In‘s Internet?
Aber sicher!

ONLINE-VORTRAG ZUM SAFER-INTERNET-DAY
AM 08.02.2024

Cybercrime kann jeden treffen

und jederzeit!

Bundeslagebild Cybercrime des BKA

Achtung: nur „Cybercrime im engeren Sinne“!

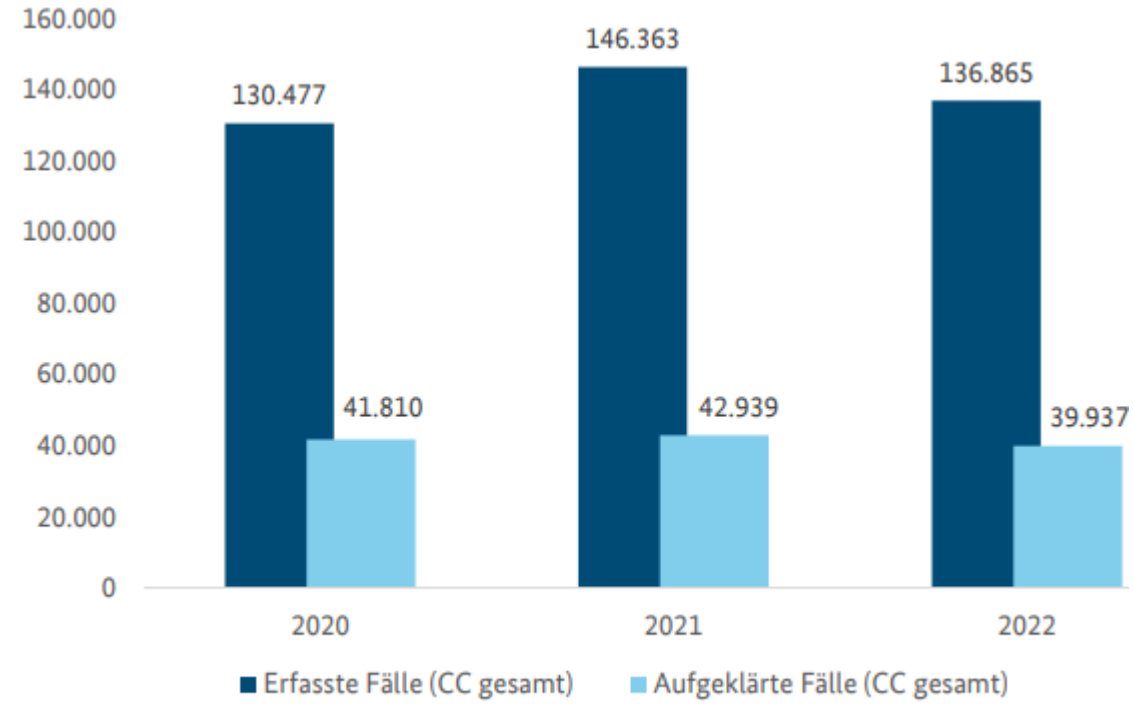


Abbildung 1: Erfasste und aufgeklärte Cybercrime-Fälle in Deutschland von 2020 bis 2022

Aufklärungsquote:

29,2 %

In 2022 erfasste Straftaten mit Auswertemerker „Tatmittel Internet“:

396.184

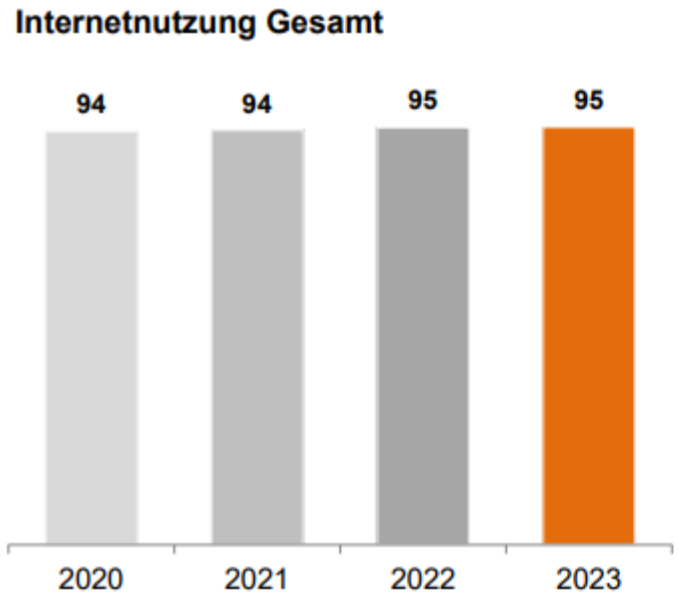
Quelle: https://www.bka.de/SharedDocs/Downloads/DE/Publikationen/JahresberichteUndLagebilder/Cybercrime/cybercrimeBundeslagebild2022.pdf?__blob=publicationFile&v=5

