

# **Sicher im Netz 2026**

## **Ein Überblick zu den Risiken ... und einige Lösungen**

**Arne Dörnenburg  
Müden am 17.03.2026**

# Das TEBO Ehrenamts-Projekt

- Wer/Wie/Was: seit 2022, Ausbildung durch KVHS, ca. 30 TEBO
- Angebot: Vorträge + Kurse, siehe: TeboWeb. Ggf. Hausbesuche
- Internetseite: <https://www.tebo-gifhorn.de>
- Finanzierung: Fördermittelgeber, Spenden

Förderung durch:



+

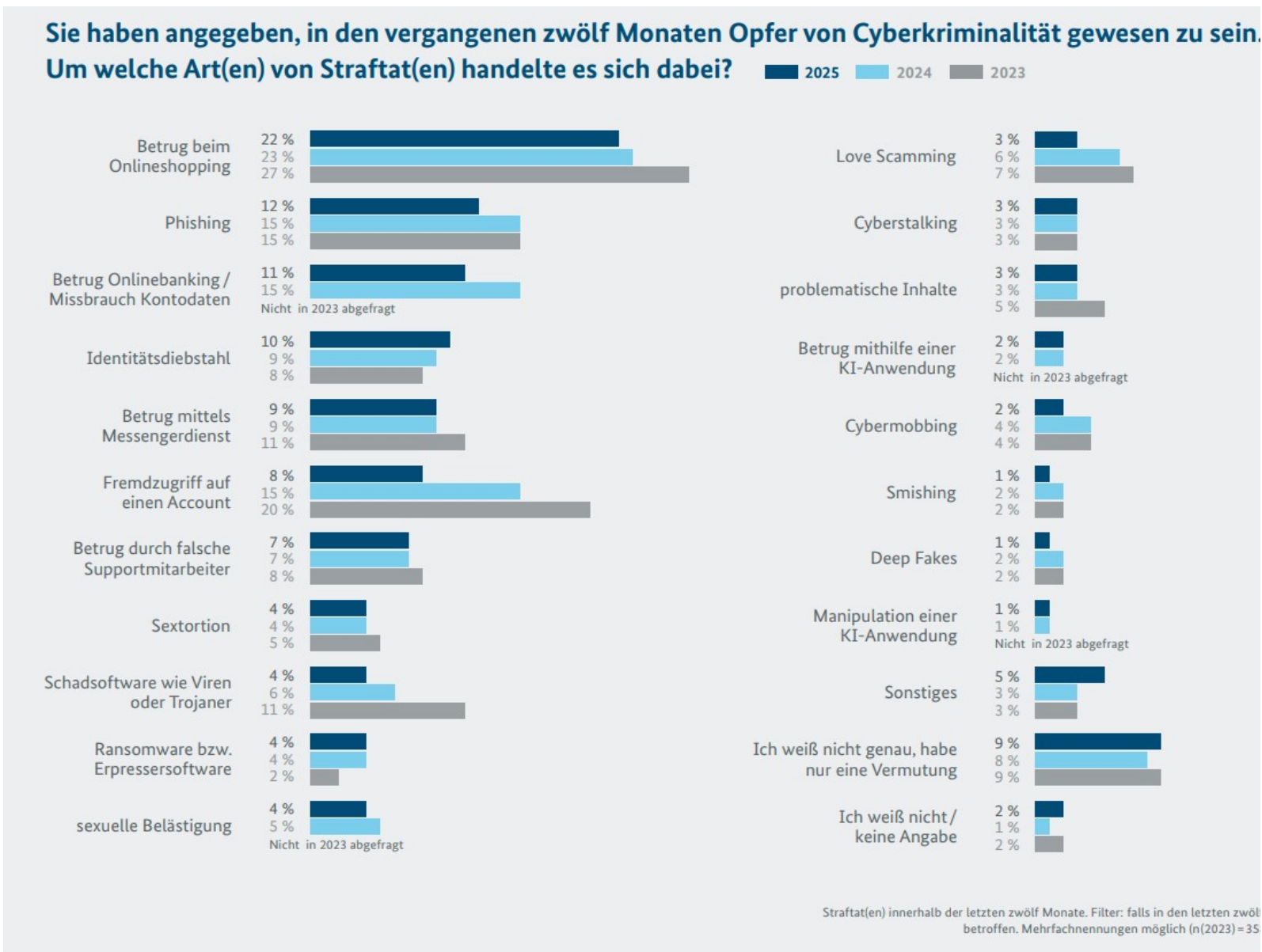


## Zusammenarbeit mit:

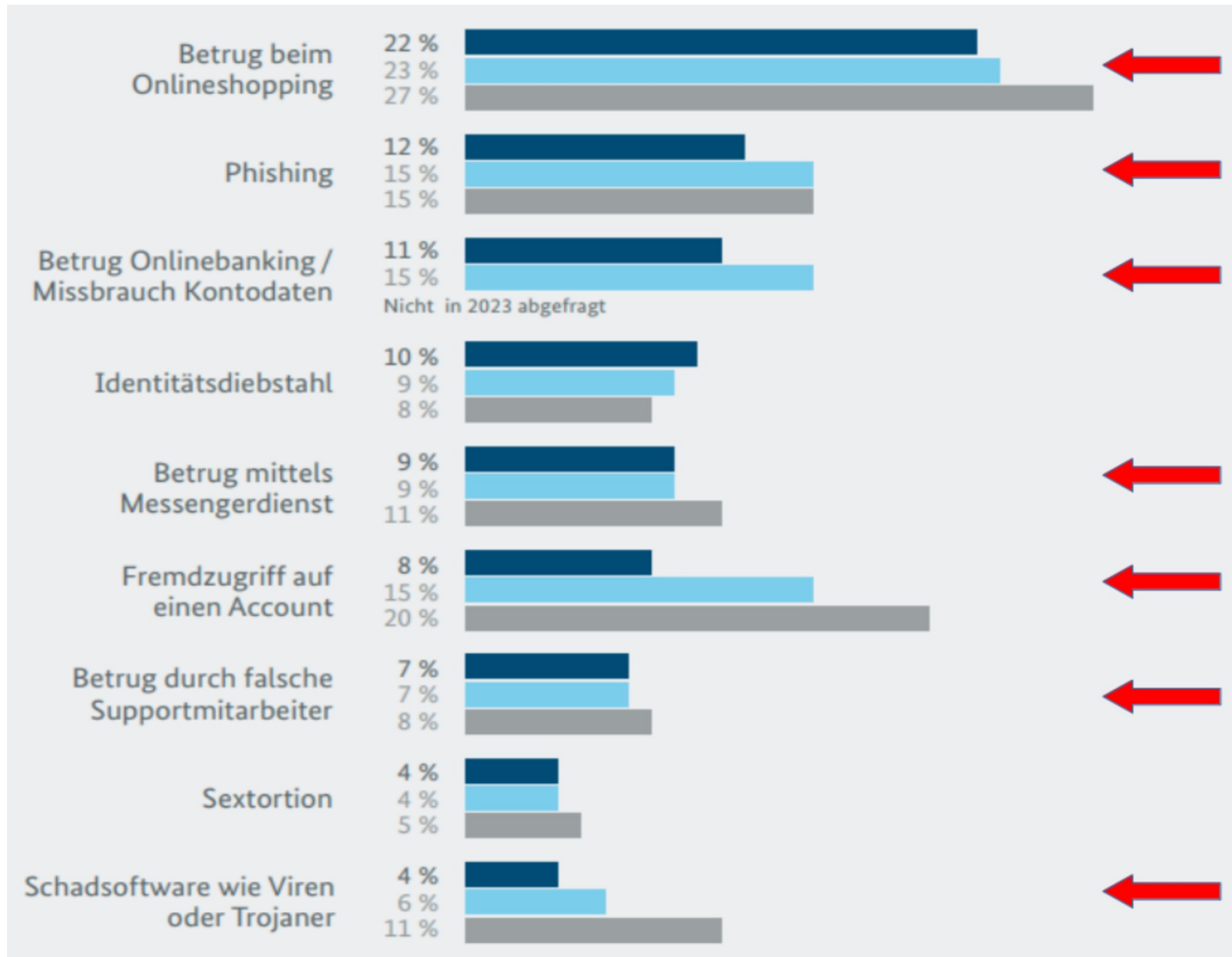


KREISSENIORENBEIRAT  
LANDKREIS GIFHORN

# Woher kommen die Bedrohungen?



# Woher kommen die Bedrohungen?



Quelle: [www.bsi.bund.de](http://www.bsi.bund.de)

