

Vorsicht, Falle!

Die Tricks der Online-Betrüger

Über mich

Marina Plag

IT-Forensikerin

Cybercrime-Zentrum Baden-Württemberg

Inhalt

- ▶ Kriminalität im Web
- ▶ Manipulation
- ▶ Software
- ▶ Zugangsdaten
- ▶ Links
- ▶ Datenmißbrauch
- ▶ Kaufen & Verkaufen
- ▶ Anlagebetrug
- ▶ Wenn's passiert ist

Kriminalität im Web



Professionalisierung

Wie ein Unternehmen mit Arbeitsteilung

- ▶ “Schulungen” von “Mitarbeitern”

Zusammenarbeit

- ▶ Legale Firmen (z.B. Provider)
- ▶ Illegale Dienstleister (z.B. Geldwäsche-Services)

International

Technologische Entwicklung

Künstliche Intelligenz

- ▶ Email-Texte, Webseiten
- ▶ Deepfakes (Stimme, Bilder, Video)
- ▶ Programmierung
- ▶ Datenanalyse

Manipulation



Druck

- ▶ Autoritätspersonen (Polizei, Finanzamt)
 - ▶ Unannehmlichkeiten (Kontosperrung)
 - ▶ Peinlich
 - ▶ Schlechte Nachrichten (Schockanrufe)
-
- ➔ Typisch: Zeitdruck
 - ➔ Ziel: klares Denken unterbinden

Amazon : Ihr Konto wurde aufgrund verdächtiger Aktivitäten gesperrt. Bitte aktualisieren Sie vor dem 27/02/2023 über : kunde-apperneuerung.com

Vertrauen

- ▶ Vertrauenswürdige Instanzen (Verbraucherzentrale)
- ▶ Beziehungen (Pig Butchering)
- ▶ Hilfsbereitschaft (Spenden)

➔ Barrieren abbauen

Hallo Mama, das is meine neue Nummer,
kannst du diese speichern und mir auf
Whatsapp schreiben

Aktuelle Ereignisse

- ▶ Prominentenklatsch
- ▶ Politik: Corona
- ▶ Saisonal: Weihnachten



**Volksbanken
Raiffeisenbanken**

um die Auswirkungen der gestiegenen Energiepreise für die Verbraucher abzumildern, wird im September ein Pauschalbetrag von 300 Euro an alle Erwerbstätigen ausbezahlt. Dies ist ein Beschluss der Bundesregierung und Inhalt des Entlastungspakets 2022, welches die durch den Ukraine-Krieg entstandene Energiekosten-Explosion etwas abfedern soll.

Wer erhält die Energiepauschale?

- **Steuerpflichtige** mit Einkünften aus Gewinneinkunftsarten (§ 13, § 15 oder § 18 des Einkommensteuergesetzes) und
- **Arbeitnehmerinnen und Arbeitnehmer**, die Arbeitslohn aus einem gegenwärtigen Dienstverhältnis beziehen und in die Steuerklassen I bis V eingereiht sind oder als **geringfügig Beschäftigte** pauschal besteuert werden.

Um Ihre Identität sowie den Anspruch auf eine Auszahlung feststellen zu können, benötigen wir eine Bestätigung Ihrer bereits angegebenen Daten bei der Erstellung Ihres Girokontos in einer unserer Filialien.

Geben Sie noch heute Ihre aktuellen Daten auf unserer Homepage an und erhalten Sie innerhalb der nächsten vier Wochen Ihre Auszahlung der Energiepauschale. Dies können Sie ganz bequem von zu Hause aus erledigen, anbei finden Sie einen Direktlink zu den geforderten ...

[Zur Homepage](#)

Zum Mitnehmen

- ▶ Auf eigene Emotionen achten
- ▶ Zeitdruck?
- ▶ Gesunder Menschenverstand
- ▶ Google
- ▶ Auf einem anderen Weg verifizieren
- ▶ Nicht interagieren: auflegen, löschen, blockieren
- ▶ Geheimwort: nicht elektronisch teilen

Software



Schadsoftware (Malware)