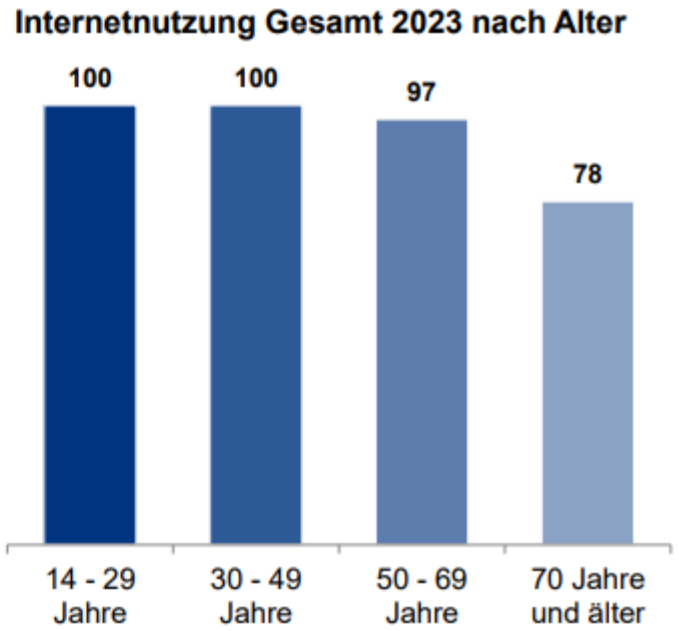
Internetnutzung in Deutschland

ARD / ZDF – ONLINE-STUDIE 2023

Die allgemeine Internetnutzung bleibt auf einem konstant hohen Niveau

Internetnutzung, Angaben in Prozent

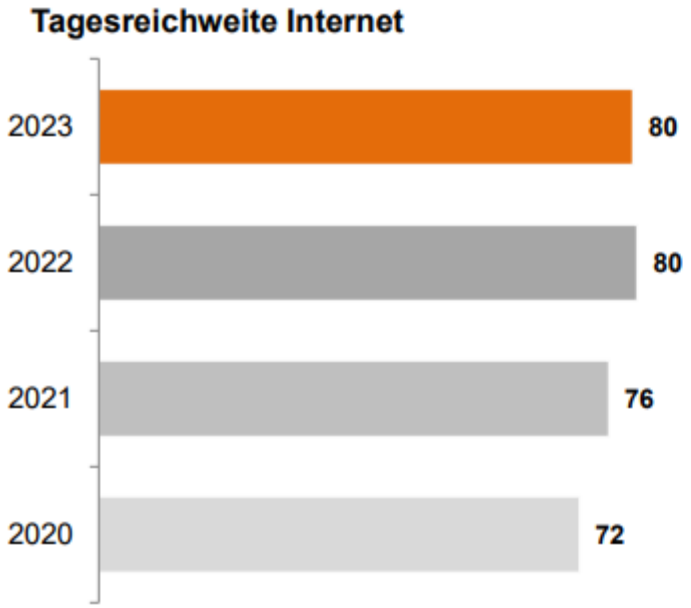


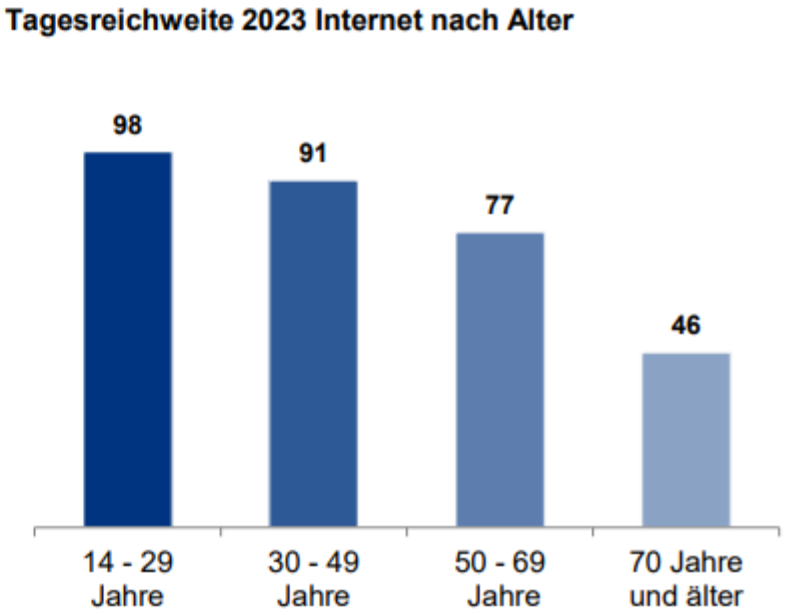


Quelle: https://www.ard-zdf-onlinestudie.de/files/2023/ARD_ZDF_Onlinestudie_2023_Publikationscharts.pdf /

Vier von fünf Menschen in Deutschland nutzen täglich das Internet

Internetnutzung, Angaben in Prozent





Quelle: https://www.ard-zdf-onlinestudie.de/files/2023/ARD_ZDF_Onlinestudie_2023_Publikationscharts.pdf /

Jeder ist für sich und seine Daten sowie für die eigene Sicherheit selbst verantwortlich!

Sicherheitsmaßnahmen funktionieren nur dann, wenn das gesamte System und Netzwerk gesichert ist.

Eine einzelne Schwachstelle im eigenen Netzwerk reicht für einen erfolgreichen Angriff evtl. schon aus.

Schwachstellen im eigenen Netz

t3n Pro News Magazin Wissen Themen Jobs Firmen Events Shop Anmeld

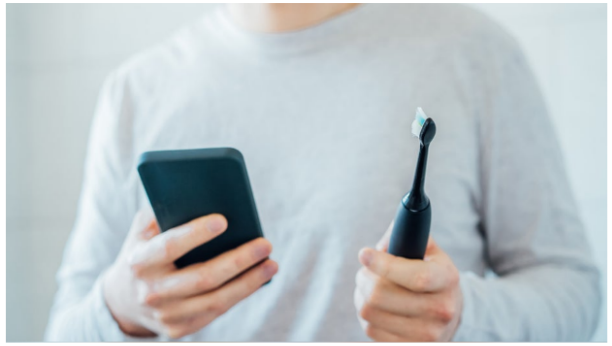
News

Smarte Zahnbürsten als Cyber-Waffe: 3 Millionen Geräte attackieren Schweizer Firma

Eine Armee an Zahnbürsten wurde kürzlich von Hackern für einen Cyberangriff auf ein Schweizer Unternehmen genutzt. Der Vorfall zeigt die Sicherheitslücken des Internet der Dinge (IoT) deutlich auf.

Von **Kay Nordenbrock**

07.02.2024, 14:30 Uhr • 1 Min. Lesezeit



Auch Zahnbürsten können gehackt werden. (Foto: Okrasiuk / Shutterstock)

Quelle: https://t3n.de/news/zahnbuersten-cyber-waffe-3-millionen-geraete-attackieren-firma-1606412/

Schwachstellen im eigenen Netz

- Hacker erlangten die Kontrolle über diese Zahnbürsten und initiierten eine Distributed Denial-of-Service (DDoS)-Attacke gegen die Website des Unternehmens.

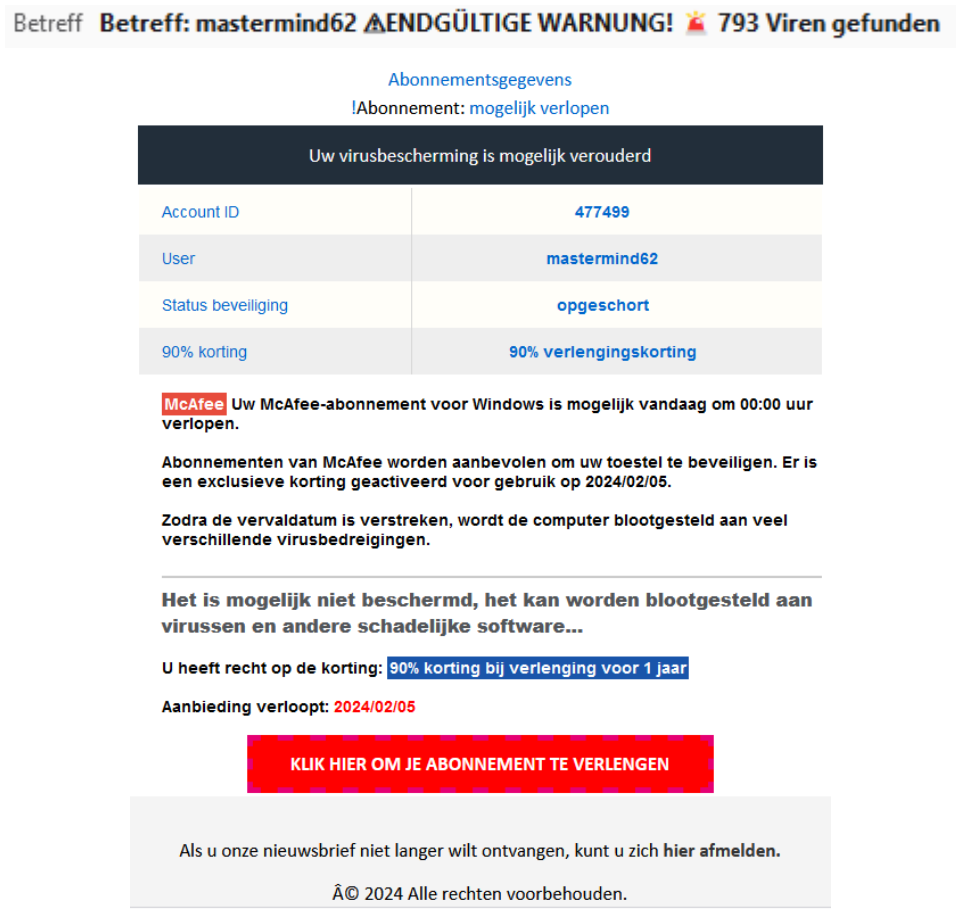
- „Jedes Gerät, das mit dem Internet verbunden ist, ist ein potenzielles Ziel – oder kann für einen Angriff missbraucht werden.“

- Experten empfehlen, die Software aller Geräte stets auf dem neuesten Stand zu halten und, wo möglich, ein Antivirenprogramm zu verwenden.