# Unsere Themen

- Warum wir betroffen sind ...
- Betrug per Telefon
- Betrug per Mail, SMS, QR, Zeitschriften
- Betrug beim Online-Einkauf: Fake-Shops, Bezahlverfahren
- Betrug beim Online-Banking
- Smartphone und Schutz
- Passworte, 2-Faktor-Authentifizierung (2FA)
- Schadsoftware, Virenschutz
- Praktische Handlungstipps

# Warum (auch) ältere Menschen betroffen sind

- Viele Menschen über 60 sind mit Werten wie Höflichkeit, Hilfsbereitschaft und Vertrauen gegenüber Autoritäten aufgewachsen
- Genau diese Eigenschaften werden von Betrügern ausgenutzt
  - Zeitdruck erzeugen („Sie müssen sofort handeln“)
  - Auslösen von Angst („Ihr Konto ist in Gefahr“)
  - Vorspiegeln von Autorität („Hier spricht die Polizei“)
  - Aufbau von Vertrauen („Ich helfe Ihnen doch nur“)
- Was kann ich tun?
  - **Wichtig:** Selbstschutz ist keine Unhöflichkeit
  - Ich darf misstrauisch sein
  - Ich darf jederzeit auflegen oder um Bedenkzeit bitten

# **Betrug durch Täuschung**

**„Früher stand der Trickbetrüger vor der Haustür.**

**Heute sitzt er irgendwo auf der Welt  
– aber klingelt digital.“**

# **Betrug durch Täuschung**

**„Früher stand der Trickbetrüger vor der Haustür.**

**Heute sitzt er irgendwo auf der Welt  
– aber klingelt digital.“**

**ChatGPT 5.2**

# Betrug durch Täuschung (Scam)

- Bekannt: Enkeltrick (WhatsApp / Neue Nummer / dringend überweisen)
- Microsoft Support ruft an
- Telefon: “angeblicher Mitarbeiter“ (Bank, Polizei, Behörde)
- Schockanrufe oder „Polizeianruf“
- Erpressung (intime Bilder) ► Nicht antworten/Passwort ändern
  
- **Was kann ich tun?**
  - **Bitte unbedingt auflegen, Kontakt abbrechen!**
  - „Enkel“ ► **Bisherige** Nr. **an**rufen, **nicht** zurückrufen, **nicht** überweisen
  - Nie Konto- oder Zugangsdaten (Online/Offline) preisgeben!
  - **Nie** Geld an Fremde senden
  - Banken bitten nie am Telefon um persönliche Daten/PIN/Passwort
  - Polizeibeamte fordern nie auf, Bargeld/Schmuck herauszugeben

# KI gestützte Betrugsformen [NEU]

- Sogenanntes „Identitäts-Deepfake“
  - Stimmen-/Video-Imitation
  - Perfekte Texte durch KI
  
- Was kann ich tun?
- **Wie beim „normalen“ Telefonbetrug**
  - Unbedingt auflegen
  - Auf **anderem Weg** beim angeblichen Anrufer sofort rückfragen

**Betrug per** 

# Betrug per Mail

**DKB**

Aktion erforderlich: Bitte aktualisieren Sie Ihre

Anmeldeinformationen

Sehr geehrte Kunde,

Mit dieser Mitteilung teilen wir Ihnen mit, dass Ihr Online-Banking-Profil aus Sicherheitsgründen deaktiviert wurde.

Die neuen Regelungen verlangen von Kontoinhabern in regelmäßigen Abständen eine kurze „Bestätigung“ ihrer aktuellen Angaben als Maßnahme gegen unbefugte „Kontonutzung“ und „Geldwäsche“.

