Deutschland sicher im Netz

PolisiN

Politiker:innen sicher im Netz

PolisiN

Politiker:innen
sicher im Netz

Vortrag: Zielscheibe Politik

So schützt du dich vor Cyberangriffen

Deutschland
sicher im Netz

PolisiN

Politiker:innen sicher im Netz

EIN KOSTENFREIES ANGEBOT VON

Deutschland sicher im Netz

DsiN engagiert sich seit 2006 als gemeinnütziger Verein für digitale Aufklärung und Cybersicherheit in Deutschland.

Unter der Schirmherrschaft des Bundesministeriums des Innern richtet sich DsiN mit praxisnahen Angeboten an Verbraucher:innen aller Altersgruppen, Beschäftigte kleiner und mittlerer Unternehmen sowie politische Entscheidungsträger:innen.

DsiN bringt Perspektiven aus Zivilgesellschaft, Wirtschaft, Politik und Wissenschaft zusammen und setzt sich gemeinsam mit seinen Mitgliedern für digitale Souveränität und Vertrauen in die Digitalisierung ein.

MEHR AUF

sicher-im-netz.de
polisin.de

Das Projekt

PolisiN
Politiker:innen
sicher im Netz

Vermittlung allgemeiner Grundlagen zur Digitalisierung

Sensibilisierung im Alltag für mehr IT-Sicherheit

Praxisnahe Orientierung, Hilfe und Austausch

Keine Rechtsberatung

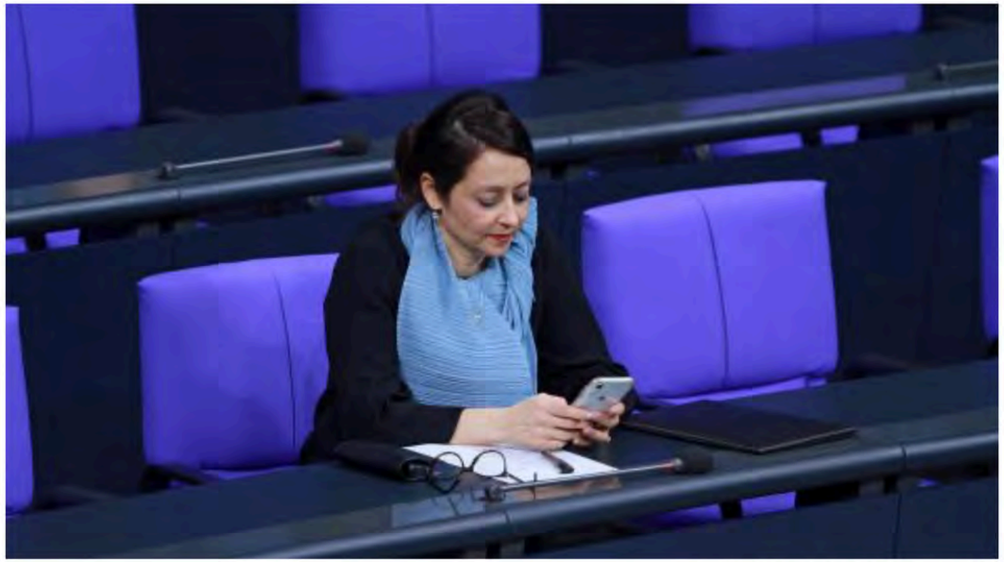
Ablauf

1. Sichere Passwörter
2. Social Engineering
3. Sichere Kommunikation
4. Einstellungen für den Browser
5. Arbeiten im Büro & unterwegs
6. Private Geräte und Schatten-IT

Cyberangriff

Hacker erbeuten persönliche Daten von Justizsenatorin Badenberg

Di 19.08.2025, 14:01 Uhr



imago images/dts Nachrichtenagentur

Quelle: rbb24

SENSIBLE DATEN

Einbruch bei CDU: Laptop von Hamburger Digitalexpertin gestohlen

03.07.2024, 13:00 Uhr • Lesezeit: 2 Minuten

Von André Zand-Vakili

Die Bundestagsabgeordnete Franziska Hoppermann (CDU) wurde Opfer eines Einbruchs.

© Marcelo Hernandez | Marcelo Hernandez

Hamburg. **Büro vom Kreisverband Wandsbek betroffen. Gerät gehört der Bundestagsabgeordneten Franziska Hoppermann. War es ein gezielter Diebstahl?**

Quelle: Hamburger Abendblatt

Sichere Passwörter

Brut-Force-Angriffe

Automatisiertes Ausprobieren von Millionen Passwort-Kombinationen in Sekunden.

*Bei Eingabe von 170.424.973 Passwörtern pro Sekunde.

Passwortlänge	Genutzte Zeichen	Dauer
5	Kleinbuchstaben (26 mögliche Zeichen)	0,069 Sekunden
6		1,8 Sekunden
7		47,1 Sekunden
8		20 Minuten 24 Sekunden
5	Klein- & Großbuchstaben & Ziffern (62 mögliche Zeichen)	5,4 Sekunden
6		5 Minuten 30 Sekunden
7		5 Stunden 42 Minuten
8		14 Tage 19 Stunden
5	Klein- & Großbuchstaben, Ziffern & Sonderzeichen (95 mögliche Zeichen)	45,4 Sekunden
6		1 Stunde 48 Minuten
7		4 Tage 17 Stunden
8		1 Jahr 2 Monate 12 Tage

Quelle: datenschutz.org

Sichere Passwörter

Ein sicheres Passwort hat mindestens zwölf Zeichen und vier verschiedene Zeichenarten.

Keine Weitergabe von Passwörtern in Chats und E-Mails.

Zusätzlich zu einem sicheren Passwort sollte eine Multi-Faktor-Authentifizierung eingerichtet werden.

Es empfiehlt sich einen Passwort-Manager zu nutzen.

Kein Abspeichern von Passwörtern im Browser, auf dem Smartphone und auf privaten Geräten.

Es braucht regelmäßige Sensibilisierung gegenüber neusten Phishing-Methoden.

Social Engineering

Phishing, Smishing & Quishing

Phishing ist der Versuch durch täuschend echte Nachrichten an vertrauliche Daten zu kommen oder Schadsoftware zu installieren.

Wie wird dies umgesetzt?