Nahezu alles kann manipuliert / gefälscht werden und somit wie echt aussehen.

Man darf nicht alles glauben!

Phishing



Betreff **Betreff: mastermind62 ⚠ENDGÜLTIGE WARNUNG! 🚨 793 Viren gefunden**

Abonnementsgegevens

!Abonnement: mogelijk verlopen

Uw virusbescherming is mogelijk verouderd

Account ID	**477499**
User	**mastermind62**
Status beveiliging	**opgeschort**
90% korting	**90% verlengingskorting**

McAfee **Uw McAfee-abonnement voor Windows is mogelijk vandaag om 00:00 uur verlopen.**

Abonnementen van McAfee worden aanbevolen om uw toestel te beveiligen. Er is een exclusieve korting geactiveerd voor gebruik op 2024/02/05.

Zodra de vervaldatum is verstreken, wordt de computer blootgesteld aan veel verschillende virusbedreigingen.

Het is mogelijk niet beschermd, het kan worden blootgesteld aan virussen en andere schadelijke software...

U heeft recht op de korting: 90% korting bij verlenging voor 1 jaar

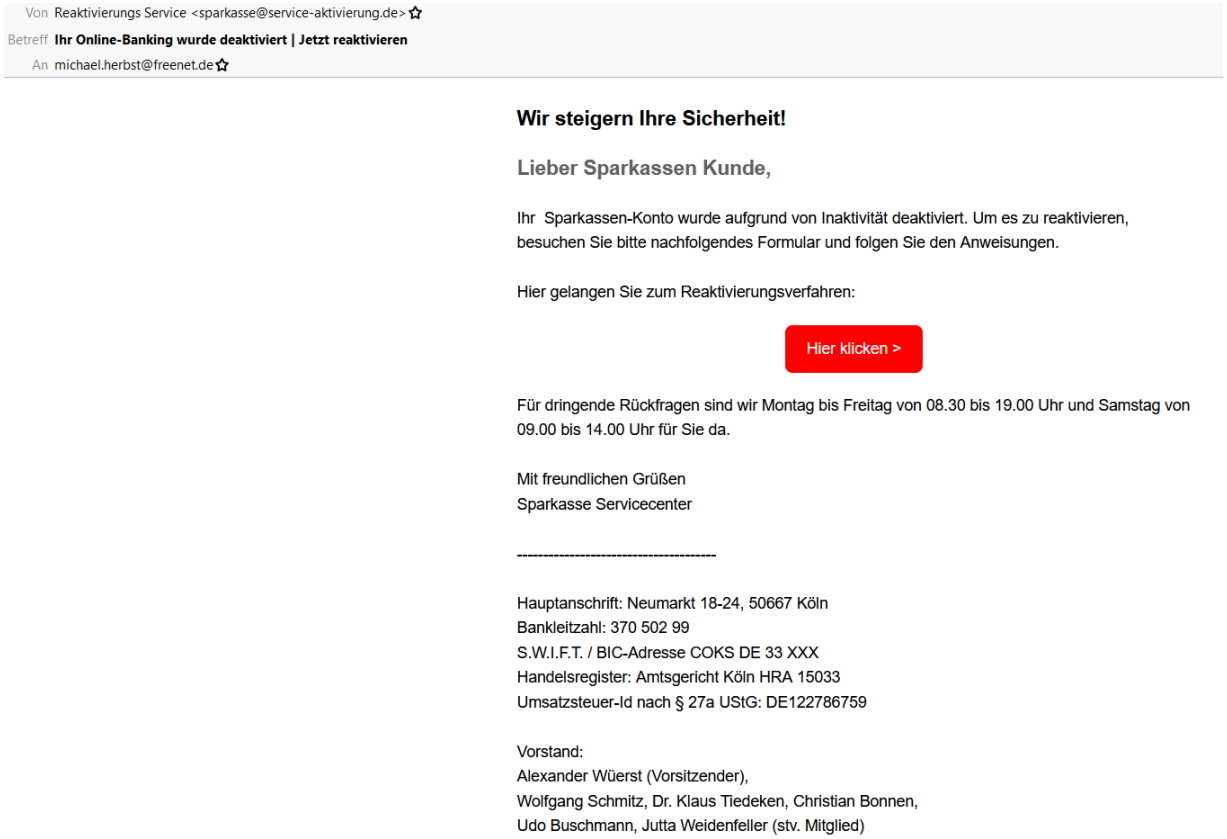
Aanbieding verloopt: 2024/02/05

KLIK HIER OM JE ABONNEMENT TE VERLENGEN

Als u onze nieuwsbrief niet langer wilt ontvangen, kunt u zich **hier afmelden.**

Â© 2024 Alle rechten voorbehouden.

Phishing



Von Reaktivierungs Service <sparkasse@service-aktivierung.de>
Betreff **Ihr Online-Banking wurde deaktiviert | Jetzt reaktivieren**
An michael.herbst@freenet.de

Wir steigern Ihre Sicherheit!

Lieber Sparkassen Kunde,

Ihr Sparkassen-Konto wurde aufgrund von Inaktivität deaktiviert. Um es zu reaktivieren, besuchen Sie bitte nachfolgendes Formular und folgen Sie den Anweisungen.

Hier gelangen Sie zum Reaktivierungsverfahren:

Hier klicken >

Für dringende Rückfragen sind wir Montag bis Freitag von 08.30 bis 19.00 Uhr und Samstag von 09.00 bis 14.00 Uhr für Sie da.

Mit freundlichen Grüßen
Sparkasse Servicecenter

Hauptanschrift: Neumarkt 18-24, 50667 Köln
Bankleitzahl: 370 502 99
S.W.I.F.T. / BIC-Adresse COKS DE 33 XXX
Handelsregister: Amtsgericht Köln HRA 15033
Umsatzsteuer-Id nach § 27a UStG: DE122786759

Vorstand:
Alexander Wüerst (Vorsitzender),
Wolfgang Schmitz, Dr. Klaus Tiedeken, Christian Bonnen,
Udo Buschmann, Jutta Weidenfeller (stv. Mitglied)

Phishing


NETFLIX
Achtung!!! Netflix Mitgliedschaft
N
Sehr geehrter Kunde,
Ihre Mitgliedschaft ist abgelaufen!
aber im Rahmen unseres
Treueprogramms können Sie jetzt
kostenlos für 90 Tage verlängern.
anytime
Kostenlos verlängern
* Nach der Anmeldung müssen Sie Ihre
Kreditkartendaten zur Validierung Ihres
Kontos eingeben.
Wir werden keine Beträge abbuchen.

Phishing


* Nach der Anmeldung müssen Sie Ihre Kreditkartendaten zur Validierung Ihres Kontos eingeben.
Wir werden keine Beträge abbuchen.
NETFLIX
Achtung!!! Netflix Mitgliedschaft
Sehr geehrter Kunde,
Ihre Mitgliedschaft ist abgelaufen!
aber im Rahmen unseres Treueprogramms können Sie jetzt kostenlos für 90 Tage verlängern.
anytime
Kostenlos verlängern
* Nach der Anmeldung müssen Sie Ihre Kreditkartendaten zur Validierung Ihres Kontos eingeben.
Wir werden keine Beträge abbuchen.

