



PC-Treff 55+

Sicherheit im Internet

6. OKTOBER 2026

DOROTHEA REICHBAUER

Wer sind wir vom PC-Treff 55+

(ehrenamtliche Mentoren)



Horst Höfer



Dorothea Reichbauer



Rainer Kaiser



Richard Weitz



Egbert Zwerschke



Heike Hauß
Leiterin MIT

Wir sprechen heute über den Schutz im Internet

- **Passwörter** - warum und wie, Passwort-Manager
- **System-Updates** warum und **Viren-Software** wo
- **Verlauf** - Liste der besuchten Seiten in der Suchmaschine
- **Cookies** - zustimmen, ablehnen und ggf. löschen
- **Geheimer Modus** - bei Arbeiten mit empfindlichen Daten

Wir sprechen heute Massnahmen zu unserem Schutz im Internet

- Geräte-Neustart – warum und wie oft
- Erkennen von fragwürdigen und sicheren Emails
- Sichere Verbindungen im eigenen oder fremden Netzwerk
- Sichere Internet-Seiten
- News-Letter-Schwemme abbestellen
- Sonstige Infos



Passwörter

- Passwörter sind wie der digitale Schlüssel zu unserem Briefkasten, Aktenschrank, Geldkassette oder Tresor.**

Erste Sicherheitsstufe

- Schützen Sie alle Ihre digitalen Geräte unbedingt mit einem Einstiegs Passwort, Entsperrmuster, Fingerabdruck oder Iris-Erkennung!!!!!!**



Pixabay

Passwörter

Zweite Sicherheitsstufe

- Den Zugang für jede Anwendung mit starkem komplexen Passwort gemäß der Passwort-Regel des Anbieters schützen
Beispiel: Mein Enkel Jonathan wurde am 22 Dezember 1985 geboren*! → MEJwa22D1985g*!
- Niemals 1234.... Das ist der erste Versuch eines Hacker!
- Für jede Anwendung ein anderes Passwort!
- Konsequenz: Passwörter aufschreiben und sicher verwahren

Passwörter



Pixabay

Achtung Passwort vergessen:

- Jede Anwendung braucht eine E-Mail-Adresse, wenn man das PW zurücksetzen muss, weil es vergessen wurde
- Folglich muss das E-Mail-Konto, das die Zurücksetzen-Mail erhält, besonders geheim sein.
- Sonst kann jemand für alle Ihre Anwendungen die Passwörter ändern.

Passwörter



Pixabay

Achtung Passwort ändern:

- Generell empfiehlt es sich turnusmäßig Passwörter zu ändern, damit es Hacker schwieriger haben.
 - Empfehlung alle 3 bis 6 Monate
 - Generell sollte reagiert werden wenn Datenklau bei einer Institution stattfand, bei der ein Zugang / Nutzerkonto besteht!
- Beispiel vom 15.07.2026 „Kriminelle erbeuten Daten von tausenden Stromkunden von Netze-BW“**



Dritte Sicherheitsstufe z.B. bei Zahlungen oder Banking

1. Einloggen in das Konto z. B. Bankkonto

Wichtig: Bei Aktivitäten mit Geld-Abfluss oder besonders sensiblen Daten.



Pixabay

Passwort Manager - einfach

Achtung: Ohne vorgeschaltetes Master-Passwort

- Browser / Suchmaschinen bieten die Möglichkeit Passwörter zu speichern, damit schneller und einfacher auf die Anwendung zugegriffen werden kann.
- ist das Gerät nicht geschützt, bzw. jemand kennt das Geräte-Passwort kann der Unbefugte auf alle Anwendungen zugreifen, die von einem gespeicherten Passwort bedient werden



Pixabay

Passwort Manager - komplex

- Passwort Manager helfen die vielen Passwörter zu verwalten. Sie erstellen komplexe und starke Passwörter. Übergeordnet gibt es ein einziges Master-Passwort, **welches niemals vergessen werden darf!**
- Risiko: Generalschlüssel-Effekt, wird Ihr Master-Passwort bei Ihnen oder dem Anbieter geknackt, hat der Hacker Zugriff auf alle Passwörter.
- Produkte: Passkey, Norton, 1Password und weitere



