

Unterwegs im Internet

...

aber sicher!

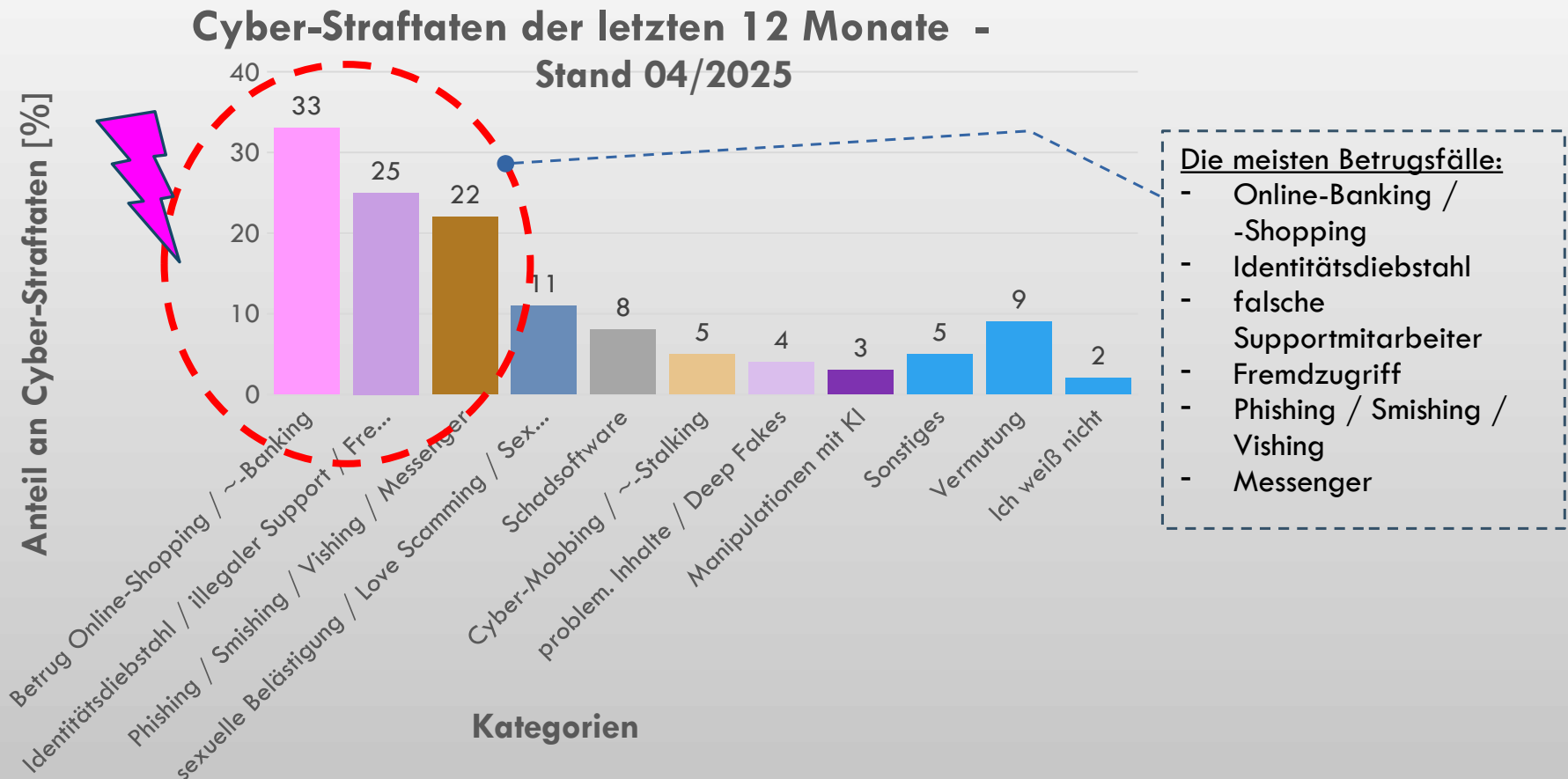
Sicher surfen,
smart schützen –
Ihr digitaler Wegweiser

Herzlich willkommen!

Bildquelle: KI MS-Copilot Designer 30.06.2024
Prompt: „Cybercrime: digital, kreativ, virtuell“

Unterwegs im Internet ... aber sicher!

1. Allgemeines – Anteile typischer Cyber-Straftaten



Mehrfachnennungen möglich! N(Studie 2025)=226

Quelle: [Cybersicherheitsmonitor 2025 - Bürgerbefragung zur Cyber-Sicherheit April 2025](#)

Unterwegs im Internet ... aber sicher!

Sicher surfen, smart schützen!

4. Unterwegs im digitalen Raum

- Umgang mit sozialen Netzwerken / Messengern
- Sicher im Internet bezahlen
- Betrug durch Phishing, Smishing, Vishing, Quishing
- Identitätsdiebstahl
- Opfer krimineller Aktivitäten? Was tun?