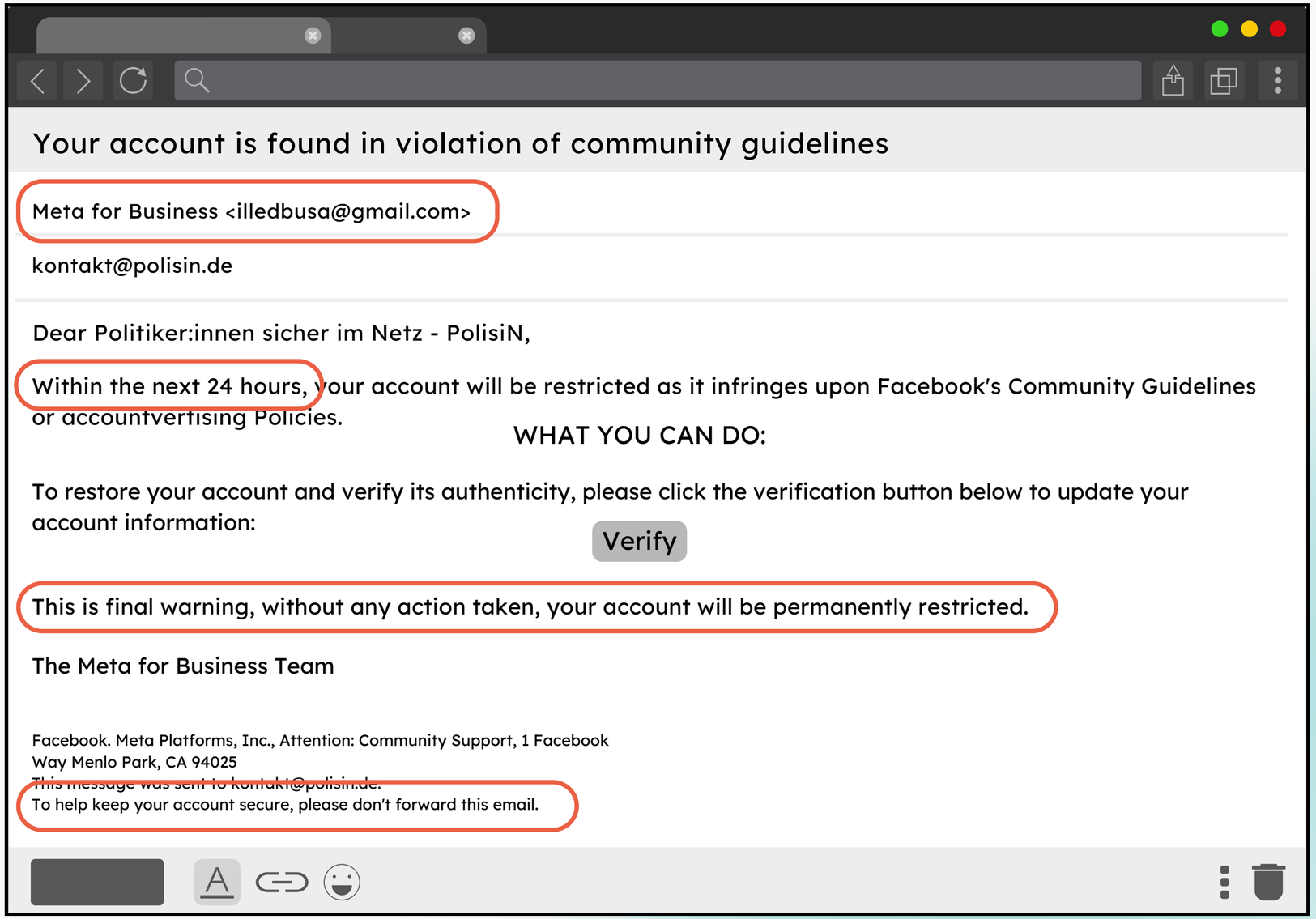
- Telefonanrufe
- Briefe
- Websites
- E-Mails
- SMS
- QR-Code

Wie kann ich mich schützen?

- Sichere Passwörter
- Multi-Faktor-Authentifizierung (MFA)
- Nutzung von Passwortmanagern
- Nutzung von Passkeys

Social Engineering

Erkennen von Phishing Nachrichten



Your account is found in violation of community guidelines

Meta for Business <illedbusa@gmail.com>

kontakt@polisin.de

Dear Politiker:innen sicher im Netz - PolisiN,

Within the next 24 hours, your account will be restricted as it infringes upon Facebook's Community Guidelines or accountvertising Policies.

WHAT YOU CAN DO:

To restore your account and verify its authenticity, please click the verification button below to update your account information:

Verify

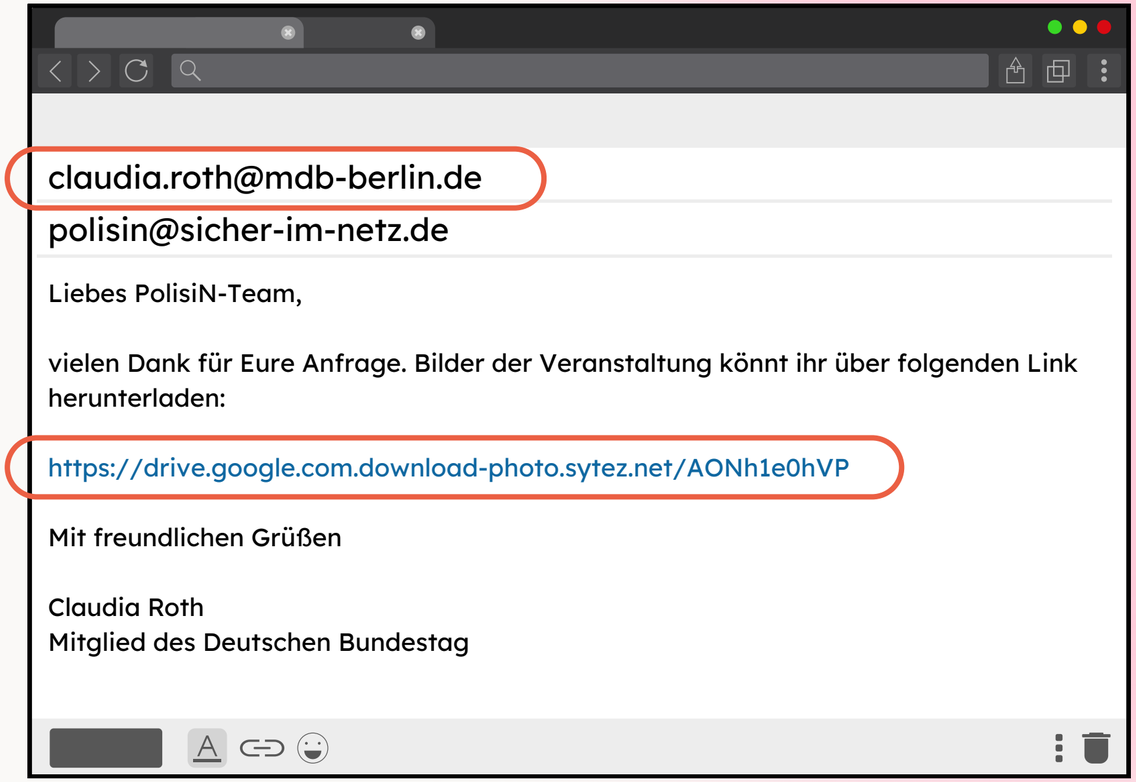
This is final warning, without any action taken, your account will be permanently restricted.