Pixabay

System-Updates und Viren-Software

- System-Updates und Viren-Software schließen Sicherheits-Lücken, die bei der Entwicklung des Systems oder APP nicht vorhersehbar waren. Darum eine Viren-Software installieren und laufend alle Updates einspielen.
- Achtung: Manche Telekommunikations-Anbieter haben schon eine Viren-Software vorgeschaltet. ABER wenn Sie außer Haus auf andere Netzwerke oder Anbieter zugreifen, sind sie schutzlos ohne Virensoftware auf dem Gerät. Viren-Software-Anbieter erlauben mehrere Geräte pro Lizenz!

Virenschutzprogramme



Pixabay

Quelle: DPA

1. [Bitdefender Total Security](#)



7. [AVG Anti-Virus Free](#)



2. [Avira Prime](#)



8. [Trend Micro Maximum Security](#)



3. [Kaspersky Premium](#)



9. [McAfee Total Protection](#)



4. [AVG Internet Security](#)



10. [Norton 360 Advanced](#)



5. [F-Secure Total](#)



11. [ESET Smart Security Premium](#)



6. [Avast Free Antivirus](#)



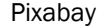
12. [Microsoft Windows Defender](#)



Internet Security-Suiten im Vergleich September 2023

Quelle: Bundespolizei

Aufruf unterschiedlich je Maschine



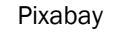
- Aufruf über...**
- Rechts oben im**
- Bild**





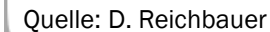
Cookies

- Cookies sind kleine Textdateien, die eine Internet-Seite auf ihrem Gerät speichert, um Funktionen zu erleichtern und Informationen zu ihrem Nutzer-Verhalten zu erlangen
 - Lehnen sie wenn möglich immer ab!
- Maximal genehmigen Sie die funktionalen Cookies**
- Cookies können in den Browser Einstellungen gelöscht werden.



- Cookies Löschen je Browser ist unterschiedlich

- Ohne
- ☒ Cookies und andere Websitedaten
- Von 24 Sites
- ☒ Zwischengespeicherte Bilder und Dateien
- Weniger als 200





Pixabay

Geheimer Modus im Browser

- InPrivate-Fenster, Incognitomodus, Privates Surfen, etc.
Name unterschiedlich je Suchmaschine
- Vorteil Daten werden nicht in den Verlauf geschrieben und temporäre Cookies werden sofort beim Verlassen gelöscht



Quelle: D. Reichbauer

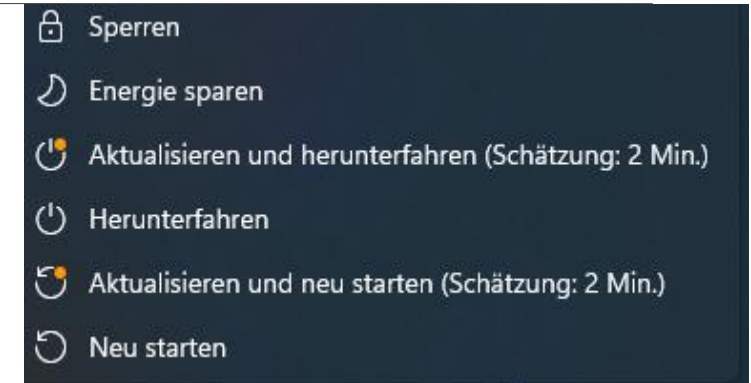
- Unbedingt bei Nutzung fremder Geräte und Bank Geschäften nutzen!