Um unsere Dienste weiterhin wie gewohnt nutzen zu können und eine drohende Schließung Ihres Kontos und Ihrer Karte zu vermeiden, tun Sie dies bitte umgehend.

[Konto Aktualisieren >](#)

**Wichtig:** Wenn Sie diese E-Mail ignorieren, haben Sie nur eingeschränkten Zugriff auf Funktionen.

Mit freundlichen Grüßen,  
**Ihre DKB**

# Betrug per Mail



[Zur Online-Version](#)

**Sehr geehrter Kunde,**

Um der betrügerischen Verwendung von Bankkarten im Internet entgegenzuwirken, verfügt die **Deutsche Kreditbank AG** über ein neues Zahlungskontrollsystem. Dieser Service ist völlig kostenlos.

Unser System hat festgestellt, dass Sie Ihren "TAN2go". - Dienst reaktivieren müssen. Klicken Sie auf den sicheren Link, um Ihren Dienst wieder zu aktivieren :

[Reaktivierung starten](#)

Viele Grüße  
**deine DKB**

Sehr geehrter Kunde,  
die Aktualisierung der DKB-APP steht aus bitte nachholen:  
<https://dkb-sicherheit.com/?tkn=b69a>



Auch: [www.commerzbank.de](http://www.commerzbank.de)

# Betrug per Mail

Verfassen: Re: Glückwunsch (no-reply) Sichern Sie sich Ihr kostenloses Erste-Hilfe-Set für Techn... — □ ×

Datei Bearbeiten Ansicht Einfügen Format Optionen Sicherheit Extras Hilfe

S... Verschl... O... R... S... A... Car... Thunder...

Von • **Schij Psejdnf.ksjdhf.sjdfn kfkxmj.sjfk** | Kopie (CC) Blindkopie (BCC) >>

An **Techniker Krankenkasse© <Noreply-ktrQQGeX@ktrQQGeXktrQQGeX.ca>**

Betreff **Re: Glückwunsch ( doe.arne) Sichern Sie sich Ihr kostenloses Erste-Hilfe-Set für Technik**

Absatz Variable Breite [Rich Text Icons]

Am 03.03.26 um 20:34 schrieb Techniker Krankenkasse©:

**HERZLICHEN GLÜCKWUNSCH**

**Erste-Hilfe-Set [ doe.arne ]**

Sie wurden ausgewählt, ein exklusives Erste-Hilfe-Set – Level 1 zu erhalten. Dies ist Ihre Gelegenheit, Ihre Vorbereitung auf Notfallsituationen mit einem praktischen, vollständigen Kit zu verbessern, das entwickelt wurde, um Ihre Sicherheit und die Ihrer Angehörigen im Alltag zu gewährleisten.

[Meine Belohnung anfordern](#) ←

**Was Ihr Erste-Hilfe-Set Enthält**

Heftpflaster (verschiedene Größen)

Schützen kleine Schnitte und Schürfwunden vor Bakterien und fördern eine schnelle Heilung.

Sterile Kompressen

Deutsch (Deutschland)

Verfassen: Re: N41-- Thunderbird — □ ×

Datei Bearbeiten Ansicht Einfügen Format Optionen Sicherheit Extras Hilfe

S... Verschl... O... R... S... A... Car... Thunder...

Von • **Schij Psejdnf.ksjdhf.sjdfn kfkxmj.sjfk** | Kopie (CC) Blindkopie (BCC) >>

An **WEIKERT DIETMAR <ho.buffett@gmail.com>** ←

Betreff **Re: N41-**

Absatz Variable Breite [Rich Text Icons]

Am 16.02.26 um 22:01 schrieb WEIKERT DIETMAR:

Hallo,

3.250.500 €

**Herzlichen Glückwunsch! Die WEIKERT DIETMAR STIFTUNG hat Ihnen 3.250.500 € gespendet.**

Für weitere Informationen zur Stiftung und zur Auszahlung des Geldes antworten Sie mir bitte, ob die von Ihnen angegebene E-Mail-Adresse gültig ist.

Ich warte auf Ihre Bestätigung, dass diese E-Mail-Adresse gültig ist.