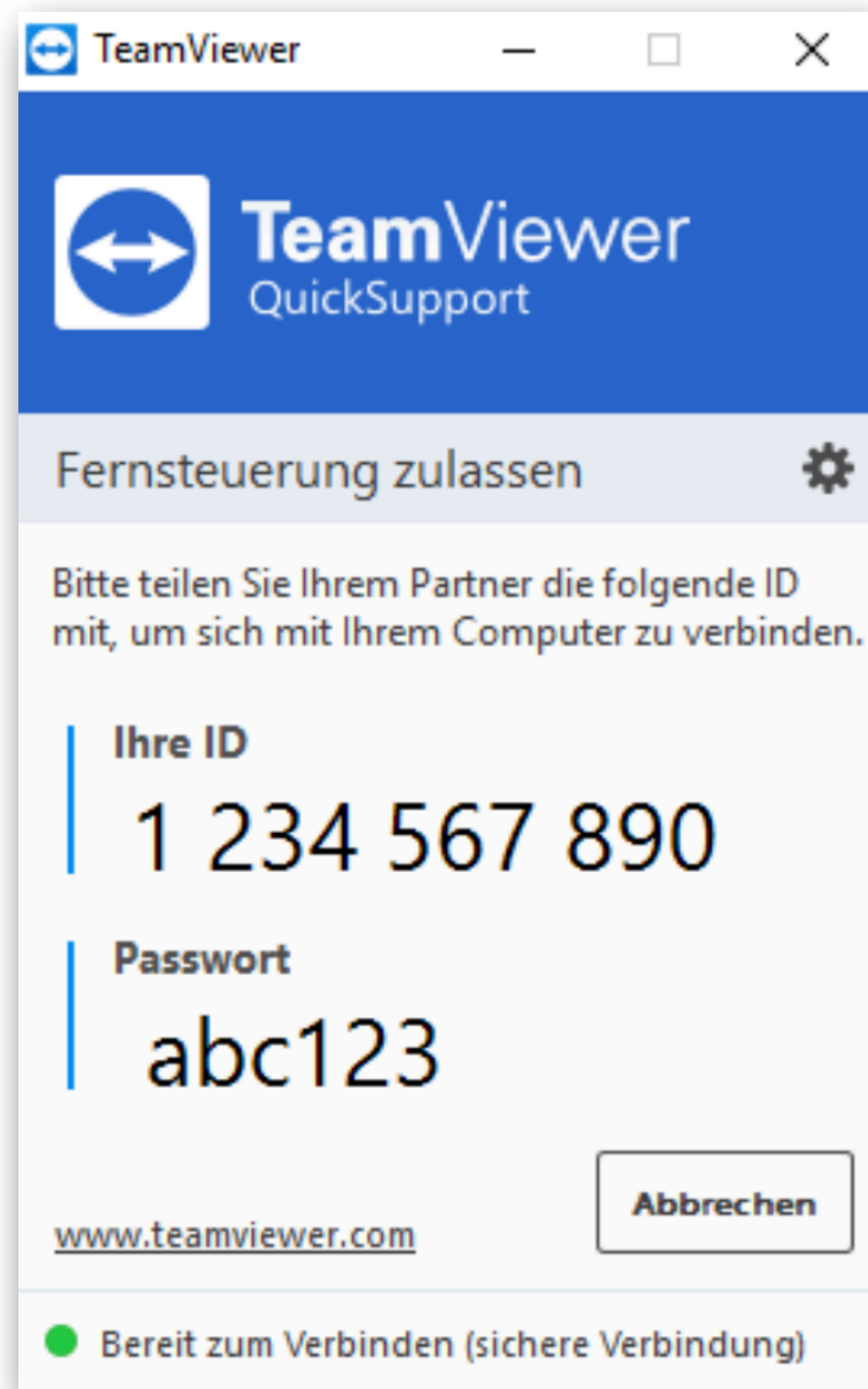
- ▶ Schäden verursachen, z.B. Daten löschen
- ▶ Daten stehlen
- ▶ unbefugten Zugriff ermöglichen

Schadsoftware einfangen

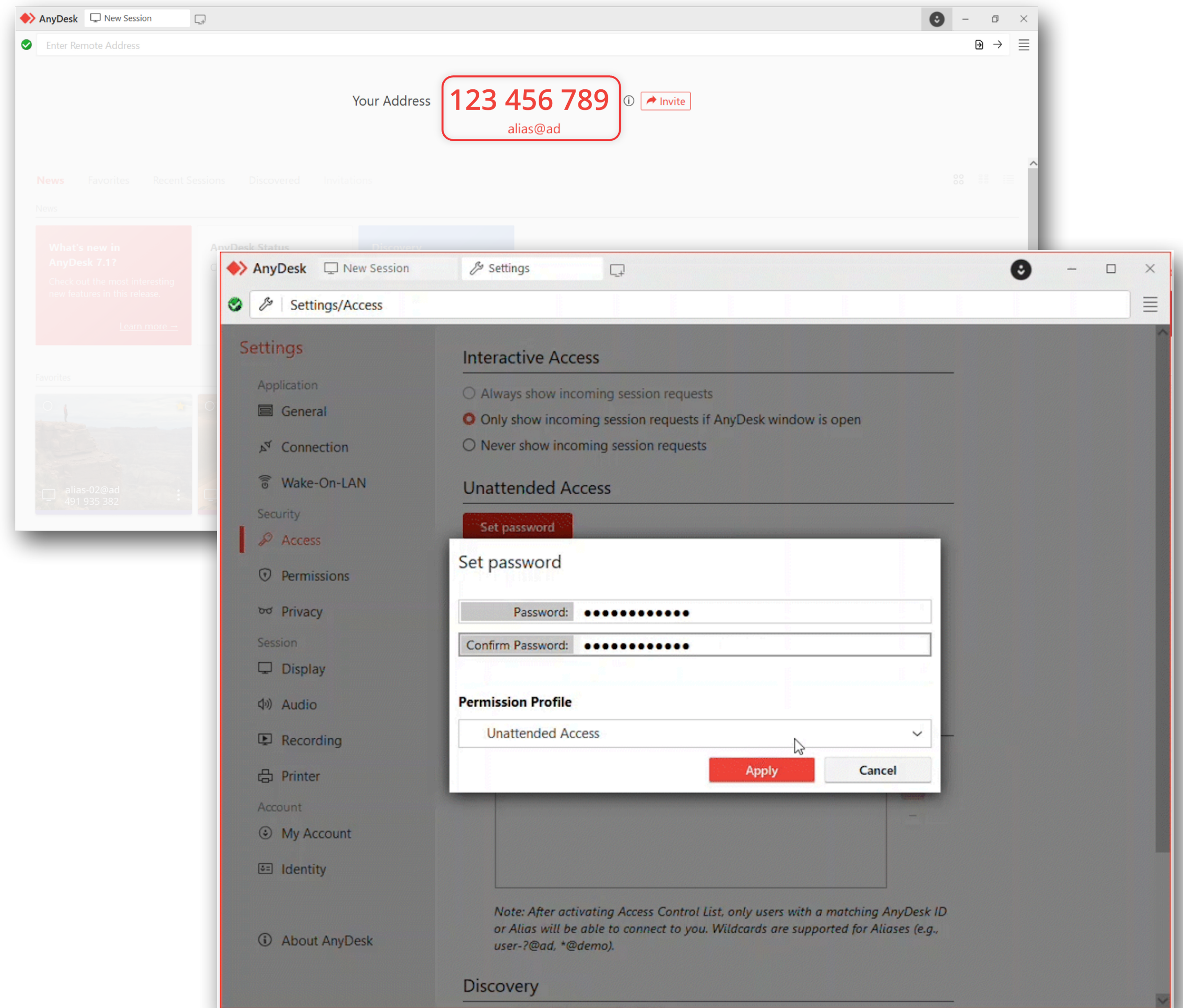
- ▶ Email-Anhänge / Links
 - ▶ Gefälschte Downloads
 - ▶ Unsichere Webseiten: Beim Besuch wird Schadsoftware nachgeladen
 - ▶ Gefälschte Apps
 - ▶ Offene WLANs
- ➔ Oft: Ausnutzung von Sicherheitslücken