The Meta for Business Team

Facebook. Meta Platforms, Inc., Attention: Community Support, 1 Facebook Way Menlo Park, CA 94025
This message was sent to kontakt@polisin.de.
To help keep your account secure, please don't forward this email.

Social Engineering

Erkennen von Phishing Nachrichten



claudia.roth@mdb-berlin.de

polisin@sicher-im-netz.de

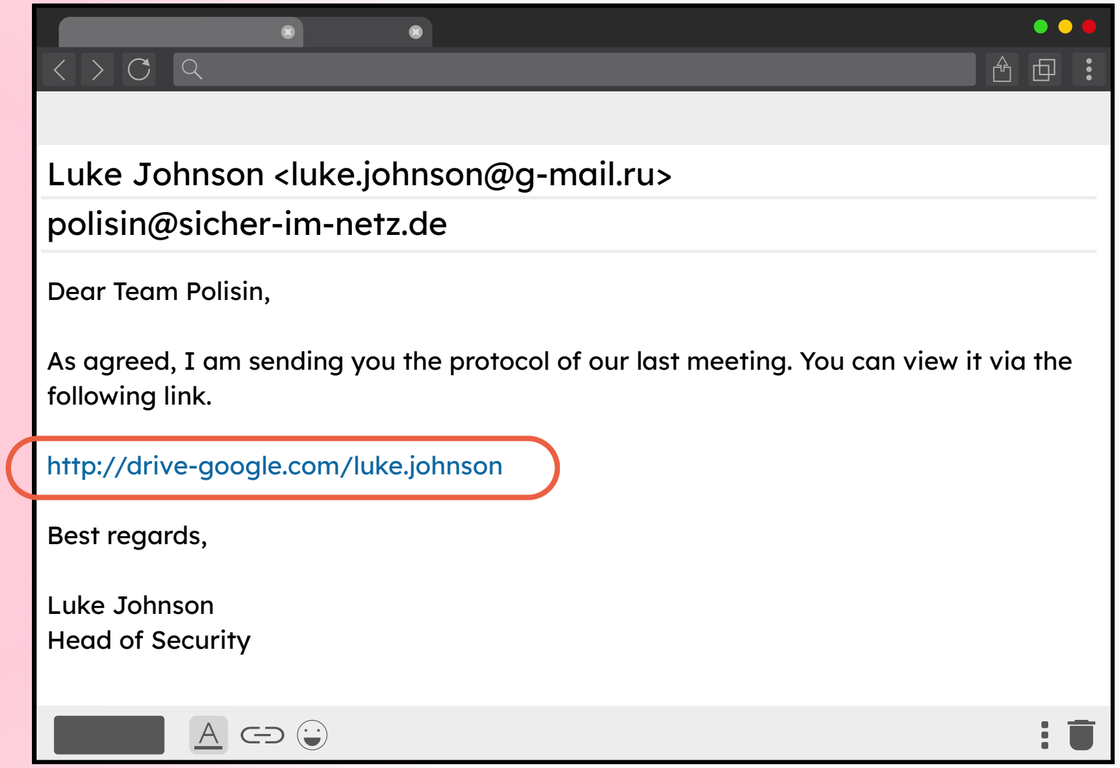
Liebes PolisiN-Team,

vielen Dank für Eure Anfrage. Bilder der Veranstaltung könnt ihr über folgenden Link herunterladen:

https://drive.google.com.download-photo.sytez.net/AONh1e0hVP

Mit freundlichen Grüßen

Claudia Roth
Mitglied des Deutschen Bundestag



Luke Johnson <luke.johnson@g-mail.ru>

polisin@sicher-im-netz.de

Dear Team Polisin,

As agreed, I am sending you the protocol of our last meeting. You can view it via the following link.