Mit freundlichen Grüßen

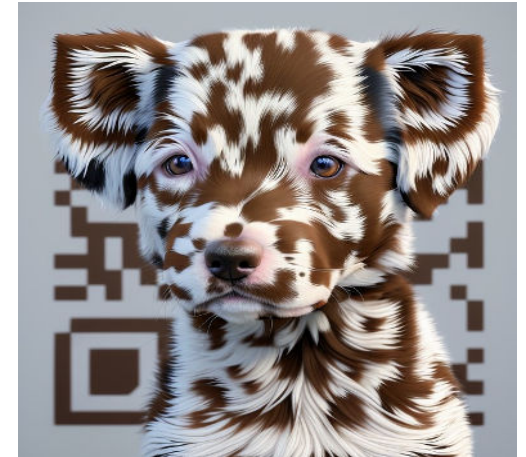
Weikert Dietmar  
Weikert Dietmar Stiftung  
E-Mail: ho.buffett@gmail.com

Hinweis: Sollten Sie diese E-Mail in Ihrem Spam-Ordner finden, liegt dies an Ihrem Internetanbieter. Bitte markieren Sie die E-Mail als „Kein Spam“ oder verschieben Sie sie in Ihren Posteingang, um darauf zu antworten.

Deutsch (Deutschland)

# Phishing, Smishing, Quishing, ...

- Betrugsmaschinen um Daten (TelNr, Adresse, ...) und Geld abzugreifen (Kreditkarte, Pin, Logindaten)
- Begriffe
  - Phishing: E-Mail Betrug
  - SMS-, QR-Code-, Telefon-Betrug
  - Gewinnspiele, Zeitschriften
- Was kann ich tun?
  - Nie Links in Emails/SMS klicken, immer original Seite aufrufen
  - Links prüfen: Leicht verändert? zB: login-dkb.de statt dkb.de (??)
  - **Nie** 2FA-Codes weitergeben
  - **Nie** direkt zahlen, offizielle App/Website prüfen
  - Immer sparsam mit persönlichen Daten
- Training/Info:
  - <https://phishingquiz.withgoogle.com/>
  - [verbraucherzentrale.de](https://www.verbraucherzentrale.de), [phishingradar](https://www.phishingradar.de)



# Online Einkauf

# Online einkaufen

- Fake-Shops: Geld kassieren, ohne Ware zu liefern
- **Veraltet:** fehlendes Impressum/Datenschutzerklärung, keine AGB, nur eine Bezahlmethode, fehlende Gütesiegel
- **Veraltet:** “Gütesiegel geben hier besondere Sicherheit“  
Jein ► (Erklärung...). Die kann ich mir aber auch kopieren
- Professionell wirkende Shops, Lebensdauer oft < 1 Tag
- Extrem günstige Preise, nur Vorkasse, Zeitdruck (andere Interessenten: „jetzt kaufen, sonst weg“)
- Angebliche Insolvenzen / Geschäftsaufgaben
- Was kann ich tun?
- **Frage Dich:** Ist es zu schön um wahr zu sein?
- <https://www.verbraucherzentrale.de/fakeshopfinder>



# Bezahlverfahren im Netz

Rechnung	+ Sicherste Bezahlmethode: ich erhalte und prüfe die Ware, bevor ich bezahle + Widerrufsrecht
Lastschrift, Nachnahme	+ Rückbuchbar, Widerrufsrecht - Kontodaten angeben, Ware nicht prüfbar
Kreditkarte	+ 2FA, viele mit Käuferschutz - alle Daten angeben, Rückabwicklung schwierig
PayPal, GooglePay, ApplePay, Klarna	+ Keine Kontodaten angeben, Käuferschutz (PayPal, Klarna)
WERO	+ Echtzeit, Bank-zu-Bank - Kein Käuferschutz
Vorkasse	- Keine Möglichkeit, Geld zurückzufordern, falls Ware mangelhaft / nicht ankommt - Kein Geld zurück, Ware nicht prüfbar

# Smartphone

# Smartphone

## ▪ Smartphone-Schutz

- **MUSS**: Muster, PIN, Passwort, Biometrie
- Updates

## ▪ **Schadsoftware**

- Nur aus offiziellen Stores laden
- Virenschutz: ja/nein...