Phishing

Sie haben Ihr Speicherlimit erreicht

iCloud

Lieber mastermind62,
Ihr iCloud-Speicher ist voll.

Aber im Rahmen unseres Treueprogramms können Sie jetzt weitere 50 GB kostenlos bevor die Dateien auf Ihrem iCloud Drive gelöscht werden.

Erhalten Sie 50

*Nach der Anmeldung müssen Sie Ihre Kreditkartendaten zur Validierung Ihrer Apple ID eingeben.
Wir **werden** keine Beträge abheben.

Wenn Sie diese E-Mails nicht mehr erhalten möchten, können Sie sich abmelden, indem Sie hier klicken oder an 6130 W schreiben Flamingostr. Las Vegas, Nevada 89103

Phishing


*Nach der Anmeldung müssen Sie Ihre Kreditkartendaten zur Validierung Ihrer Apple ID eingeben.
Wir **werden** keine Beträge abheben.
Sie haben Ihr Speicherlimit erreicht
iCloud
Lieber mastermind62,
Ihr iCloud-Speicher ist voll.
Aber im Rahmen unseres Treueprogramms können Sie jetzt weitere 50 GB kostenlos bevor die Dateien auf Ihrem iCloud Drive gelöscht werden.
Erhalten Sie 50
*Nach der Anmeldung müssen Sie Ihre Kreditkartendaten zur Validierung Ihrer Apple ID eingeben.
Wir **werden** keine Beträge abheben.
Wenn Sie diese E-Mails nicht mehr erhalten möchten, können Sie sich abmelden, indem Sie hier klicken oder an 6130 W schreiben Flamingostr. Las Vegas, Nevada 89103

Cybertrading

Cybertrading

https://b2createaccounthero.s3.us-east-005.backblazeb2.com/LINK.html#4cd2fcce52d683948ed2065c2eda67dd/5013/s322

Cybertrading

BILD PLUS NEWS POLITIK GELD UNTERHALTUNG SPORT BUNDESLIGA LIFESTYLE RATGEBER RAISE AUTO DIGITAL SPIELE REGIO VIDEO

„Höhle der Löwen“ System macht Swiss Bürger reich! Sendung darf nicht ausgestrahlt werden, der Sender ist stinksauer

BILD untersucht die Wahrheit über das geheime System zum Geld verdienen

Cybertrading

MITTWOCH, 7. FEBRUAR 2024

56-Jährige um 100 000 Euro betrogen

Polizei warnt vor Internetkriminalität / Lauenhäger fällt nicht auf Masche herein

VON NINA JÜRGENSMEIER

HEUERSSEN/LAUENHAGEN. Gleich zwei Fälle von Betrug sind am Wochenende bei den Polizeiinspektionen der Samtgemeinden angezeigt worden. Während ein Mann aus Lauenhagen nicht auf die Masche eines angeblichen Motorradkäufers reinfiel, ist eine Heuerßerin nun um 100 000 Euro ärmer.

Die 56-Jährige gab am Samstag bei der Polizei zu Protokoll, dass sie seit Mai 2023 einen Anlageberater beauftragt habe, den sie allerdings nicht persönlich kenne. Die Korrespondenz habe nur per E-Mail stattgefunden.

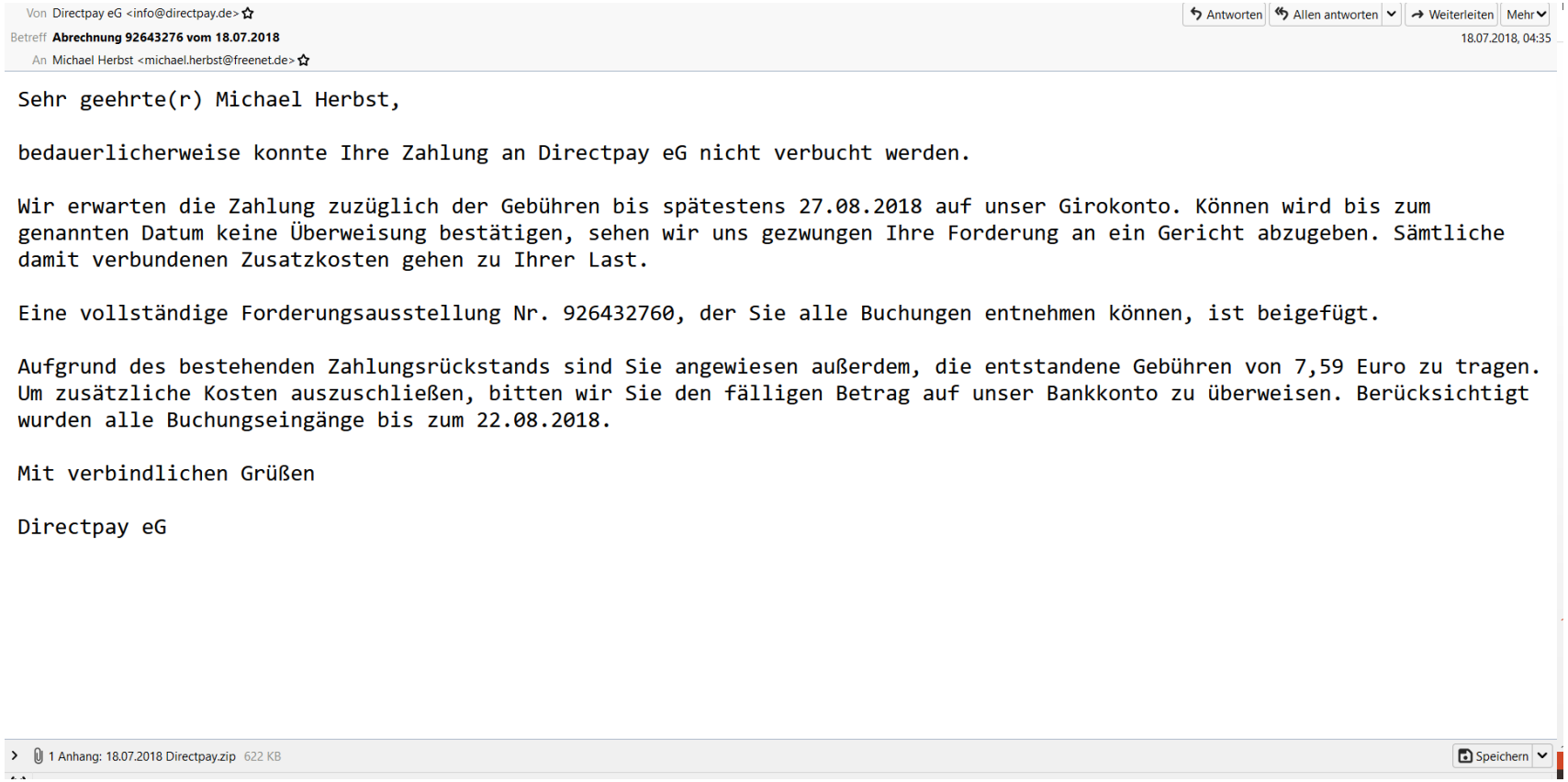
Wie die Frau weiterhin mitteilte, habe der Anlageberater mittels einer Software vollen Zugriff auf ihren Computer gehabt. Im Laufe des vergangenen Jahres habe er immer wieder Beträge von ihrem Konto dazu genutzt, um angeblich in Kryptowährungen zu investieren. Inzwischen seien circa 100 000 Euro durch ihn investiert worden.