Fernwartungssoftware

- ▶ Zugriff über das Internet auf einen entfernten Rechner
 - ▶ volle Kontrolle über den Rechner
 - ▶ Beispiele: TeamViewer, AnyDesk
- ➔ Gerne von Kriminellen benutzt



<https://www.connex.de/pdf/TeamViewer-Manual-Remote-Control-de.pdf>



<https://support.anydesk.com/docs/de/quick-start-guide>

Zum Mitnehmen

Regelmäßige Updates (Betriebssystem und alle Programme)

Software installieren

- ▶ Funktionen der Software googeln
- ▶ Nur von offiziellen App-Stores und Hersteller-Seiten herunterladen
- ▶ Keine Zugangsdaten an Unbekannte für Fernwartungssoftware weitergeben

Zugangsdaten

Wie Zugangsdaten gestohlen werden

- ▶ Am Telefon erfragen
- ▶ Schadsoftware
- ▶ Sicherheitslücken
- ▶ Datenlecks (normalerweise Password-Hashes)

Zugangsdaten erraten

- ▶ Oft benutzte Passwörter
- ▶ Bekannte Daten: Geburtstag, Hochzeitstag, Name des Hundes etc.
- ▶ Passwort-Hashes cracken: Leicht bei kurzen Passwörtern
- ▶ Gleiche Passwörter bei mehreren Konten

TOP 20 privater Passwörter in Deutschland 2024

Pos.	Passwort	Pos.	Passwort
1.	123456	11.	111111
2.	password	12.	123456a
3.	12345	13.	654321
4.	12345678	14.	1q2w3e4r5t
5.	abc123	15.	monkey
6.	123456789	16.	dragon
7.	1234567	17.	ashley
8.	qwerty	18.	princess
9.	iloveyou	19.	q1w2e3r4t5y6
10.	password1	20.	a123456

<https://identeco.de>

<https://www.uni-bonn.de/de/neues/236-2024>

Zum Mitnehmen

Sichere Passwörter

- ▶ Länge > 15
- ▶ Keine offensichtlichen Wörter
- ▶ Keine Wiederverwendung
- ▶ Wechseln bei Sicherheitsvorfällen

2-Faktor-Authentifizierung

Zugangsdaten sind privat!

Passwort-Manager

Alternative zu Passwörtern: Passkeys

Links



Link-Aufbau

<https://www.postbank.de>

<https://banking.postbank.de/#/login>

Link-Tricks

- ▶ Ähnliche Schreibweise
- ▶ Ähnliche Buchstaben (auch aus verschiedenen Zeichensätzen)