## ▪ **Öffentliches WLAN**

- Wenn: Bei WLAN kein Passwort erforderlich ist
- Dann: Keine Bankgeschäfte oder sensible Infos

## ▪ **Vor Spam Anrufen/Nachrichten schützen**

- Drittanbieter-Sperre (Mobilfunkanbieter)
- Spamschutz auf Smartphone aktivieren
- Apps: Truecaller / CleverDialer



# Smartphone

- Im Folgenden „Live-Anpassung“ der Smartphones
  - **Bildschirm-Zugangs-Sperre einrichten**
  - Evtl.: Spamfilter für Nachrichten
  
- Alle, die mit ihrer Bildschirm-Sperre „unglücklich“ sind oder gar keine haben, können jetzt gemeinsam mit uns die Sperre einrichten bzw. anpassen
  
- Unterstützung durch die **TEBOs**

# Smartphone: Zugangs-Sperre einrichten

## Android



- Einstellungen
- Sperrbildschirm
- Art der Sperre (Typ)

## iOS



- Einstellungen
- Face-ID + Code oder
- Touch-ID + Code

# Smartphone: Spamfilter für Nachrichten

## Android

- Öffne die App „Messages“ („Nachrichten“)
- Tippe oben rechts auf das „Kontobild“
- Tippe auf „Messages-Einstellungen“
- Sicherheit und Datenschutz → „Spamschutz“ einschalten

## iOS

- Spamfilter für Nachrichten ist ab iOS 26 standardmäßig aktiv
- Öffne die App „Nachrichten“
- Tippe oben rechts auf „Filter“ → „Filter verwalten“
- Aktiviere oder deaktiviere „Spam filtern“
- Optional: „Unbekannte Absender überprüfen“: Nachrichten filtern

# Passworte

- Passworte = Hausschlüssel, wer den Schlüssel hat, kann rein!

- Häufigste Passworte Deutschland

123456	123456789	565656
12345678	hallo123	kaffeetasse
1234567	passwort	lol123

- Diese Passworte werden in unter einer Sekunde geknackt

- Oft empfohlene Maßnahmen

- Jeder Dienst 1 Passwort
- mindestens 12 Zeichen lang sein
- Groß- und Kleinbuchstaben, Zahlen und Sonderzeichen enthalten
- nicht im Wörterbuch vorkommen
- keine persönliche Informationen enthalten  
(Geburtsdaten, eigene oder Haustier-/Partner-Namen, etc.)



# Passworte

- Das ist für die meisten Menschen **viel** zu kompliziert
- Alternativen:
  - Passwort-Manager. **JA!** Es gibt leider keine für Senioren
  - Passwort im Browser speichern. JEIN: Vor-/Nachteile
  - Zwei-Faktor-Authentifizierung (2FA): Geht noch nicht überall
  - Passkeys: Auch Super! Aber: noch am Anfang...
  - **Nur zuhause:** Zettel. Aber nicht auf dem Schreibtisch
  - Mein Vorschlag: Ein Basispasswort, viele Endungen...
    - AimMk,hwu1gNg:fa22
    - Ih3KudhK,PuL:ac
- Was kann ich tun?
  - **Unbedingt:** Jeder Dienst 1 Passwort
  - **Wo immer möglich:** 2FA
  - Passwortmanager oder Basispasswort+Endung

Als ich meinen Mann kennenlernte, haben wir uns eine ganze Nacht geküsst

Ich habe drei Kinder und die heißen Karl, Paul und Laura (:facebook)

# Maßnahmen / Tipps

# Maßnahmen (Internet)

## ▪ **BITTE**

- Keine Daten an Gewinnspiele
- Keine Daten an Social-Media-Profile
- Keine Personalausweisdaten ohne Not

## ▪ **MERKE**

- Microsoft ruft **NICHT** an (und will auf Deinen Rechner)
- Bankmitarbeiter ruft **NICHT** an (und erfragt Deine Daten)
- Polizei/Behörde ruft **NICHT** an (und erfragt persönliche Daten)
- Mr. BöserBube hat **KEINE** Nacktbilder von Dir!
- Der Dandy vom Online-Date **WIRD** Geld wollen