Unterwegs im Internet ... aber sicher!

4.

Sicher im Internet bezahlen!

1. Hinweise zu seriösen Online-Shops:

- gutes Web-Layout mit passenden AGBs sind kein ausreichendes Kriterium!
- Überprüfung des Impressums: vollständige Angabe der Kontaktdaten inklusive Adresse und Telefonnummer
- Lesen der Erfahrungsberichte von anderen Usern v.a. auch auf anderen Plattformen
- Online-Shop nur mit Verschlüsselung (https://) nutzen!

Weitere
Informationen
[Finanztipp](#)

Unterwegs im Internet ... aber sicher!

4.

Sicher im Internet bezahlen!

2. Wie kann man im Internet bezahlen?

- Rechnung – am sichersten
- Nachnahme – erhöhte Kosten / unsicher
- Bankeinzug – Rückbuchung 8 Wochen lang möglich!
- Vorkasse – überhaupt nicht zu empfehlen!
- Ratenkauf – evtl. erhöhte Kosten
- Kreditkarte – weltweiter Einkauf ggf. mit Zusatzkosten / Rückbuchung möglich

Weitere
Informationen
[Finanztipp](#)

Unterwegs im Internet ... aber sicher!

4.

Sicher im Internet bezahlen!

3. Bezahldienste über Drittanbieter:

- Paypal – Hinweis: niemals über „Freunde und Familie“ bezahlen; besser „Geld senden für Waren und Dienstleistungen“
- Giropay (Einstellung Ende 2024!)
- Sofortüberweisung
- Klarna
- Amazon Pay
- Gutscheinkarten – keine Bankverbindung erforderlich
- Ratenkauf über Sezzle oder Afterpay

4. weitere Hinweise:

- regelmäßige Kontrolle der Abbuchungen
- ggf. Löschen des eigenen Shop-Zugangs
- ggf. Sperrung Kreditkarte

Weitere Informationen
[Finanztipp](#)

Unterwegs im Internet ... aber sicher!

4.

Hackerangriffe – Was ist das? Wie geht das?

Wie kommen Hacker an fremde Daten? – Teil I

- Angriff per Social-Engineering, z.B. Enkeltrick
- klassische Manipulationstricks per Phishing / Smishing / Vishing / Quishing durch gefälschte E-Mails, Websites, SMS, Anrufe / falsche QR-Codes
- Man-in-the-Middle-Attacke in offenen Hotspots
- Brute-Force-Attacke – Ausprobieren von Passwörtern



Unterwegs im Internet ... aber sicher!

4.

Hackerangriffe – Was ist das? Wie geht das?

Wie kommen Hacker an fremde Daten? – Teil II

- Drive-by-Downloads – *unbeabsichtigtes Laden* von Schadsoftware z.B. von gefälschten Websites
- Ausführen von infizierter Software aus *zweifelhafter* Quelle
- Ausnutzen *Systemschwachstellen*
- *Diebstahl* eines Endgerätes



Unterwegs im Internet ... aber sicher!

4.

Erkennung von Phishing, Smishing / Vishing / Quishing – Teil I



Mindestens eines der folgenden Merkmale erfüllt sehr wahrscheinlich eine **Phishing-E-Mail**:

- ❖ E-Mail-Text gibt *dringenden* Handlungsbedarf vor, z.B. Zugangssperre, Datenverlust
- ❖ Einsatz von *Drohungen*, z.B. „Falls Sie nicht ..., müssen wir Ihr Konto sperren“
- ❖ *Eingabeaufforderung* von vertraulichen Daten, z.B. PINs für Online-Banking, Kreditkartennummer
- ❖ E-Mail enthält *unklare* Links oder Formulare
- ❖ *ungewöhnliches* Anliegen eines vertrauten Absenders
- ❖ verdächtiger *falscher* Absender

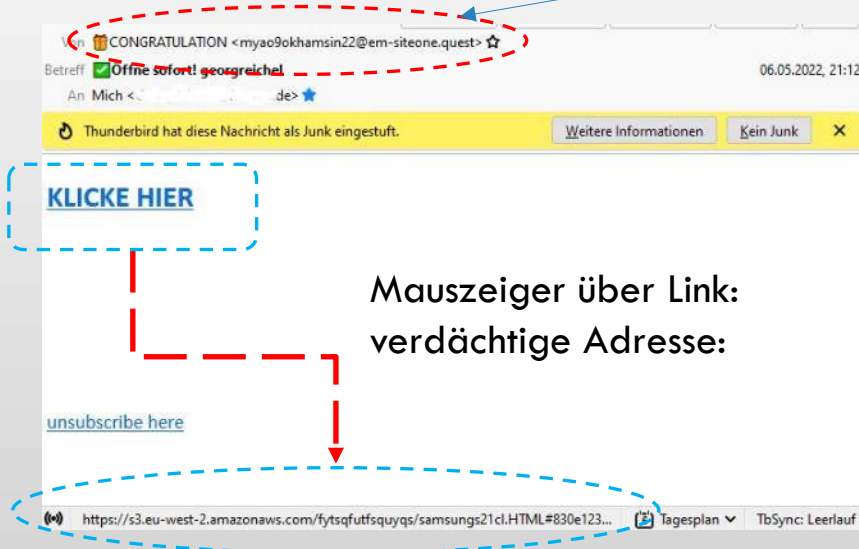
[BSI-Information zum Phishing](#)

Unterwegs im Internet ... aber sicher!