<https://srv1.paypal.com.xyz.com/login>

rnicrosoft.com

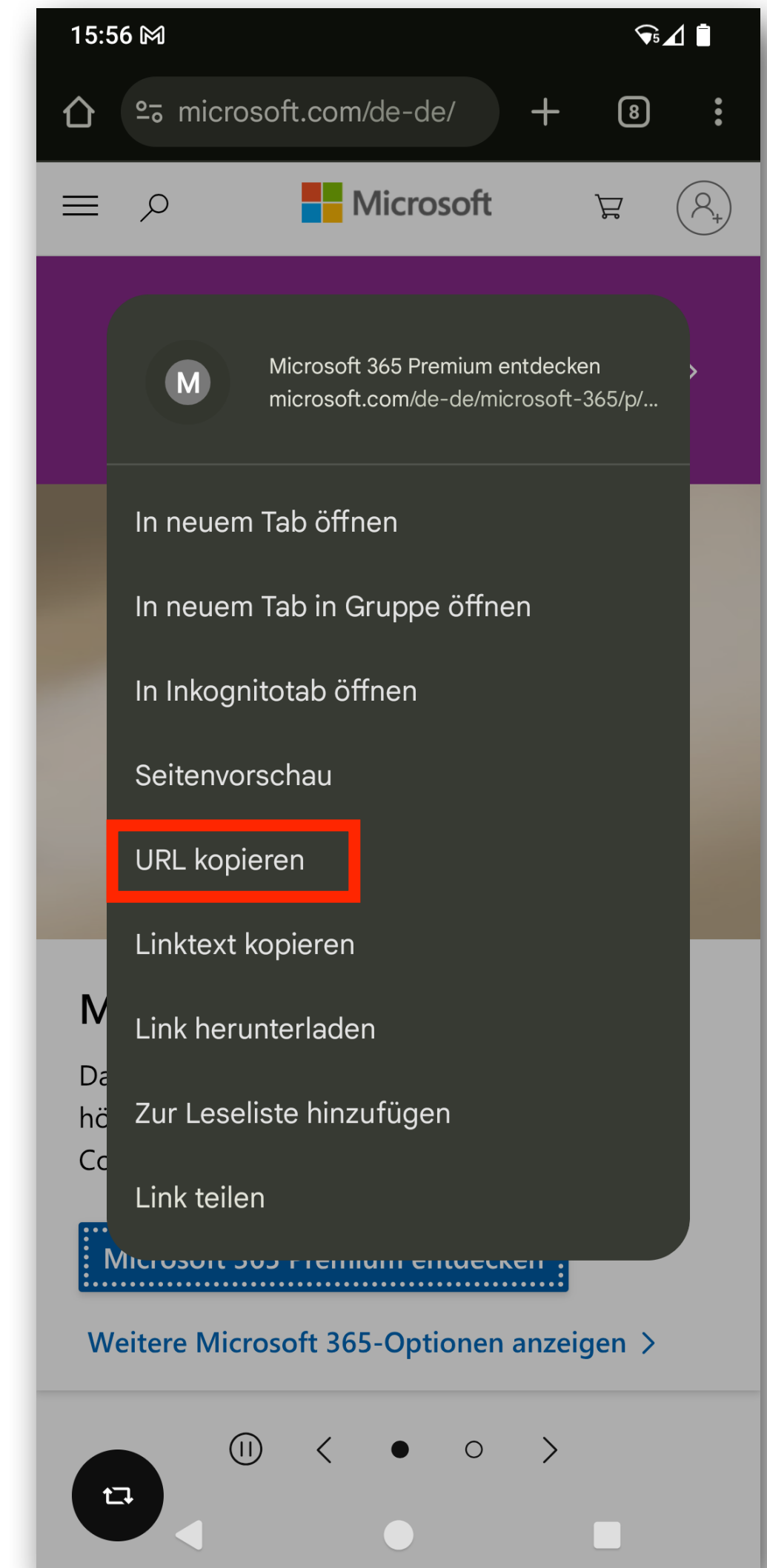
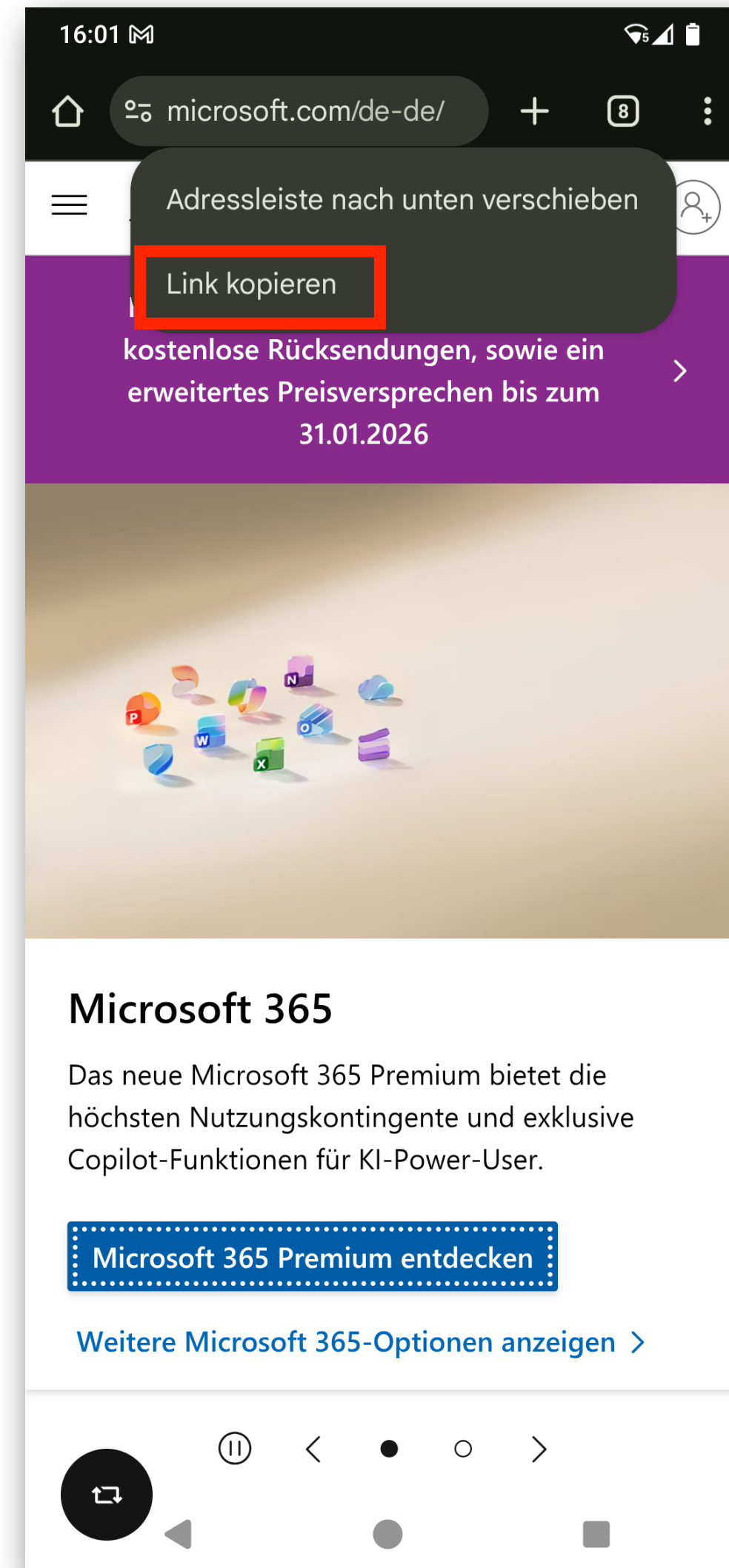
rnicrosoft.com