Pixabay

Neustart des Geräts

- „Herunterfahren“ behält Daten im Arbeitsspeicher für die nächste Sitzung.
 - „Neustart“ entleert den Arbeitsspeicher vollständig und lädt alle Dienste und Treiber neu.
 - Wichtig: System-Änderungen / Updates werden dadurch erst wirksam!
- Generelle Empfehlung 1-mal pro Woche einen Neustart machen



Quelle: D. Reichbauer



Pixabay

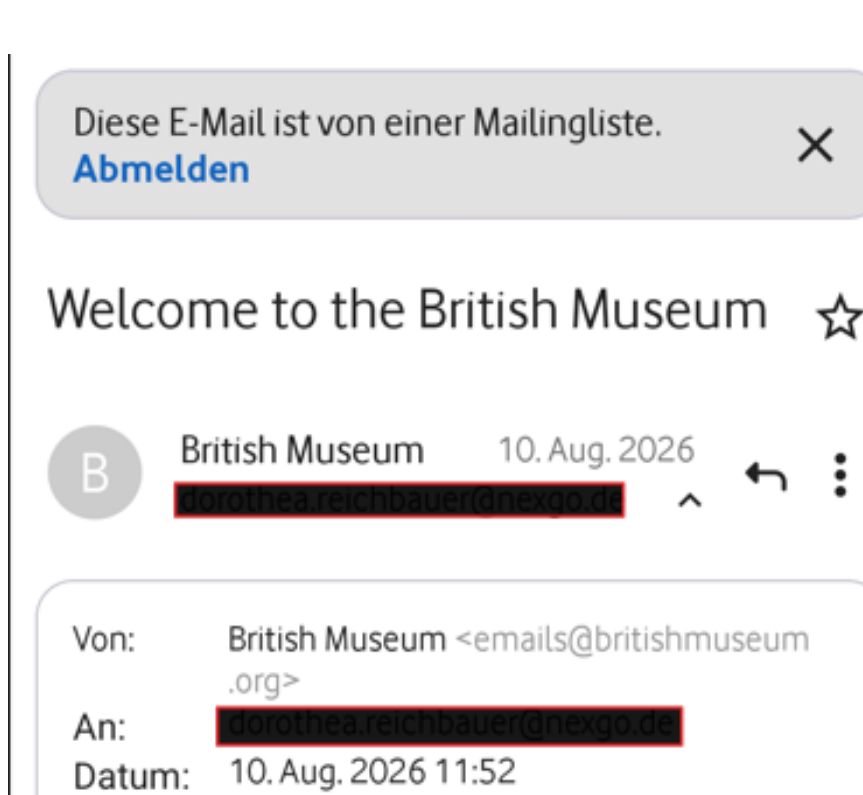
E-Mail-Betrüger erkennen

- Eine E-Mail die sensible Daten abfragt, wie Kreditkarten-Nummer, PIN, TAN, Passwörter o. ä. niemals beantworten!
- Banken kontaktieren Kunden nie so.
- E-Mail können offiziell aussehen, aber es ist ein Betrugsversuch. Solche SPAM-Nachrichten bitte sofort löschen und **keinesfalls** einen Link im E-Mail anklicken!
- Im Zweifel die Bank oder den Anbieter kontaktieren.