Die versprochenen Gewinne

Eine Frau aus Heuerßen ist von einem angeblichen Anlageberater um rund 100 00 Euro betrogen worden. FOTO: DPA

Quelle: Schaumburg Nachrichten v. 07.02.2024, Seite 11

Verbreitung von Schadsoftware



Von Directpay eG <info@directpay.de>
Betreff **Abrechnung 92643276 vom 18.07.2018**
An Michael Herbst <michael.herbst@freenet.de>

Antworten | Allen antworten | Weiterleiten | Mehr
18.07.2018, 04:35

Sehr geehrte(r) Michael Herbst,

bedauerlicherweise konnte Ihre Zahlung an Directpay eG nicht verbucht werden.

Wir erwarten die Zahlung zuzüglich der Gebühren bis spätestens 27.08.2018 auf unser Girokonto. Können wird bis zum genannten Datum keine Überweisung bestätigen, sehen wir uns gezwungen Ihre Forderung an ein Gericht abzugeben. Sämtliche damit verbundenen Zusatzkosten gehen zu Ihrer Last.

Eine vollständige Forderungsausstellung Nr. 926432760, der Sie alle Buchungen entnehmen können, ist beigefügt.

Aufgrund des bestehenden Zahlungsrückstands sind Sie angewiesen außerdem, die entstandene Gebühren von 7,59 Euro zu tragen. Um zusätzliche Kosten auszuschließen, bitten wir Sie den fälligen Betrag auf unser Bankkonto zu überweisen. Berücksichtigt wurden alle Buchungseingänge bis zum 22.08.2018.

Mit verbindlichen Grüßen

Directpay eG

1 Anhang: 18.07.2018 Directpay.zip 622 KB

Speichern

Verbreitung von Schadsoftware

Von Directpay eG <info@directpay.de>
Betreff **Abrechnung 92643276 vom 18.07.2018**
An Michael Herbst <michael.herbst@freenet.de>

Antworten | Allen antworten | Weiterleiten | Mehr
18.07.2018, 04:35

Sehr geehrte(r) Michael Herbst,

bedauerlicherweise konnte Ihre Zahlung an Directpay eG nicht verbucht werden.

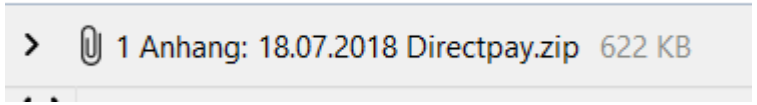
Wir erwarten die Zahlung zuzüglich der Gebühren bis spätestens 27.08.2018 auf unser Girokonto. Können wird bis zum genannten Datum keine Überweisung bestätigen, sehen wir uns gezwungen Ihre Forderung an ein Gericht abzugeben. Sämtliche damit verbundenen Zusatzkosten gehen zu Ihrer Last.

Eine vollständige Forderungsausstellung Nr. 926432760, der Sie alle Buchungen entnehmen können, ist beigefügt.

Aufgrund des bestehenden Zahlungsrückstands sind Sie angewiesen außerdem, die entstandene Gebühren von 7,59 Euro zu tragen. Um zusätzliche Kosten auszuschließen, bitten wir Sie den fälligen Betrag auf unser Bankkonto zu überweisen. Berücksichtigt wurden alle Buchungseingänge bis zum 22.08.2018.

Mit verbindlichen Grüßen

Directpay eG



1 Anhang: 18.07.2018 Directpay.zip 622 KB
Speichern

Verbreitung von Schadsoftware

Sehr geehrte(r) Michael Herbst,

wie vereinbart haben wir versucht den Betrag für Ihre Bestellung von Ihrem Konto abzubuchen. Die Bezahlung dieser Bestellung konnte damit nicht abgeschlossen werden.

Wir fordern Sie mit diesem Schreiben auf, den nicht beglichenen Betrag in Höhe von EUR 257,07 bis spätestens 20.03.2019 unter Angabe des Verwertungszwecks NR 25817447 auf unser Konto zu überweisen.

Michael Herbst
Am Eichkamp 24
31559 Haste

Tel. 057238413

Ihre persönliche Abrechnung finden Sie unter folgender Adresse

Nach Ablauf dieser Frist wird unser Inkassobüro ein gerichtliches Mahnverfahren gegen Sie Michael Herbst einleiten.

Mit freundlichen Grüßen

Micropayment GmbH
53797 Lohmar
USt-Id: DE 591500026
Sitz der Gesellschaft: Lohmar

Verbreitung von Schadsoftware

Von Micropayment GmbH Mail Service <Service@densothanhhoa.com>

Antworten | Allen antworten | Weiterleiten | Mehr

Betreff **Micropayment GmbH Michael Herbst - Ihr gespeichertes Bankkonto ist nicht hinreichend gedeckt**

14.03.2019, 06:32

An Michael Herbst <michael.herbst@freenet.de>

Sehr geehrte(r) Michael Herbst,

wie vereinbart haben wir versucht den Betrag für Ihre Bestellung von Ihrem Konto abzubuchen. Die Bezahlung dieser Bestellung konnte damit nicht abgeschlossen werden.

Wir fordern Sie mit diesem Schreiben auf, den nicht beglichenen Betrag in Höhe von EUR 257,07 bis spätestens 20.03.2019 unter Angabe des Verwertungszwecks NR 25817447 auf unser Konto zu überweisen.