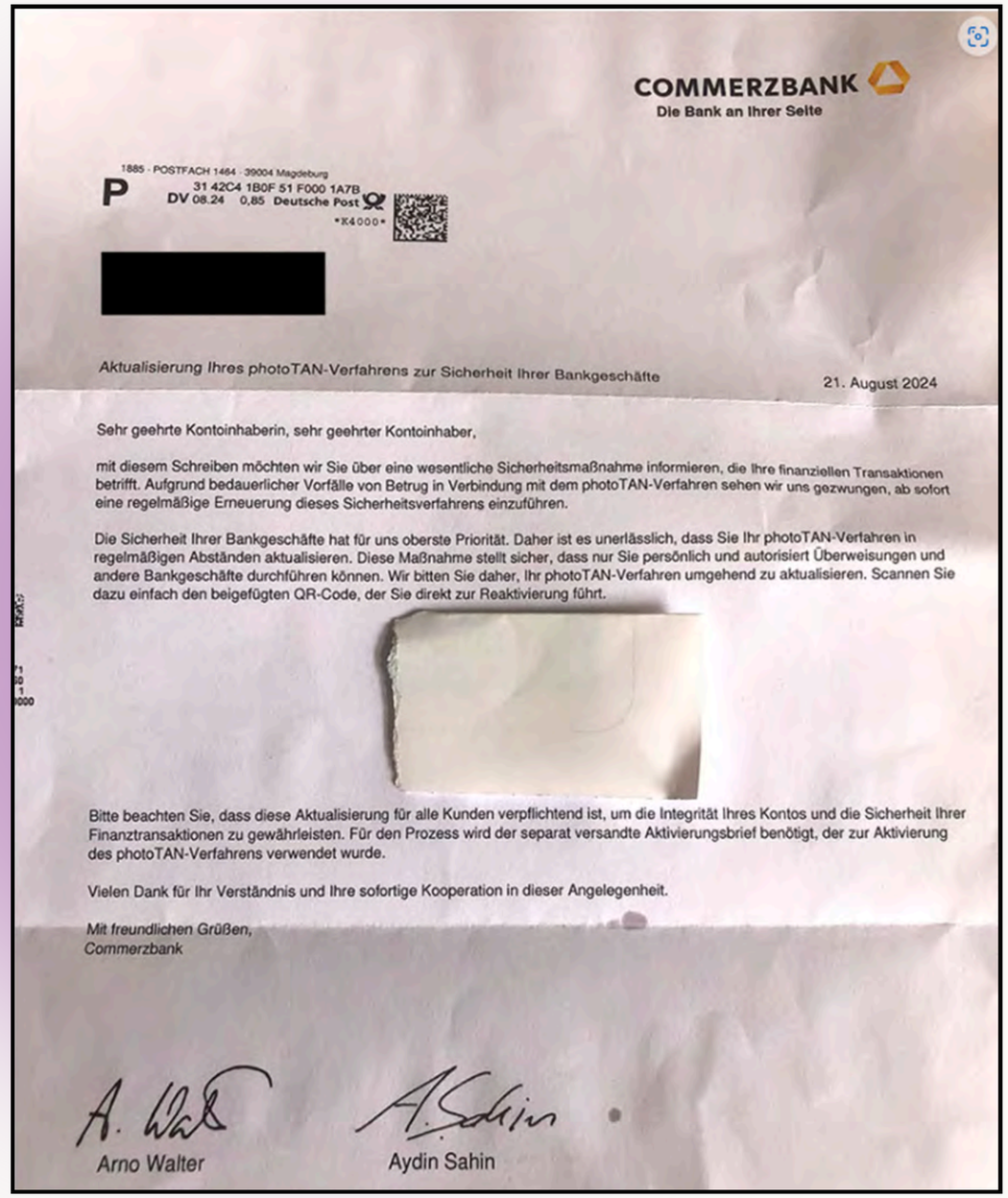
http://drive-google.com/luke.johnson

Best regards,

Luke Johnson
Head of Security

Social Engineering

Erkennen von Phishing Nachrichten



COMMERZBANK
Die Bank an Ihrer Seite

1885 · POSTFACH 1464 · 39004 Magdeburg
P 31 42C4 1B0F 51 F000 1A7B
DV 08.24 0,85 Deutsche Post
K4000

[redacted]

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.

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

A. Walter
Arno Walter

A. Sahin
Aydin Sahin

Social Engineering

Phishing und Co.: Präventive Lösungsansätze

Tipp: Sicherheitssatz
“Die Erdbeere ist eine fruchtige Nuss.“

- E-Mail-Filter nutzen.
- Absender, Nachrichten, Links und (unerwartete) Anhänge genau prüfen.
- Regelmäßig über neue Entwicklungen schulen.
- Grafiken, Inhalte und Wording kontrollieren.
- Datenbackups erstellen.

Social Engineering

Was ist Ransomware?

Ransomware ist Schadsoftware, die Daten und Systeme verschlüsselt und Lösegeldzahlungen fordert, um Zugänge wieder herzustellen

Folgen:

- Verlust von Daten und Informationen
- Arbeitsausfall
- Finanzieller Schaden

RANSOMWARE

IT-Wiederaufbau in Schwerin könnte Wochen dauern

Nach dem Ransomware-Angriff auf Systeme der Stadt Schwerin und eines Landkreises müssen Bürger wohl länger mit Einschränkungen rechnen.

in Pocket speichern merken

16. Oktober 2021, 13:12 Uhr, Sebastian Grüner/ dpa

Quelle: golem.de

Ransomware: Hackerangriff legt Uni Duisburg-Essen lahm

News

16 Dezember 2022 • 3 Minuten

Cyberkriminalität

Wegen einer Ransomware-Attacke wurde die IT-Infrastruktur der Uni Duisburg-Essen komplett lahmgelegt. Die Täter drohen jetzt damit, sensible Daten im Darknet zu veröffentlichen.

Quelle: CSO

Social Engineering

Ransomware: Lösungsansatz

Um Reaktionsfähig zu bleiben ist die Erstellung eines **Notfallplans** mit **Zuständigkeiten** für alle Teammitglieder ratsam.

Sollte es zu einem sicherheitsrelevanten Vorfall kommen ist die **Checkliste** zu beachten.

Checkliste:

- ☑ Ruhe bewahren
- ☑ Vom Netzwerk trennen
- ☑ Meldung machen (Fehlerkultur)
- ☑ Endgerät eingeschaltet lassen
- ☑ Letzte Anwendung speichern
- ☑ Nichts löschen, nichts klicken
- ☑ Gerät wechseln
- ☑ Fortsetzung Notfallplan mit IT

Quelle: BSI

Social Engineering

Ransomware: Lösungsansatz

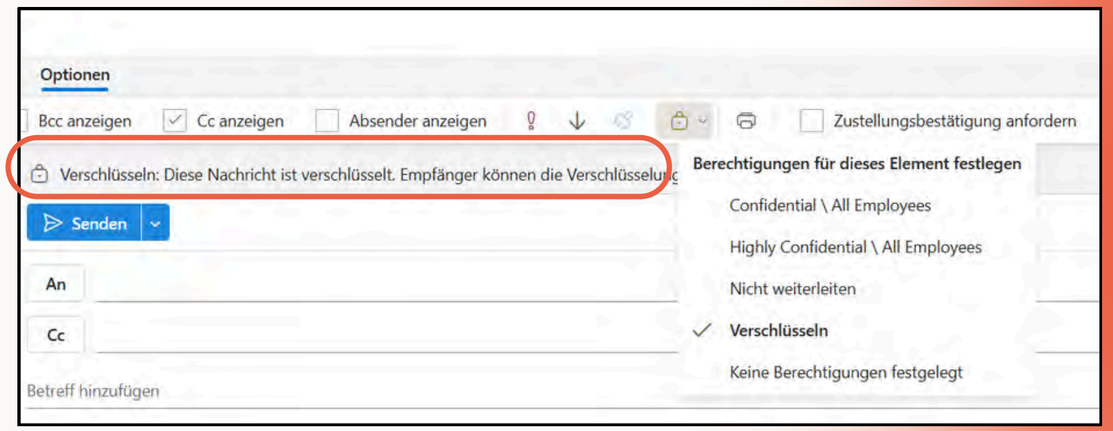
Was tun im privaten Ernstfall?

