 Uhr

DiGAs und DiPAs

 27.05.2025, 10:00-11:30 Uhr

Austausch: Herausfordernde Situationen

 17.06.2025, 10:00-11:30 Uhr

Sicher bezahlen mit dem Smartphone

 19.06.2025, 15:00-16:30 Uhr

[Alle Lerneinheiten im Überblick](#)



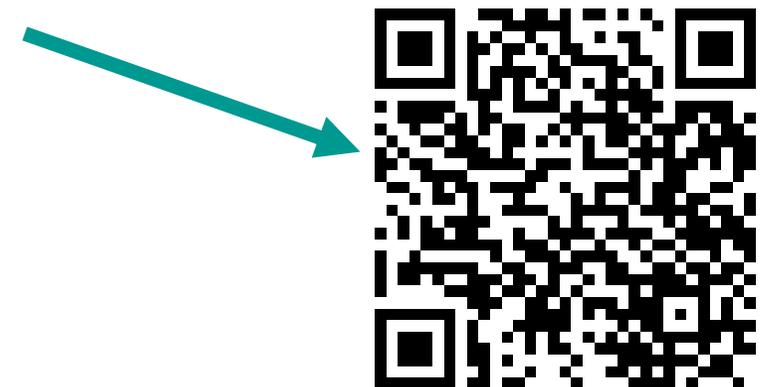
Kommende Online-Veranstaltungen



- 16.06.25, 10-12:00 Uhr: Wearables – Fitnessstracker, Smartwatches & Co.
- 18.06.25, 10-12:00 Uhr: Smartphone und Tablet Grundlagen
- 27.06.25, 10-11:30 Uhr: Arzttermine online buchen und Videosprechstunden

Alle Termine finden Sie unter

www.digitaler-engel.org/online-veranstaltungen



Vielen Dank für Ihre Aufmerksamkeit!
Mehr Informationen erhalten Sie unter



Digitaler_engel



Digitaler Engel



Digitaler Engel TV



Digitaler-engel.org



schulungen@digitaler-engel.org