Links im Browser

The screenshot shows a web browser window with the address bar containing `microsoft.com/de-de/`. The page features a navigation bar with the Microsoft logo and links to Microsoft 365, Teams, Copilot, Windows, Surface, Xbox, and Mehr. A purple banner at the top of the main content area reads: "Kostenloser Versand und verlängerte kostenlose Rücksendungen, sowie ein erweitertes Preisversprechen bis zum 31.01.2026 >". Below this, there is a large image of Microsoft 365 application icons (Word, Excel, PowerPoint, Outlook, OneDrive, Teams, and OneNote). To the right of the image, the heading "Microsoft 365" is displayed, followed by the text: "Das neue Microsoft 365 Premium bietet die höchsten Nutzungskontingente und exklusive Copilot-Funktionen für KI-Power-User." Below this text is a blue button labeled "Microsoft 365 Premium entdecken" and a link "Weitere Microsoft 365-Optionen anzeigen >". At the bottom of the browser window, the address bar shows the full URL: `https://www.microsoft.com/de-de/microsoft-365/p/microsoft-365-premium/cfq7ttc11z3q?icid=mscom_marcom_H1a_M365Premium`.

Links auf dem Handy

- ▶ Kontext-Menü durch langes Drücken
- ▶ Link kopieren / URL kopieren
- ▶ In einer App mit Text einfügen



Phishing

- ▶ Stehlen von vertraulichen Daten wie Passwörter, Kreditkarten, Personalausweiskopien
- ▶ Durch gefälschte E-Mails, Webseiten oder Nachrichten

Betreff: Zuverlässigkeitsproblem beim Konto



PayPal-Support-Desk <58814587@wsm.net>

an PayPal-Support-Desk ▼

(vor 0 Minuten)

Wichtige Sicherheitsüberprüfung notwendig

Grund der Maßnahme: Neue Anmeldung festgestellt. [Details zur Bedrohung]|Zum Schutz Ihres Kontos wurden einige Funktionen vorübergehend deaktiviert.}

3. Befolgen Sie die Sicherheitscenter-Richtlinien

Was passiert während der Verifizierung?:

- Geld überweisen oder erhalten
- Beträge von Ihrem Bankkonto abheben
- Kontoinformationen ändern
- Mit PayPal bezahlen

Identität bestätigen

Falls Sie Fragen haben, wenden Sie sich an unseren Kundenservice.

Mit freundlichen Grüßen,

app.getsendmail.com/p/.../QDJtLm1hOFBiV296U2E=



E-Mail-Adresse oder Handynummer

bildlicherreicherlemming@holio.day

[E-Mail-Adresse vergessen?](#)

Weiter

oder

Neu anmelden

· **Deutsch** · English · Français · Italiano · Nederlands



bildlicherreicherlemming@holio.day

[Ändern](#)

Passwort

|

[Passwort vergessen?](#)

Einloggen

oder

Neu anmelden

· **Deutsch** · English · Français · Italiano · Nederlands



Sicherheitscode eingeben

Wir haben einen Code an Ihre registrierte Methode gesendet, um Ihre Identität zu bestätigen.

4 5 2 4 7 8|

[Neuen Code senden](#)