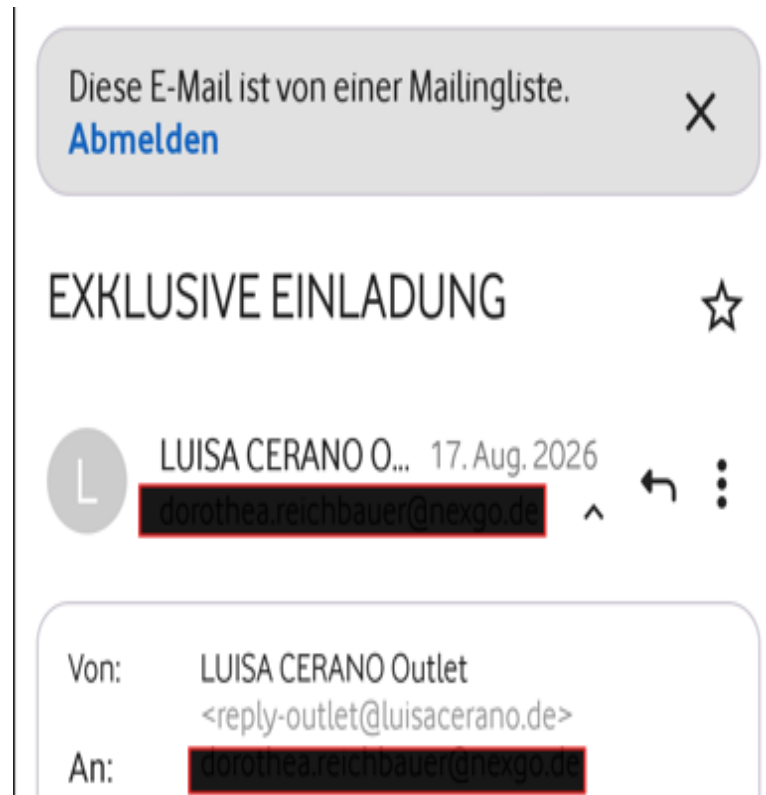
Beispiel von seriösen E-Mail-Adressen



**Vertrauens-
würdige Mails
sind oft schon
an der E-Mail-
Adresse zu
erkennen.**



Quelle: D. Reichbauer



Quelle: D. Reichbauer



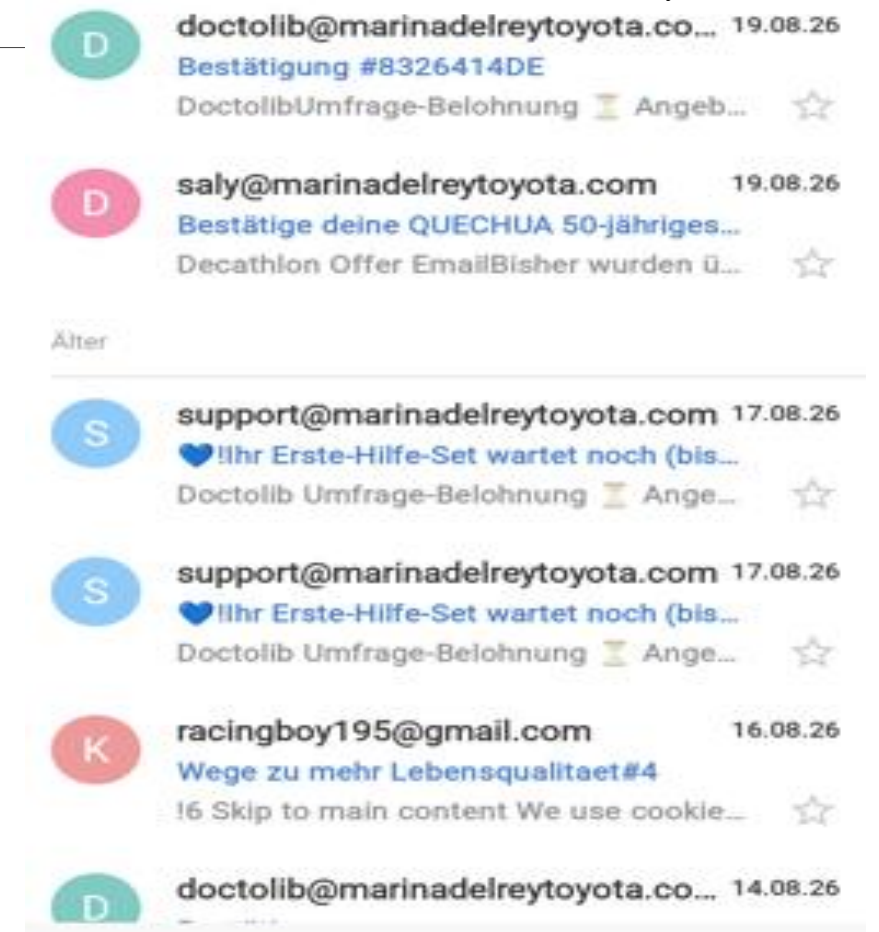
Pixabay

Typische Phishing-E-Mail

Betrügerische E-Mails haben oft irrwitzige Adressen, Betreffzeilen, Sonderzeichen, Endungen, etc.