# Maßnahmen (Telefon)

- Ausländische Telefonnummer? Kenne ich da überhaupt wen?
- Bei unterdrückter Nummer nicht abnehmen oder gar zurückrufen\*
- Dasselbe bei unbekannter Nummer\* ► Guck auf die Nummer!
- **Was kann ich tun?** ...falls ich doch abgenommen habe
  - Sofort auflegen wenn niemand spricht, oder Bandansage
  - Ruf Deinen Menschen unter der **bisherigen** Nummer an, wenn er (angeblich) eine neue hat
  - Wenn Dich jemand am Telefon nach persönlichen Daten fragt, ist es **NICHT** seriös!
  - Nicht „Ja“ antworten auf: Können Sie mich hören/Sind Sie noch dran?
    - Allg. Empfehlung: Ich höre Sie / Ich bin noch dran

# Maßnahmen (Telefon)

- Ausländische Telefonnummer? Kenne ich da überhaupt wen?
- Bei unterdrückter Nummer nicht abnehmen oder gar zurückrufen\*
- Dasselbe bei unbekannter Nummer\* ► Guck auf die Nummer!
- **Was kann ich tun?** ...falls ich doch abgenommen habe
  - Sofort auflegen wenn niemand spricht, oder Bandansage
  - Ruf Deinen Menschen unter der **bisherigen** Nummer an, wenn er (angeblich) eine neue hat
  - Wenn Dich jemand am Telefon nach persönlichen Daten fragt, ist es **NICHT** seriös!
  - Nicht „Ja“ antworten auf: Können Sie mich hören/Sind Sie noch dran?  
► Noch besser: **NEIN!**

# Maßnahmen

- Handle nicht unter Zeitdruck. Wenn Du nervös wirst: LASS ES!
- Dringender Handlungsbedarf ist immer ein Hinweis auf Betrug
- Möglichst wenig Daten über sich preisgeben. **Immer!**
- JEDER Dienst braucht ein EIGENES Passwort
- Vorsicht bei öffentlichem WLAN (kein Schloss/Passwort)
- Zwei-Faktor-Authentifizierung einschalten (2FA)
- Bei unklaren Nachrichten beim Absender nachfragen (2. Weg)
- Gib niemals persönliche Daten oder PIN/Passwort auf unbekanntem Seiten ein

# Maßnahmen

## ▪ FRAGE DICH

- Brauchen die für **diesen Zweck** wirklich all diese Daten von mir?
- Habe **ICH** die Mail/SMS ausgelöst? Nein? Wer dann?
- Wieso will die Bank meine IBAN wissen?
  - ▶ Dreh den Spieß um: „Sagen Sie es mir, ich bestätige dann“
- Wenn man sich unsicher ist oder sich überfordert fühlt:
  - ▶ “Bitte melden Sie sich bei mir schriftlich“
- Ist es zu schön um wahr zu sein?
- Ist ja komisch... Kann das überhaupt sein?
- Wieso bin ich gerade nervös/habe Angst?
  - ▶ Sofort aufhören!

# Maßnahmen

- Vorbeugend lernen / Info
  - Phishingbeispiele: <https://phishingquiz.withgoogle.com/>
  - Phishing-Radar: [verbraucherzentrale.de](https://www.verbraucherzentrale.de), [phishingradar](https://www.phishingradar.de)
  - Identitätsdaten ausspioniert? <https://sec.hpi.de/ilc/search>
  - TEBO: <https://tebo-gifhorn.de/>
  
- Checklisten
  - Email/SMS
    - Öffne keine Links oder Anhänge in Emails, sondern immer App bzw. bekannte Webseite
  - Bezahlvorgang
    - Nutze am besten Rechnung
    - Nie 2FA-Codes weitergeben
  - „Oma, ich brauche Geld...“
    - Auf bisheriger Nummer anrufen, **nicht** zurückrufen
    - Kein Geld überweisen

# Wenn es doch passiert: Notfall

- Notfallplan (Bank)
  - Bank sofort anrufen
  - Karte sperren (+49 116 116)
  - Anzeige erstatten
  - Nicht schämen
  
- Notfallplan (Telefon)
  - Das Wichtigste: **Bleib ruhig, denk nach!**
  - Es geht nicht um Sekunden!
  - Kann das überhaupt sein?
  - Hat mir vielleicht jemand nur Angst gemacht?