- ☑ Ruhe bewahren
- ☑ Internetverbindung trennen
- ☑ Passwörter ändern (auf anderem Gerät!)
- ☑ Wichtige Konten prüfen (E-Mail, Bank, Social Media)
- ☑ Betroffene Dienste informieren (z. B. Bank)
- ☑ Hilfe holen (IT-affine Personen, BSI)

Sichere Kommunikation

E-Mail

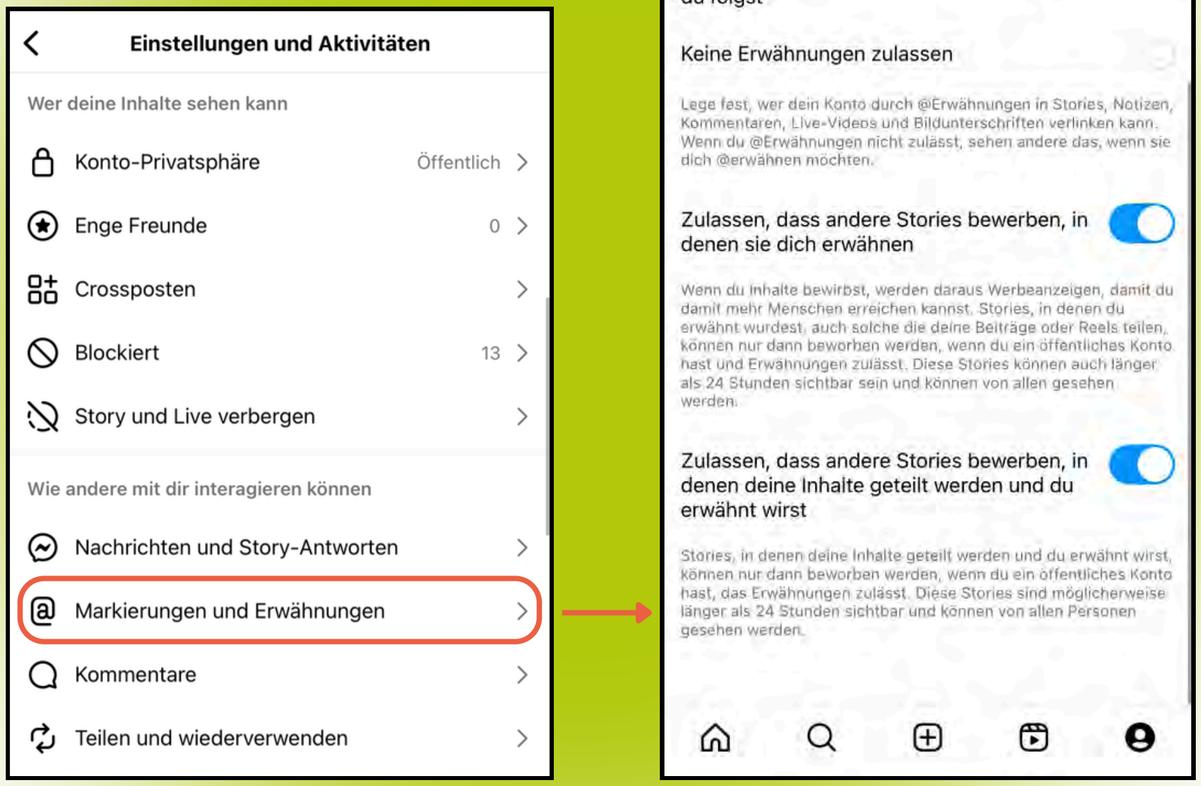
- Sensible E-Mails, besonders bei häufigen Kontakten, verschlüsseln
- Möglichst komplett auf Datenanhänge verzichten und stattdessen Cloud-Daten verlinken.
- Verschiedene Möglichkeiten der E-Mail-Verschlüsselung ausloten: Bspw. entweder Plugins installieren, Modus „Vertraulich“ in Gmail nutzen oder Verschlüsselung direkt in Outlook aktivieren.



Sichere Kommunikation

Social Media

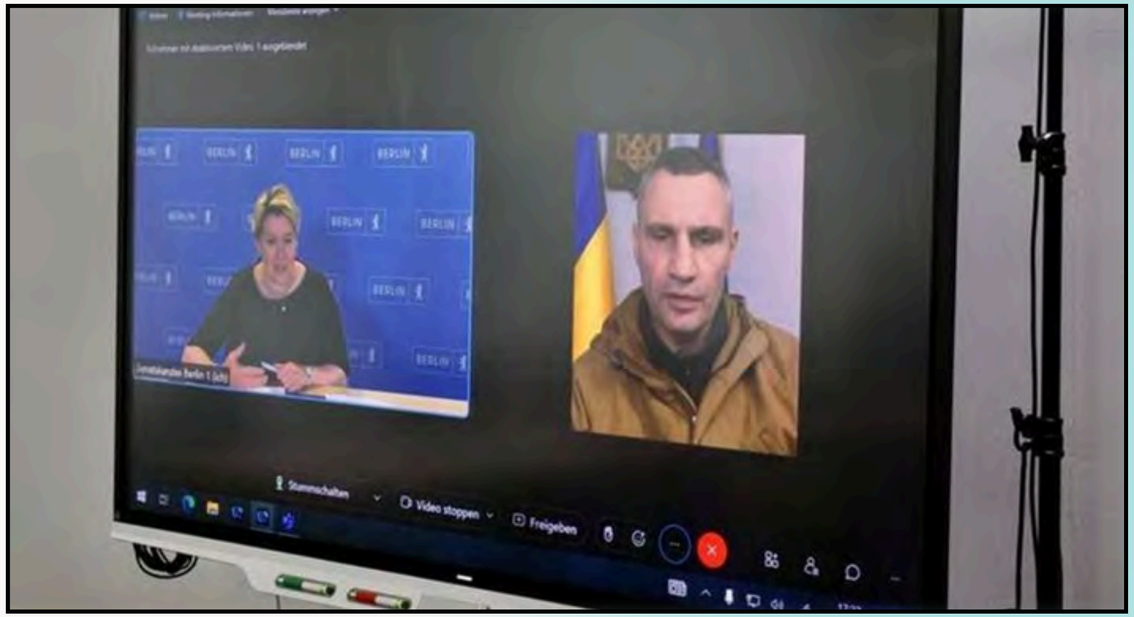
- Markierungen und Erwähnungen einschränken oder manuell freigeben.
- Standortfreigabe deaktivieren.
- Asynchron posten.
- Auf Hintergründe in Fotos achten.



Sichere Kommunikation

Risiken in der Nutzung von Videokonferenztools

- Videokonferenzen können abgehört oder durch unbefugte gestört werden (sog. Zoombombing).
- Dies wird durch schwache oder fehlende Zugangsbeschränkungen begünstigt.
- Videokonferenzen können durch Dritte gespeichert und Aufzeichnungen missbräuchlich verwendet werden.
- Fotos, Videos oder Audios können in Echtzeit durch KI manipuliert werden .



Quelle: deutschlandfunk

Sichere Kommunikation

Lösungsansätze zur sicheren Nutzung von Videokonferenztools

- [x] Nutzung von Wartezimmern und Passwörtern.
- [x] Nutzung sicherer Videokonferenz-Tools mit Ende-zu-Ende-Verschlüsselung.
- [x] Vermeidung der Freigabe von Teilnahme-Links oder Meeting-IDs in öffentlichen Räumen.
- [x] Beschränkung der Aufnahmefunktionen und sichere Speicherung von Aufzeichnungen.
- [x] Sensibilisierung zur Erkennung von KI generierten Deepfakes.
- [x] Zwei-Kanäle-Kommunikation einrichten.