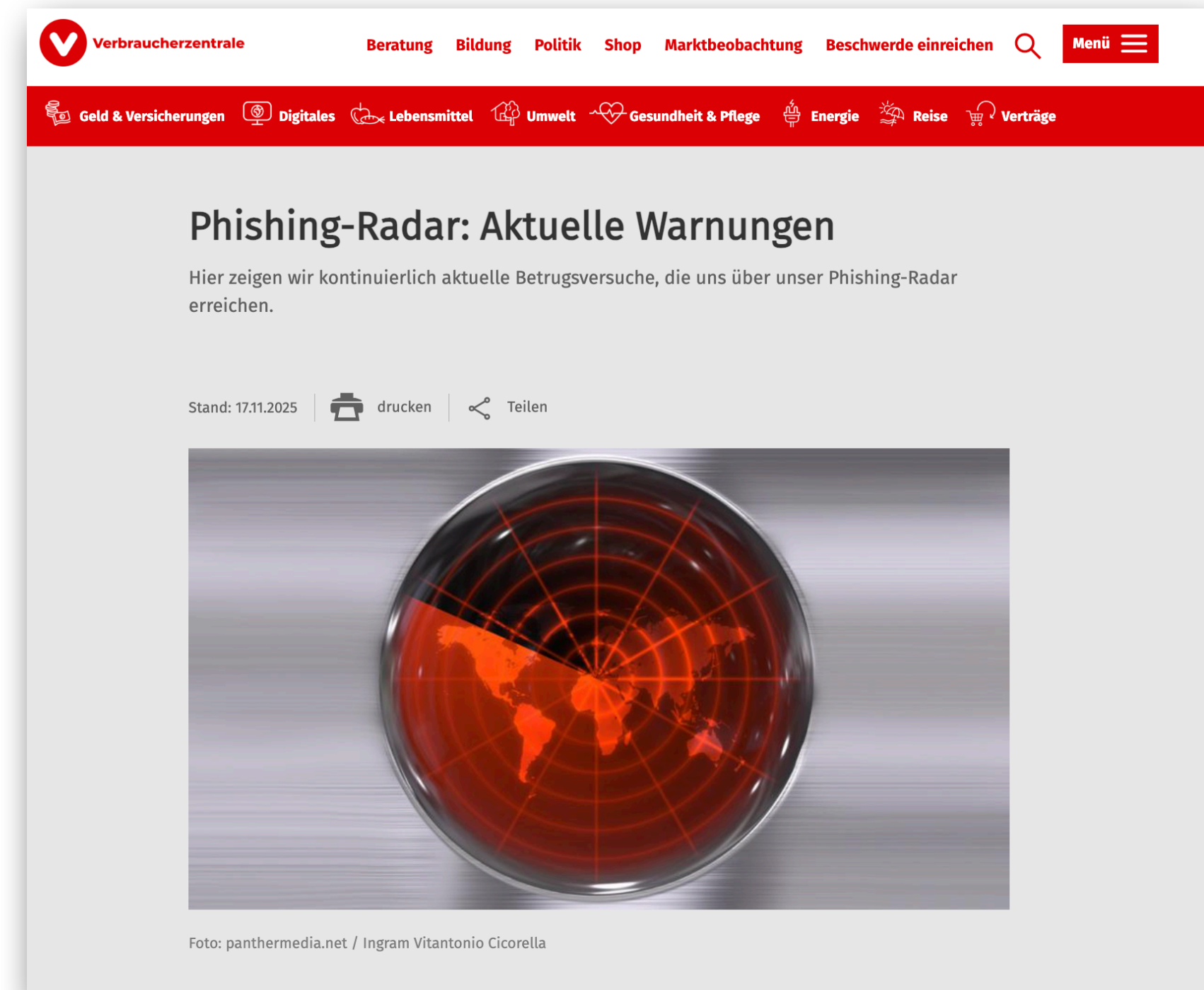
Dieses Gerät für zukünftige Logins merken.

Weiter

[Andere Option versuchen](#)

Zum Mitnehmen

- ▶ Links überprüfen
- ▶ Verdächtige Links nicht öffnen
- ▶ Löschen / als Spam kennzeichnen / Blockieren
- ▶ Links selbst eingeben
- ▶ Verbraucherzentrale: Phishing-Radar



<https://www.verbraucherzentrale.de/wissen/digitale-welt/phishingradar/phishingradar-aktuelle-warnungen-6059>

Datenmißbrauch



Nützlich für weiteren Betrug

- ▶ Anmeldedaten (Passwort, PIN) —> Einloggen im Bank-Account
- ▶ Kreditkarten —> Waren kaufen
- ▶ Kopie vom Personalausweis —> Verträge auf Ihren Namen abschließen
- ▶ Telefonnummern —> Telefonbetrug
- ▶ Email-Adresse —> Spam, Konten hacken durch Passwort-Raten
- ▶ Urlaubsbilder auf Social Media —> man ist nicht zu Hause (Diebstahl)
- ▶ persönliche Details: Name, Geburtstag, Hobbies, Stromanbieter, Bank etc. —> personalisierte Nachrichten und Telefonate
- ▶ Fotos können den Aufenthaltsort verraten



<https://challenge.bellingcat.com/>

Zum Mitnehmen

- ▶ Datensparsamkeit
- ▶ Social Media: Sichtbarkeit einschränken (Sicherheit & Datenschutz / Privacy Settings)
- ▶ Personalausweiskopie
 - ▶ Unnötige Daten schwärzen
 - ▶ Zweck vermerken
 - ▶ Sichere Übermittlung (verschlüsselte Datei, Papier)

Kaufen & Verkaufen



Fake Shops

- ▶ Häufig nicht auf den ersten Blick zu erkennen
- ▶ Indizien
 - ▶ deutlich günstiger als anderswo
 - ▶ Keine oder falsche Informationen: Impressum, Handelsregistereintrag, Umsatzsteuer-ID, Datenschutzerklärung, Widerrufsbelehrungen, Versandbedingungen
 - ▶ Adresse stimmt nicht mit Google Maps überein
- ▶ Gefälschte Gütesiegel
- ▶ Kontaktmöglichkeiten eingeschränkt: z.B. nur Mobiltelefon oder Kontaktformular
- ▶ Unsichere Zahlung: Vorkasse, Paypal "Freude & Familie" ohne Käuferschutz