Quelle: D. Reichbauer



Quelle: D. Reichbauer



Pixabay

Typische Phishing-E-Mail

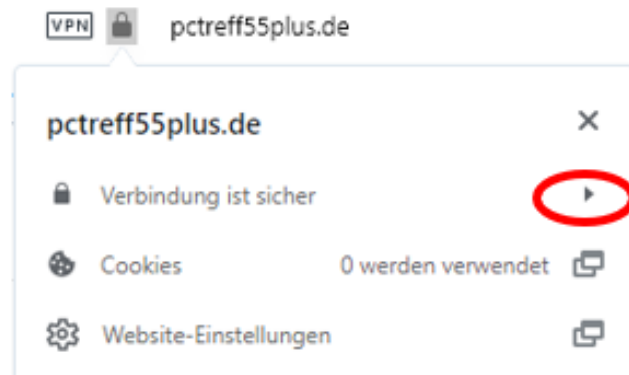
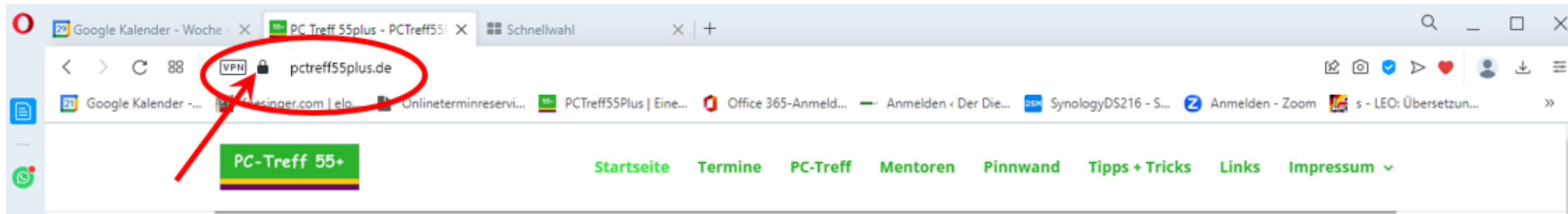
- **Niemals offensichtlich betrügerische E-Mails öffnen, denn bei aktivierter Lesebestätigung weiß der Absender, dass die E-Mail-Adresse real ist.**
- **Und die Angriffe werden weiter gehen.**



Beispiel einer sicheren Verbindung



Pixabay



Quelle: PC-Treff 55+



Pixabay

VPN - Virtual Private Network

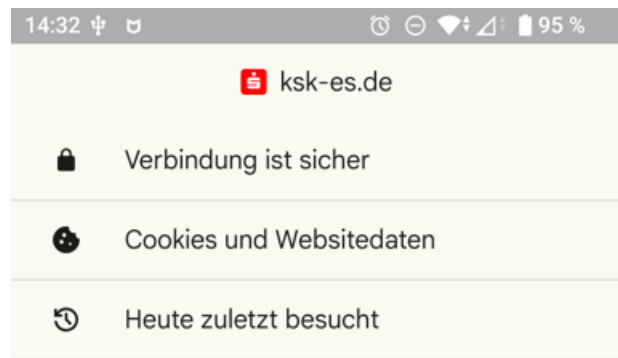
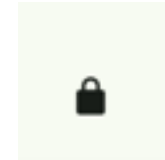
- Ein VPN verschlüsselt den Datenverkehr und stellt damit eine sichere Verbindung ins Internet zu einem anderen Netzwerk oder Server her. Es macht das surfen anonym und immun für Man-in-the-Middle-Angriffe.
- Im Cafe, Hotel, Zug oder öffentlichem Netzwerk, schützt das VPN meine Daten vor dem Mitlesen durch Fremde im selben Netzwerk. Es gibt kostenlose und kostenpflichtige VPN-Anbieter, eine Lizenz ist immer für mehrere Geräte.
- NordVPN, Surfshark, ExpressVPN, TotalVPN, Norton



Pixabay

Sichere / Unsichere Homepage

- **Sichere Internet-Adresse beginnt mit `https://` das neuste verschlüsselte Internet Protokoll**