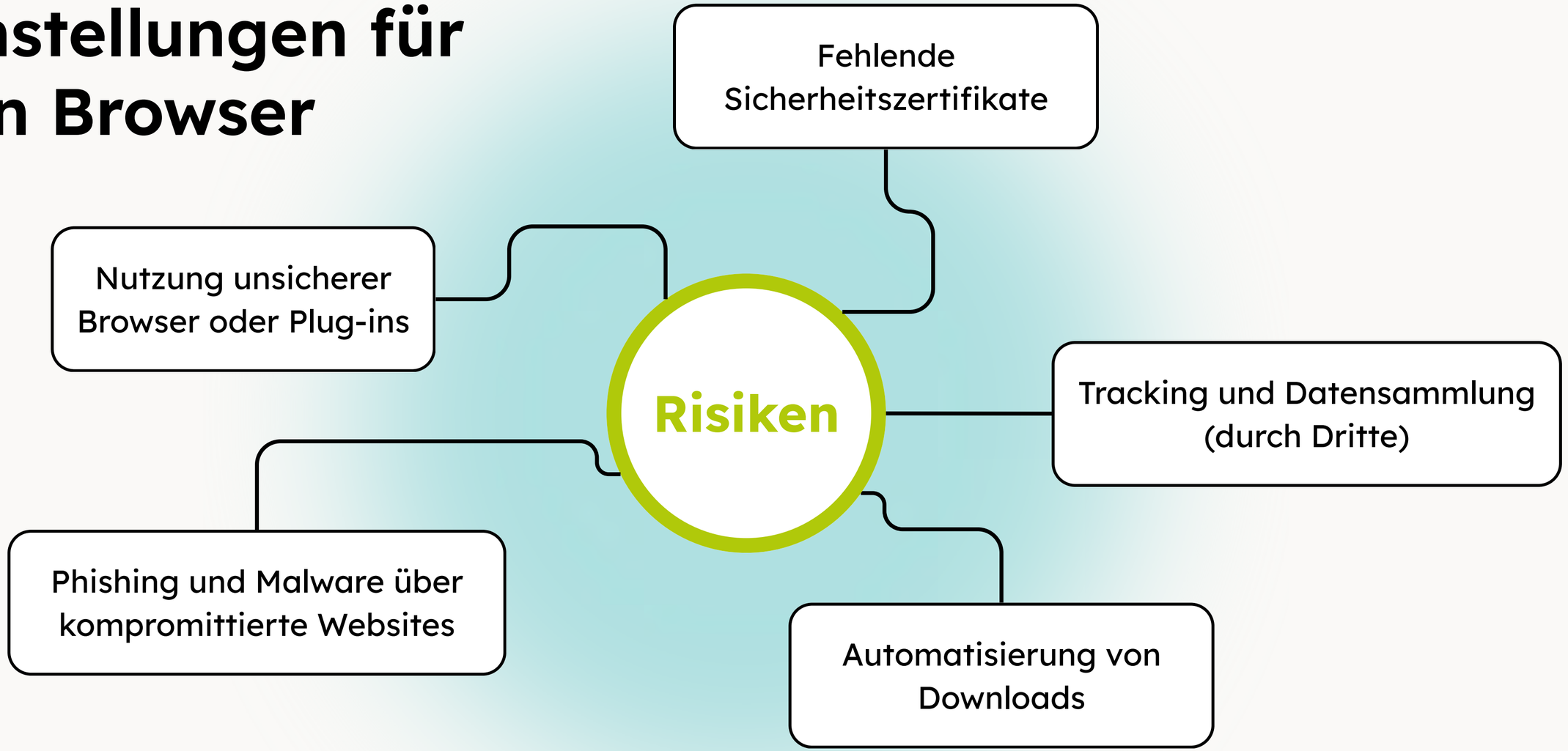
Sichere Kommunikation

Lösungsansätze zur Erkennung von Deepfakes

Tools für Videoüberprüfungen

- InVID Plugin
- Deepware.ai
- sensity.ai
- Quellenkritik

Einstellungen für den Browser



Einstellungen für den Browser

Es gilt grundsätzlich: Anwendungen, Dateien oder Mails **in einem aktuellen Browser zu öffnen ist sicherer, als lokal auf dem Endgerät** in einem Programm, selbst bei installiertem Virenschutz.

Einstellungen für den Browser

Cookies

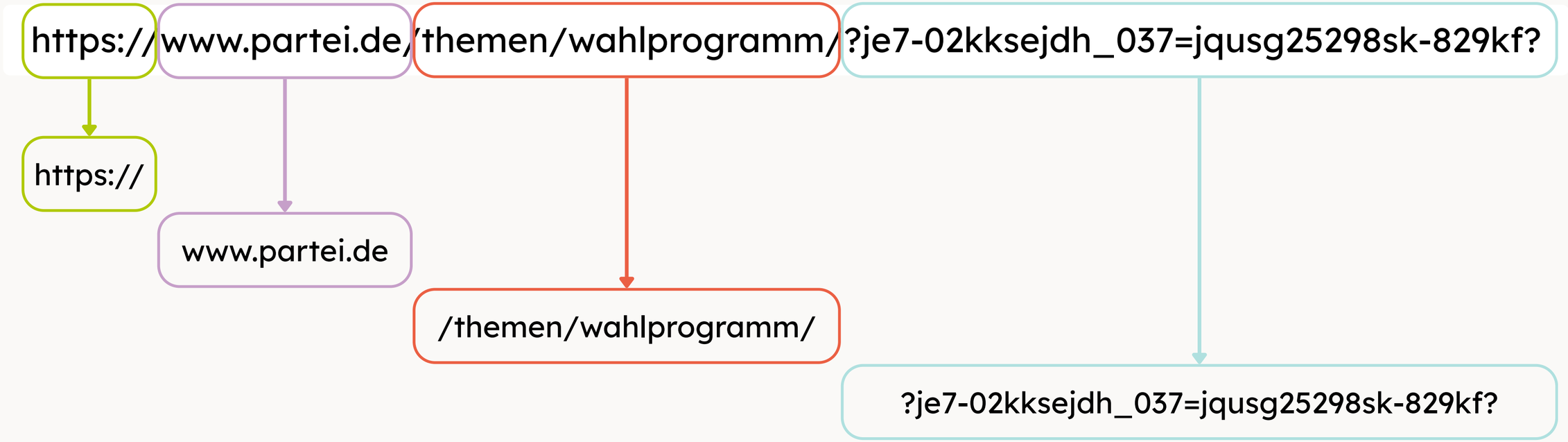
Was wird alles durch Cookies gespeichert?