# Wenn es doch passiert: Wer kann helfen?

- Doch auf den Link geklickt? Doch schon eingeloggt?  
Mache Screenshots, dokumentiere alles
- Erstattete Anzeige bei Polizeien/Onlinewachen der  
Länder oder örtliche Polizeidienststelle  
<https://www.polizei.de/>
- Quellen:
  - <https://www.bka.de>
  - <https://www.bsi.bund.de>
  - <https://www.polizei-beratung.de>
  - <https://www.verbraucherzentrale.de>

# Ende

- Vielen Dank für ihr Interesse
  
- Einer geht noch: Wer kriegt das noch zusammen?
  - AimMk,hwu1gNg
  - Ih3KudhK,PuL
  
- Weitere Vorträge / Kurse unter  
<https://www.tebo-gifhorn.de>
  
- Letzte Erinnerung: Im Falle das, ...

Bleib ruhig, denk nach!

In Zusammenarbeit mit den  
Seniorenbeiräten  
im Landkreis Gifhorn

# Wir brauchen mehr TEBOs



Internetseite: <https://www.tebo-gifhorn.de>




**Werden Sie ehrenamtliche/r Technikbotschafter/in**

Unterstützen Sie SeniorenInnen im Umgang mit Smartphone, Tablet und Co.

In Kooperation mit  
**TEBO** | Landkreis Gifhorn

*Helfen macht glücklich.*



**Sie erreichen uns**

Montag – Mittwoch  
08:30–12:30 Uhr


Donnerstag  
10:00–12:30 Uhr

Freitag  
08:30–12:30 Uhr

**Interessiert? Rufen Sie uns an:  
Telefon 05371 3453 609**

Ansprechpartner: Ralf Überheim  
E-Mail: [r.uberheim@kvhs-gifhorn.de](mailto:r.uberheim@kvhs-gifhorn.de)  
Internet: [www.kvhs-gifhorn.de](http://www.kvhs-gifhorn.de)

Geschäftsstelle KVHS  
Freiheit-vom-Stein-Straße 24  
38518 Gifhorn



**Sie sind gerne mit älteren Menschen zusammen und haben Lust auf ein interessantes Ehrenamt?**

SeniorenInnen haben oft Angst vor den neuen Technologien und tun sich entsprechend schwer im Umgang mit Smartphones, Tablets und Co.


Sie könnten als zertifizierte/r ehrenamtliche/r Technikbotschafter/in für unsere SeniorenInnen im Landkreis Gifhorn eine wunderbare Unterstützung sein. Denn mit Ihrem Wissen können Sie ängstlichen, jedoch interessierten SeniorenInnen den Einstieg in die Welt der digitalen Medien bieten.

\*\*\* Wir bilden auch Pflegekräfte zu zertifizierten „Tebos“ in der KVHS Gifhorn aus. \*\*\*

**Technik verbindet und bereitet Freude.**

**Helfen Sie bei der Kommunikation:**  
Senden und Empfangen von E-Mails, Videochat mit Freunden und Verwandten ...

**Helfen Sie bei der Informationssuche:**  
Waren-, Reise- und andere Dienstleistungen, Gesundheitsthemen, Nachrichten ...



Ziel ist es, das selbstbestimmte Leben älterer Menschen im Landkreis Gifhorn zu unterstützen. Ihnen insbesondere den Kontakt mit Familie und Freunden digital zu ermöglichen, ist für uns eine Herzensangelegenheit.

**Als „Tebo“ helfen Sie dabei, digitale Medien gezielt einzusetzen.**

Unsere zukünftigen TechnikbotschafterInnen „Tebos“ werden in der KVHS Gifhorn ausgebildet und zertifiziert, so dass sie auf persönliche Wünsche und Anforderungen älterer Menschen mit viel Ruhe gezielt eingehen können.

**ENDE**