Michael Herbst
Am Eichkamp 24
31559 Haste

Tel. 057238413

Ihre persönliche Abrechnung finden Sie unter folgender Adresse

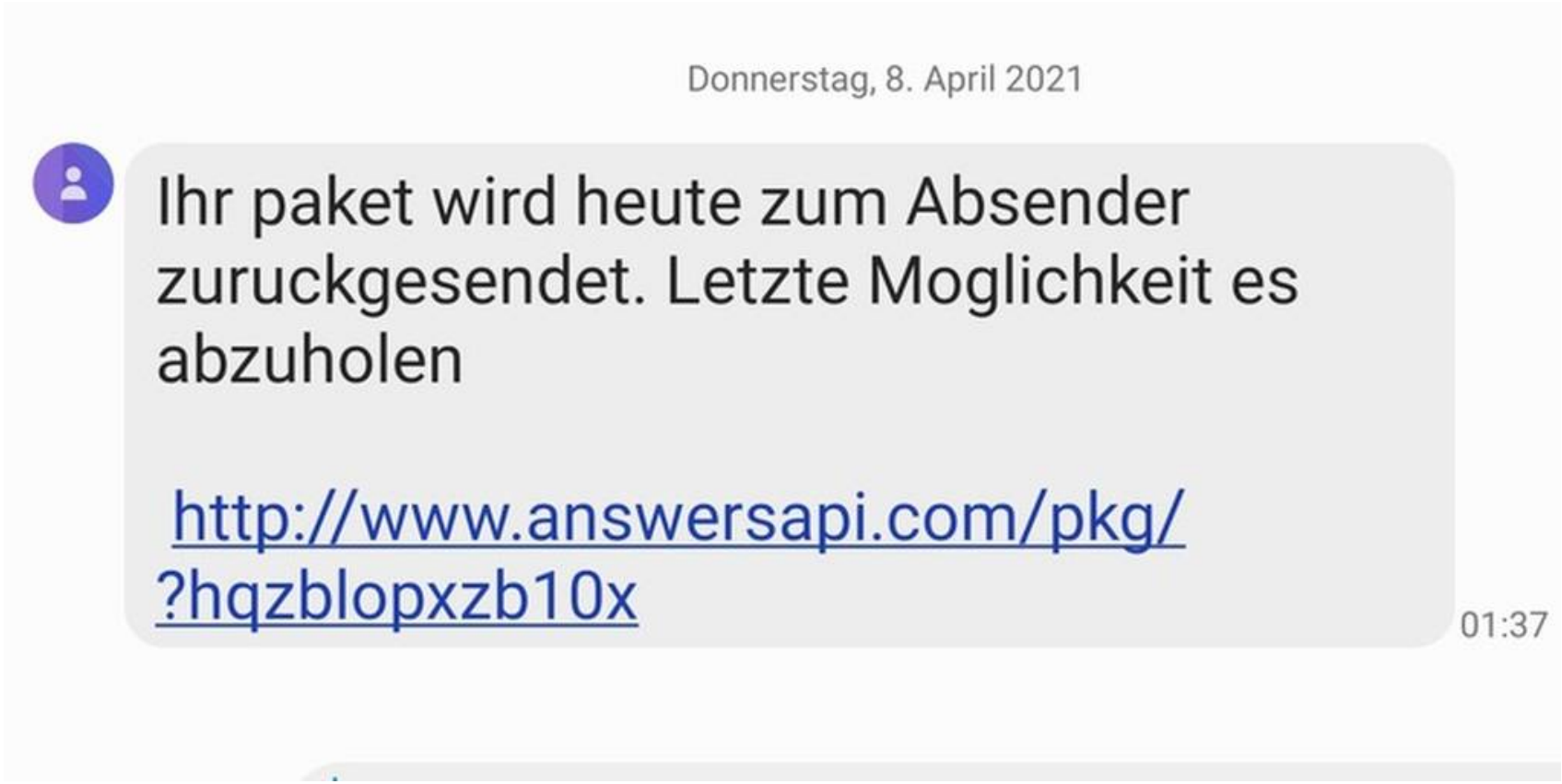
http://www.manyataexpress.com/css/K87227016568062662496571064241912.zip

Nach Ablauf dieser Frist wird unser Inkassobüro ein gerichtliches Mahnverfahren gegen Sie Michael Herbst einleiten.

Mit freundlichen Grüßen

Micropayment GmbH
53797 Lohmar
USt-Id: DE 591500026
Sitz der Gesellschaft: Lohmar

Smishing

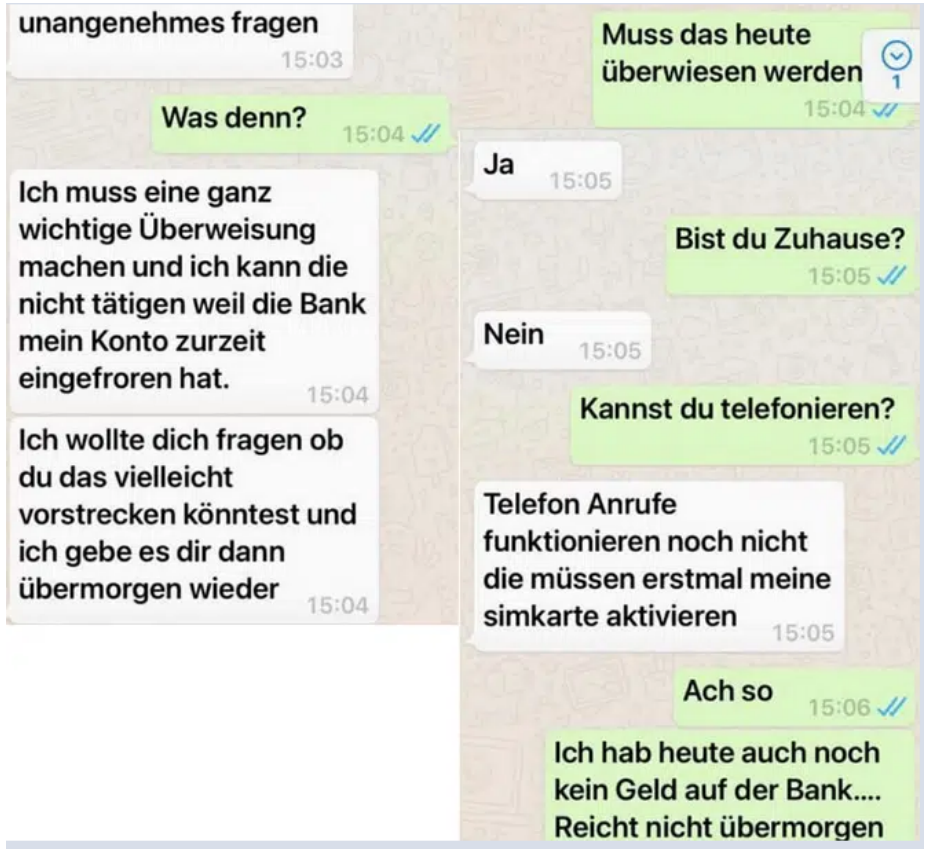

Donnerstag, 8. April 2021
Ihr paket wird heute zum Absender zuruckgesendet. Letzte Moglichkeit es abzuholen
http://www.answersapi.com/pkg/?hqzblopxzb10x
01:37

Smishing


Donnerstag, 7. Oktober 2021
Ihre VR-SecureGo Registrierung läuft am 07.10.2021 ab. Bitte verlängern Sie Ihren Zugang mit dem folgendem link: https://volksbank.de-secrue-go-873.xyz/


SMS-Nachricht
Heute, 11:13
Sie haben . einen verpassten Anruf. Der Anrufer ¿ hat Ihnen eine Nachricht . hinterlassen http://humandiagnostics.co.in/p/?rg3c-ltrt3c

Betrugsdelikte



Sicherheit und Bequemlichkeit sind zwei Faktoren, die oft nicht gut harmonieren!

100 Prozent Sicherheit gibt es nicht!

Aber Sie können es den Tätern schwerer machen!

Das Internet bietet viele gute Möglichkeiten!

Nutzen Sie die Vorteile und sorgen Sie recht-zeitig vor, um sich vor Gefahren zu schützen!

Betriebssystem und Programme

- Aktuelles System
- Aktuelle Updates / Automatische Updates aktivieren
- Gilt auch für Browser, Mailprogramm, Office-Programme, PDF-Reader, Apps …
- Auf Systemmeldungen achten und entsprechende Maßnahmen ergreifen
- Mehrere Benutzerkonten einrichten (Admin, eingeschränkte Benutzer)

Virenschutz

- Aktuelle Programmversionen
- Aktuelle Virendefinitionen
- Automatische Updates aktivieren
- Kostenpflichtige Programme verfügen in der Regel über einen besseren Leistungsumfang als kostenfreie Versionen
- Entscheidungshilfe: https://www.av-test.org/de/
- Nie zwei Antivirenprogramme gleichzeitig! (Ausnahme: Windows Defender)
- Eigener Virenschutz schützt auch andere

Firewall

- Firewalls von Router und Betriebssystemen reichen in der Regel aus
- Zusätzliche können – anders als beim Virenschutz – nicht schaden

Privatsphäre / Tracking

Quelle: https://de.statista.com/infografik/12252/tracking-reichweite-von-internet-unternehmen/

Privatsphäre / Tracking

Berliner Unternehmen

Datenhändler verticken Handy-Standorte von EU-Bürger*innen

Eine Enthüllung in den Niederlanden zeigt die Risiken durch den weltweiten Datenhandel – auch für die nationale Sicherheit. Demnach standen detaillierte Standortdaten von potentiell Millionen Niederländer*innen zum Verkauf, darunter Angehörige des Militärs.