Privat Kaufen & Verkaufen

- ▶ Plattformen wie kleinanzeigen.de, quoka.de
- ▶ Funktionen der Plattformen
 - ▶ Chat / Sichere Kommunikation mit Datenschutz
 - ▶ Sicher bezahlen / Sichere Kaufabwicklung
 - ▶ Betrugserkennung
- ➔ Kriminelle versuchen, die Kunden von der Plattform wegzulocken

Zum Mitnehmen

- ▶ Preisvergleichsportale: Geizhals, Idealo
- ▶ Handelsregister
- ▶ Verbraucherzentrale: Fakeshop-Finder
- ▶ Gütesiegel: Trusted Shops, EHI Retail Institute, Trustpilot
- ▶ Sichere Bezahlmethoden
- ▶ Funktionen der Plattformen nutzen: Chat, Bezahlen

TRUSTED SHOPS Services ▾ Warum Trusted Shops? ▾ **Für Unternehmen** Login ▾

Gemeinsam sind wir #trstd

Wo echte Shops auf echte Shopper treffen – mit Vertrauen

Finde vertrauenswürdige Shops

45 Mio. Shopper **32.000** Shops **1 Mio. pro Tag** Transaktionen

<https://www.trustedshops.de/>

Anlagebetrug



Erstattungsbetrug / Recovery Scam

- ▶ Kontaktaufnahme: Anwalt, Opfervertreter, Agentur, Behörde etc.
- ▶ Kenntnis über den Betrugsfall
- ▶ Vorkasse:
 - ▶ Bearbeitungsgebühr
 - ▶ Aktivierungstransaktion
- ▶ Keine Auszahlung

Sehr geehrter Herr [REDACTED]

vielen Dank für Ihre Rückmeldung. Gern beantworte ich Ihre Fragen der Reihe nach:

1. Ich vertrete ein Vermittlungsunternehmen, das sich auf Rückforderungen von Investitionen sowie auf Chargeback-Prozesse spezialisiert hat. Im Anhang finden Sie die Registrierungsurkunde unseres Unternehmens.
2. Die Betrüger haben unter verschiedenen Namen operiert – einer davon war beispielsweise „InfinityFX“.
3. Sobald Sie bereit sind, die Aktivierungstransaktion durchzuführen, erhalten Sie von uns die Zahlungsdaten unseres Steuerbeauftragten, der Teil unseres Teams ist.

Zum Mitnehmen

Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin)

- ▶ Unternehmensdatenbank
- ▶ Warnungen

The screenshot shows the search interface of the BaFin Unternehmensdatenbank. At the top left is the BaFin logo and the text 'Bundesanstalt für Finanzdienstleistungsaufsicht'. Below this is a search box with the label 'Suche' and 'Stand der Daten: 16.11.2025'. The search criteria include: 'Unternehmen:' (text input), 'BaFin-ID:' (text input), 'Bak Nr.:' (text input), 'Reg Nr.:' (text input), and 'Kategorie:' (dropdown menu). A 'Suche' button is located below the criteria. At the bottom left, there is a navigation menu with letters A-Z and 'Sonstige'.

The screenshot shows a warning article on the BaFin website. The header includes the BaFin logo and the text 'Bundesanstalt für Finanzdienstleistungsaufsicht'. A search bar is located at the top right. The main navigation menu includes 'Unternehmen', 'Verbraucher', 'Internationales', 'Recht & Regelungen', 'Publikationen & Daten', and 'Die BaFin'. The breadcrumb trail is 'Verbraucher > Warnungen & Aktuelles > BaFin warnt vor nahezu identischen Websites'. The article title is 'BaFin warnt vor nahezu identischen Websites' and the date is '30.05.2025'. The article text states: 'Die Finanzaufsicht BaFin warnt vor einer Reihe nahezu identischer Websites. Nach ihren Erkenntnissen bieten die Betreiber dort ohne Erlaubnis Finanz- und Wertpapierdienstleistungen an.' The article also mentions that the presentation on these websites begins with the sentence: 'Verdient Ihr Vertrauen Geringe Spreads Plattform - [Name der Plattform] Bieten Sie Ihren Kunden eine breite Palette von CFD-Handelsprodukten wie Devisen, Metalle und Rohstoffe, Aktienindizes usw.'. The article is dated 30.05.2025 and has the theme 'Unerlaubte Geschäfte, Verbraucherschutz'.