4.

Beispiel für Phishing

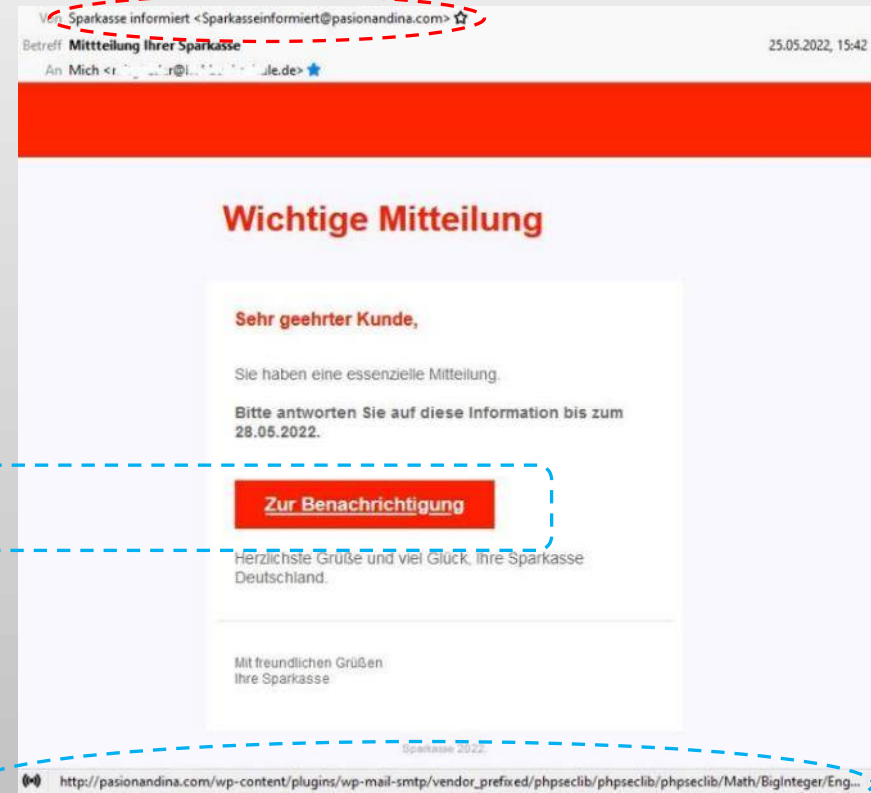
Verdächtige E-Mail-Adresse:



Mauszeiger über Link:
verdächtige Adresse:

Mauszeiger über Link:
verdächtige Adresse:

SPAM „Sparkasse“



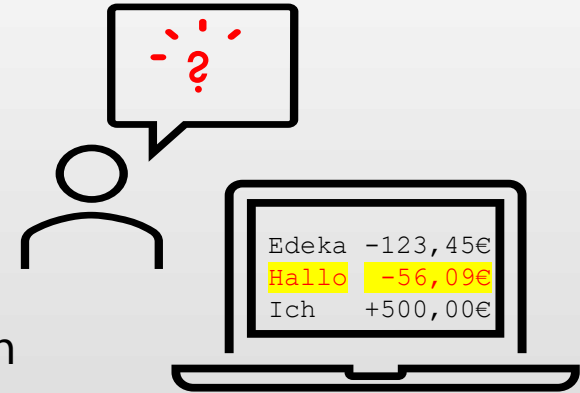
Unterwegs im Internet ... aber sicher!

4.

Opfer krimineller Aktivitäten? Was tun?

Missbrauch Online-Banking:

- sofortiger Viren-Scan der Endgeräte und ggf. Virenbeseitigung
- Zugangsdaten **sofort** ändern und möglichst Zwei-Faktor-Authentifizierung anwenden
- bei gesperrtem Zugriff: neues Passwort anfordern über „*Passwort vergessen*“
- kriminelle Transaktionen widerrufen
- Betreiber informieren
- ggf. sofort Konto sperren lassen – [Sperr-Notruf](#): +49 116 116
- Erstattung Anzeige bei der [Online-Wache](#)



Unterwegs im Internet

...

aber sicher!

Vielen Dank für Ihre Aufmerksamkeit!

Ihre Fragen sind gern willkommen!