17.01.2024 um 16:01 Uhr - Ingo Dachwitz, Sebastian Meineck - in Datenschutz - 6 Ergänzungen

Personalisierte Werbung

Sie können wählen, ob Werbung, die Sie in Google-Diensten und auf Websites von Google-Partnern sehen, für Sie personalisiert wird

Mein Anzeigen-Center

Personalisierte Werbung auf Google

Aus

Einstellungen für Werbung auf Partnerwebsites

Optionen für Werbung auf Websites von Google-Partnern

Privatsphäre / Tracking

Wer uns trackt:

- Der Hersteller des Betriebssystems
- Der Hersteller des Endgeräts (herstellereigene Software)
- Der Internet-Anbieter, der uns die Verbindung ermöglicht (z. B. über DNS)
- Der Hersteller der Software / Apps, die wir nutzen
- Der Betreiber der Cloud, in der wir unsere Daten speichern
- Der Betreiber der Website, die wir besuchen
- Der Drittanbieter, der auf der besuchten Website Werbung schaltet
- Der Mailanbieter, bei dem wir unser Mailkonto haben
- Der Absender der Mail, die wir im Mailprogramm öffnen
- Und viele mehr…

Browserschutz / Privatsphäre

- Ausschließlich: Nutzung sicherer Verbindungen: https://…
- Flashplayer und Java deaktivieren / deinstallieren
- Addons und PlugIns zum sicheren / anonymeren Surfen im Netz:
  - Adblocker
  - Scriptblocker
  - Flagfox (nur Firefox)

Browserschutz / Privatsphäre

- Nutzung alternativer Suchmaschinen / Startseiten
- Der „Inkognito“-Modus im Browser anonymisiert nicht!
- Die „do-not-track“ - Option im Browser ist lediglich eine Empfehlung an die Betreiber von Webseiten

Google wendet Milliardenklage gegen Inkognito-Modus per Einigung ab

Der Inkognito-Modus von Chrome verspricht "privates Surfen", doch wie strikt dieser aktivierbare Schnüffelschutz ist, darüber kann man diskutieren. Denn auch per Inkognito werden diverse Daten erfasst. Dazu gab es auch eine Klage, diese wurde nun außergerichtlich beigelegt.

Quelle: https://winfuture.de/news,140351.html

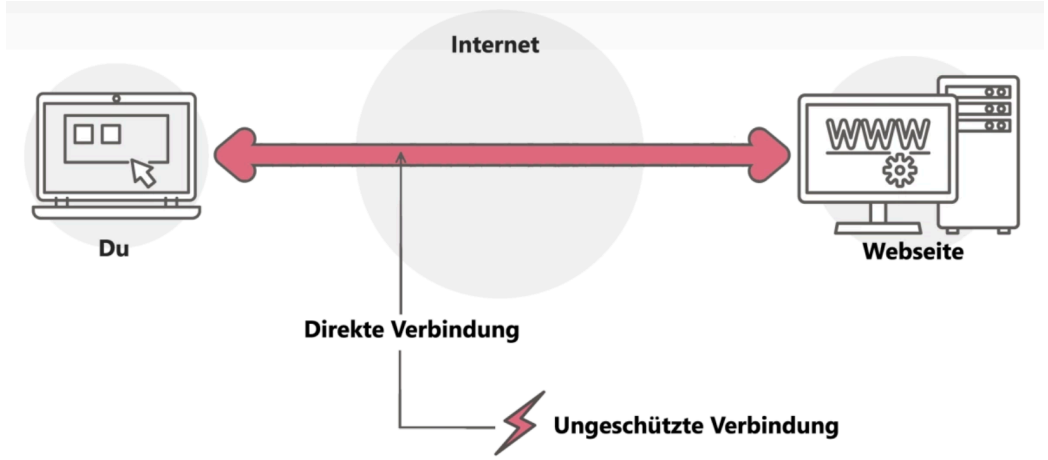
Alternative Anwendungen

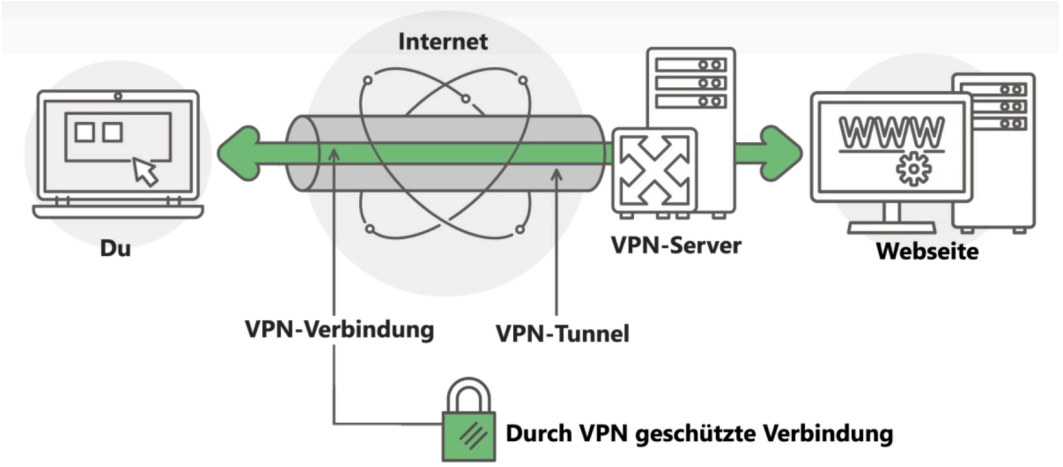
- Browser:
  - Mozilla Firefox
  - Brave (oder alle Chromium-basierten Alternativen)
  - Opera
  - TOR-Browser
- Mobiler Browser:
  - Mozilla Firefox
  - Brave
  - Fennec
  - Mull
- Alternative Suchmaschinen:
  - DuckDuckGo
  - Startpage (bedingt, zeigt gesponserte Suchergebnisse)
  - Metager
  - Quant
    - Speziell für Kinder: Quant Junior