- Scrollverhalten
- Eingaben in Formularfeldern
- Klickverhalten
- Conversions-Daten
- Weiterleitungen und Herkunftsquellen

- Verweildauer auf Webseiten
- Häufigkeit der Besuche
- Daten über Browser, Betriebssystem und Bildschirmauflösung
- IP-Adressen und Gerätedetails der Endgeräte
- Standortdaten

Einstellungen für den Browser

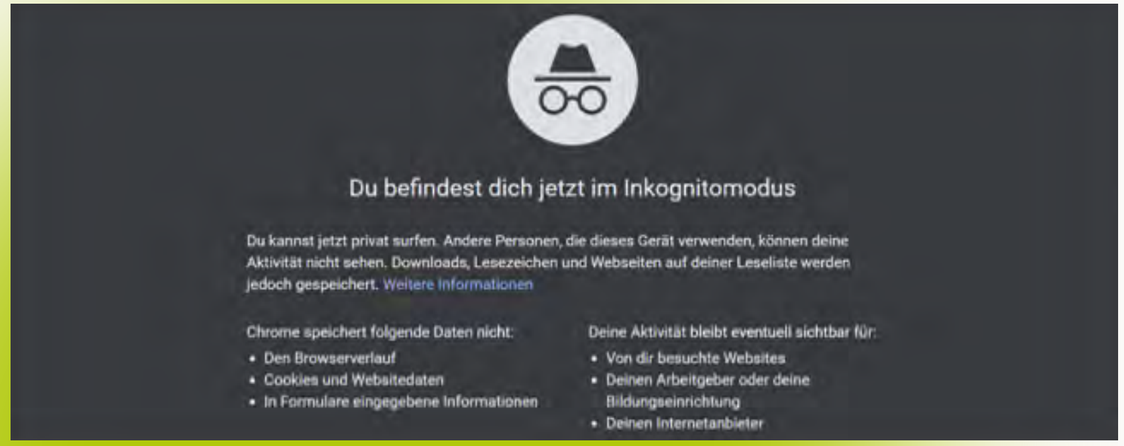
Was verrät uns eine URL?

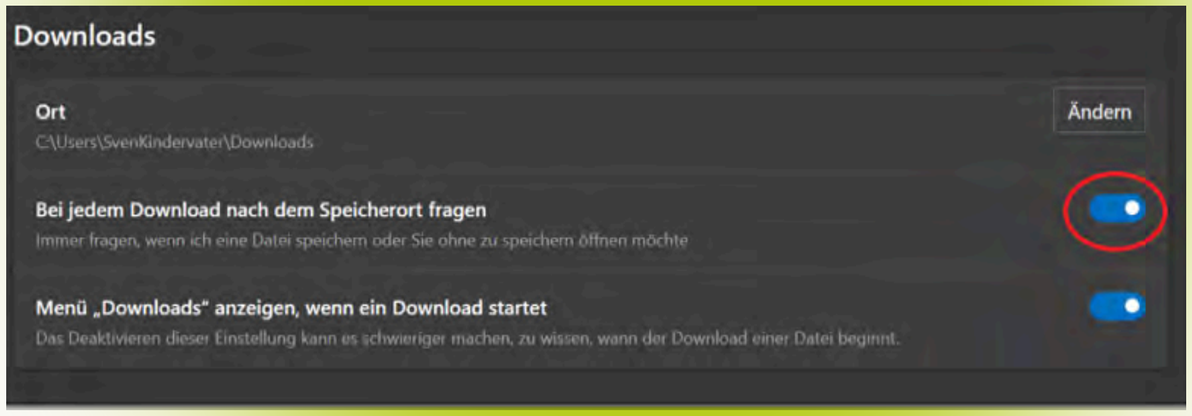


Einstellungen für den Browser

Lösungsansätze für eine sichere Browsernutzung

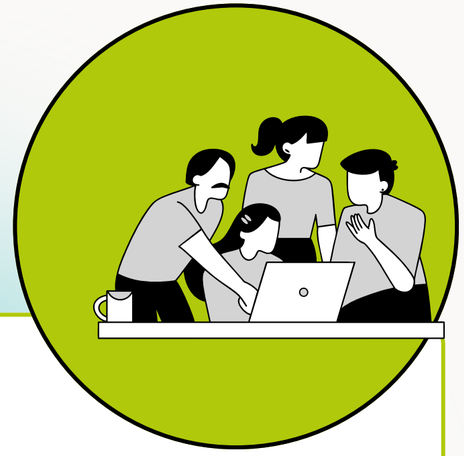
- Browserdaten regelmäßig löschen.
- Werbung blockieren.
- Nachverfolgung blockieren.
- Browser updaten und aktuell halten.
- Cookies überprüfen und nicht immer annehmen.
- Download-Abfrage aktivieren.
- Inkognito oder VPN nutzen.





Arbeiten im Büro & unterwegs

Szenario: Arbeiten im Büro

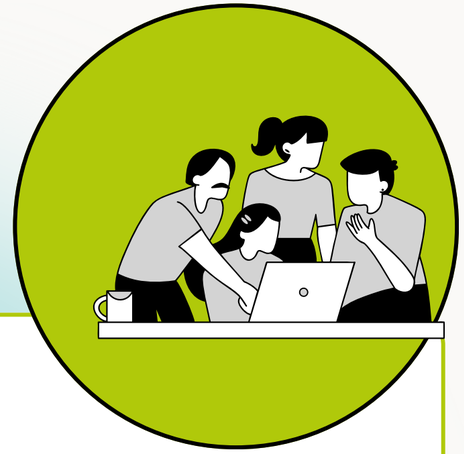


Risiken im Büroalltag

- Gemeinsam genutzte Geräte
- Ungesicherte Geräte
- Fehlende Übersicht über die vorhandenen Geräte
- Einbruch und Diebstahl
- Vernetzung mit privaten Geräten
- Unklare Zuständigkeiten, Abläufe und Kompetenzen
- Datenverlust durch lokale Speicherung statt Cloud-Lösung

Arbeiten im Büro & unterwegs

Szenario: Arbeiten im Büro



Sicherheitsmaßnahmen und praktische Hinweise

- Einrichtung sicherer Arbeitsplätze
- Sperren von Computern bei Abwesenheit
- Sensible Dateien stets sichern bzw. die Cloud nutzen
- Einsatz sicherer Passwörter
- Nutzung von Passkeys
- Verwendung von Schließsystemen
- Regelmäßige Schulungen im Team
- Ausarbeitung von Sicherheitsrichtlinien und Notfallplänen