<https://www.bafin.de/>

Wenn's passiert
ist



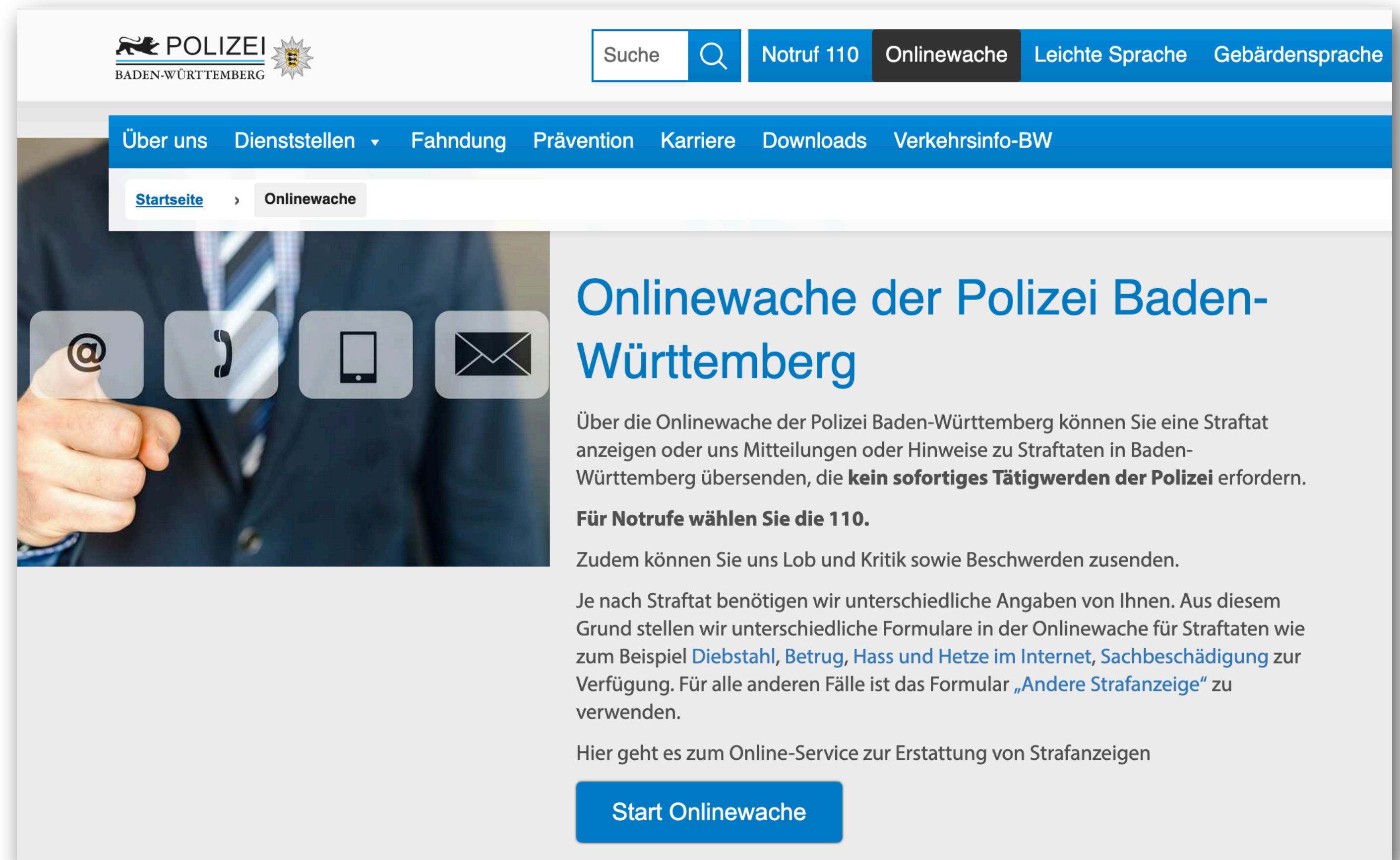
Allgemein

Täter aussperren

- ▶ Passwörter ändern
- ▶ AnyDesk u.Ä. deinstallieren
- ▶ Benutzer blockieren
- ▶ Konten sperren

Polizei

- ▶ Akute Gefahr: 110
- ▶ örtliche Polizeidienststelle
- ▶ Onlinewache



The screenshot shows the website for the Baden-Württemberg Police's online reporting service. At the top left is the logo 'POLIZEI BADEN-WÜRTTEMBERG'. To the right is a search bar and navigation links for 'Notruf 110', 'Onlinewache', 'Leichte Sprache', and 'Gebärdensprache'. Below this is a main navigation menu with links for 'Über uns', 'Dienststellen', 'Fahndung', 'Prävention', 'Karriere', 'Downloads', and 'Verkehrsinform-BW'. A breadcrumb trail shows 'Startseite' and 'Onlinewache'. The main content area features a large image of a police officer's hand pointing, with icons for email, phone, mobile, and envelope. The heading reads 'Onlinewache der Polizei Baden-Württemberg'. The text explains that users can report crimes or provide tips, but notes that some cases require immediate police action. It lists examples of crimes like theft, fraud, and internet harassment. A prominent blue button at the bottom says 'Start Onlinewache'.

<https://www.polizei-bw.de/onlinewache/>

Warum zur Polizei?

Konkrete Straftaten

- ▶ Ermittlungen einleiten
- ▶ Fehlendes Puzzle-Stück in einem Verfahren
- ▶ Kenntnis über aktuelle Maschen → gezielt reagieren

Selbstschutz

- ▶ Mißbrauch von persönlichen Daten
- ▶ Verstrickung in Geldwäsche

Beweismaterial

- ▶ Anzeige zeitnah erstatten
- ▶ Beweismaterial (Emails, Chats, Fotos ...) nicht verändern
- ▶ Technisch versierte Nutzer: speichern, ausdrucken, Screenshots etc.
- ▶ Details notieren

Betroffene

- ▶ Der Täter trägt die Schuld
- ▶ Jeder kann Opfer werden
- ▶ Scham überwinden
- ▶ Unterstützung durch das Umfeld
- ▶ Hilfe holen
 - ▶ Telefonseelsorge
 - ▶ Hilfsorganisationen, z.B. Weiße Ring e.V.

Fragen?