Quelle: D. Reichbauer



Quelle: D. Reichbauer

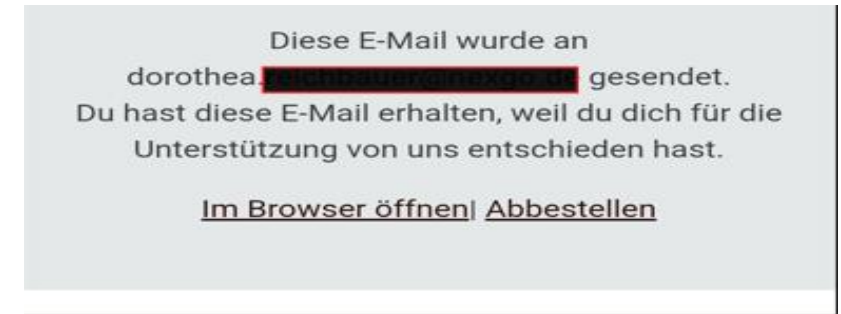
- **Unsichere Internet-Adresse beginnt mit `http://` das ist ein veraltetes Internet Protokoll**

Newsletter abbestellen/abmelden

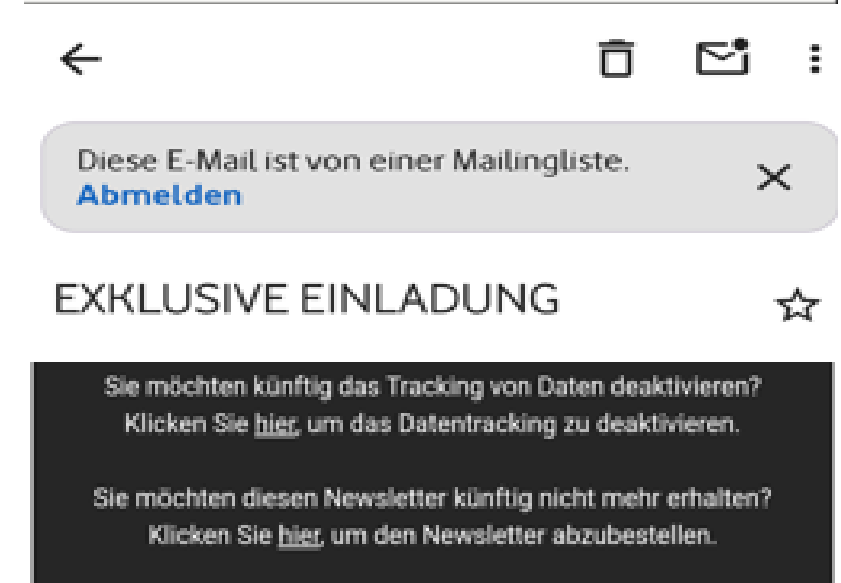


Pixabay

- Newsletter bekommt man oft nachdem Cookies zugestimmt wurden. Auch werden E-Mail-Adressen verkauft.
- Meist gibt es am unteren Mail-Ende einen Hinweis und Funktion zum Newsletter abbestellen. Der Wortlaut ist vielfältig und teilweise extra schwierig formuliert.



Quelle: D. Reichbauer



Quelle: D. Reichbauer

Quelle: D. Reichbauer



Weitere hilfreiche Informationen rund um das Thema
„Sicherheit im Internet“ finden Sie auf den Seiten
des [Bundesamts für Sicherheit in der Informationstechnik](https://www.bsi.bund.de).



Pixabay

Digitaler Verbraucherschutz



Aktuelle Themen und Vorfälle



Sicher im digitalen Alltag



Kooperationen und Forschung



Verbraucherschutz-Newsletter
"Sicher informiert"



Bericht zum Digitalen
Verbraucherschutz



IT-Sicherheitskennzeichen



Sie haben einen IT-
Sicherheitsvorfall?



Internet der Dinge / Smart Home /
vernetztes Fahren



Wie Sie eine Cloud für Ihre Daten
sicher nutzen



5G, Blockchain und Co. sicher
gestalten



Identitätsdiebstahl und seine Folgen

Quelle: Bundesamt für Sicherheit in der Informationstechnik



Pixabay

Fazit

**Auch wenn Sie technische Hilfsmittel zum Schutz in
der Internetnutzung einsetzen,
bleiben Sie kritisch und wachsam!**



Pixabay

Vielen Dank für Ihre Aufmerksamkeit