Arbeiten im Büro & unterwegs

Szenario: Mobiles Arbeiten

Risiken beim mobilen Arbeiten

- Risiken wie beim Arbeiten im Büro +
- Nutzung öffentlicher WLAN-Zugänge
- Abhören von Gesprächen und Auslesen des Bildschirms
- Unbefugter Zugriff auf die Geräte
- Höhere Gefahr für Verlust von Geräten
- Nutzung unsicherer Ladestationen (Juice Jacking)
- Erreichbarkeiten und Abläufe in Notfällen
- Höhere Wahrscheinlichkeit von Interaktionen mit Unbekannten

Arbeiten im Büro & unterwegs

Szenario: Mobiles Arbeiten

Sicherheitsmaßnahmen und praktische Hinweise

- Maßnahmen wie beim Arbeiten im Büro +
- VPN-Nutzung
- Nutzung eigener Hotspots
- Keine öffentlichen Gespräche über vertrauliche Themen
- Displayfolie verwenden
- Sicheres Zubehör nutzen
- Kein automatisches Einwählen in (öffentliche) Wifi-Netze
- Automatische Anmeldungen bei Diensten überprüfen
- Geräte nicht unbeaufsichtigt lassen
- Externen Zugang zu Geräten vorher prüfen und bei Verlust sofortige Sperrung veranlassen
- Cloud-Nutzung statt lokaler Daten, lokale Daten verschlüsseln

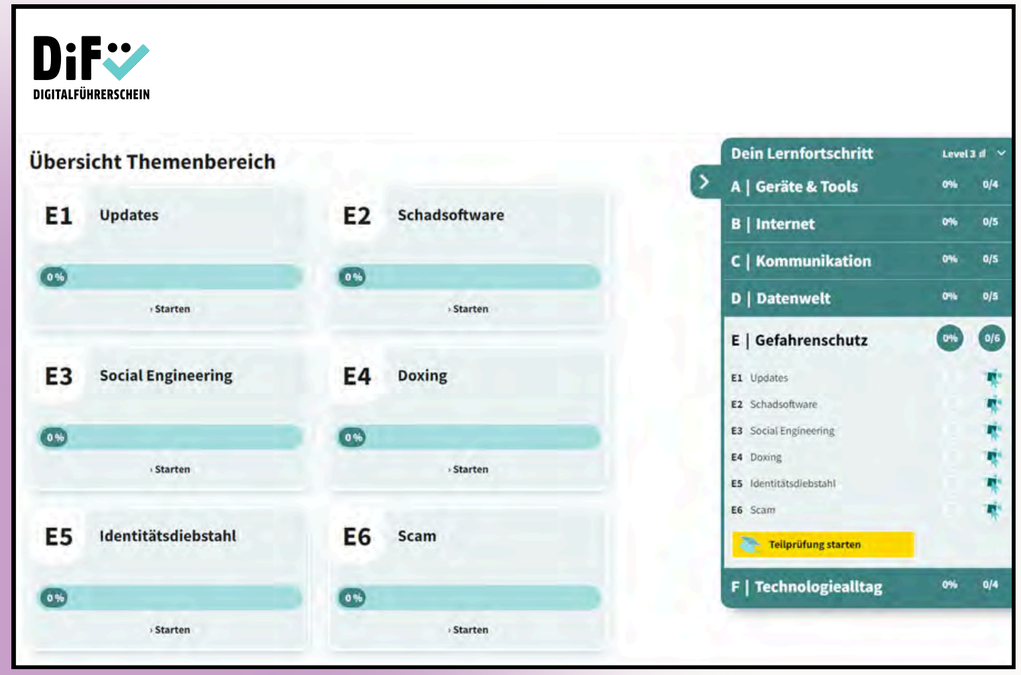
Private Geräte und Schatten-IT

Private Geräte und Schatten-IT

Lösungsansätze

- Minimierung der Verwendung privater Geräte von Schatten-IT
- Installation von Sicherheitssoftware
- Richtlinien für die Nutzung privater Geräte festlegen
- Trennung zwischen privaten und beruflichen Daten
- regelmäßige Sicherheitschecks
- Erfassen sämtlicher privater Geräte, die im beruflichen Kontext verwendet werden
- Prüfen welche Zugriffe nötig sind und auf was tatsächlich zugegriffen werden kann

Hier geht's zur SiBa App



Hier geht's zum Digitalführerschein

Offene Fragen und Austausch

Folge uns für mehr Informationen

PolisiN Politiker:innen sicher im Netz

@polisin_dsin

PolisiN - Politiker:innen sicher im Netz

DsiN Deutschland sicher im Netz

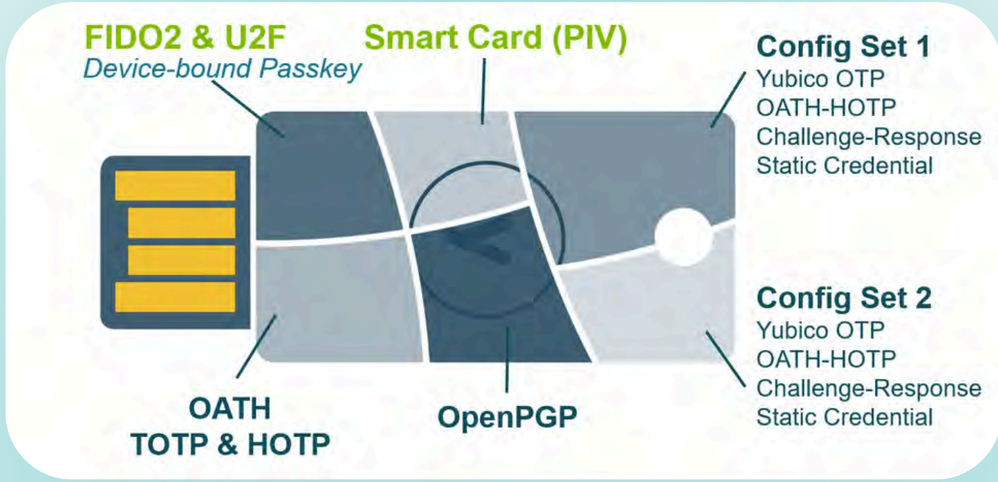
@deutschland.sicher.im.netz

Deutschland sicher im Netz e.V. (DsiN)

Mit Unterstützung von

GOVERNIKUS

yubico



PolisiN
Politiker:innen
sicher im Netz

Vielen herzlichen Dank!

Wir freuen uns über eine Weiterempfehlung.

Kontakt:

+49 30 767581564
polisin@sicher-im-netz.de

DsiN Deutschland sicher im Netz

GOVERNIKUS

yubico