Alternative Anwendungen

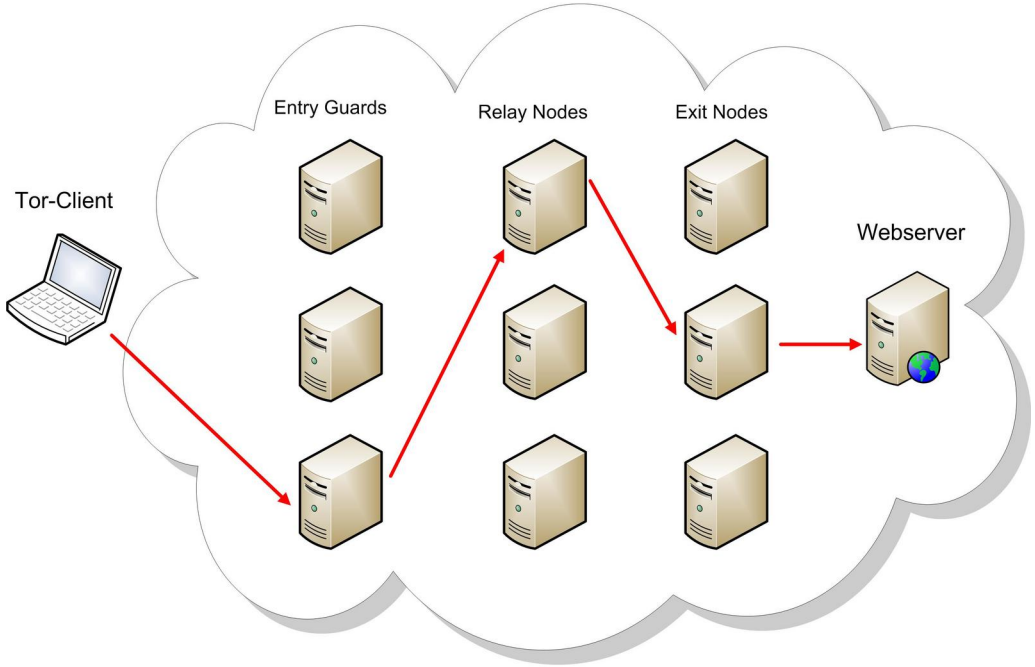
- Für fortgeschrittene Nutzer:
  - Anonymisierungsdienste (VPN / TOR-Netzwerk) nutzen
  - Alternative DNS-Server (z. B. dns3.digitalcourage.de)
  - Selbstgehostete DNS-Server (Adguard, Pi-Hole)

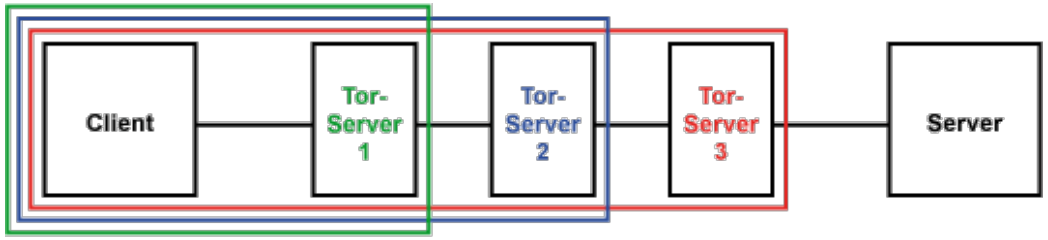
Virtual Private Networks (VPN)





Das TOR-Netzwerk - das „böse“ Darknet

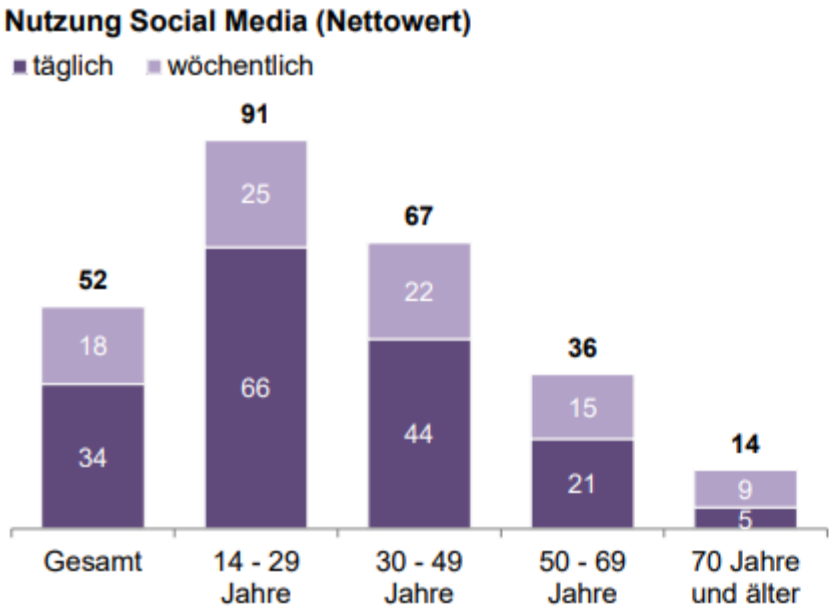


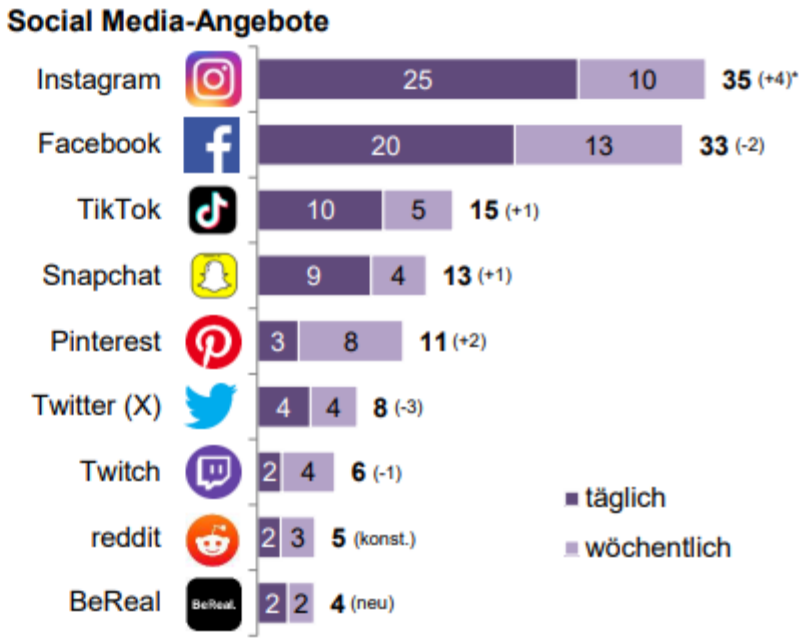


Verschlüsselung nach dem Zwiebel-Prinzip

Social Media

Social Media-Angebote, Angaben in Prozent





Quelle: https://www.ard-zdf-onlinestudie.de/files/2023/ARD_ZDF_Onlinestudie_2023_Publikationscharts.pdf /

Social Media

Quelle: https://www.toonpool.com/cartoons/Sprechstunde_160718#img9

Social Media

Ein Thema, das mir besonders am Herzen liegt:

- Auch Kinder und Jugendliche haben selbstverständlich ein Recht am eigenen Bild!

- Kinderbilder gehören nicht ins Netz!

Alternative Anwendungen

Herzlich willkommen im Fediverse!

Facebook	=>	Friendica / Hubzilla
Twitter / X	=>	Mastodon
Instagram	=>	Pixelfed
Youtube	=>	Peertube / Funkwhale

Messenger-Dienste

Mailempfang und Versand

- Keine unerwarteten / unbekannten Anhänge öffnen (egal welcher Art und auf welchem System!)
- Anhänge von Bekannten erfragen / auf Schadsoftware prüfen
- Linkziel (Mouseover-Einblendung) beachten, im Zweifel keinen Links aus Mails folgen, ggf. nachfragen
- Achtung: Täter täuschen gern Rechnungen, Mahnungen, Faxe, Kontosperrungen, Überweisungen, Lieferungen, ungelesene Nachrichten, Teilnahmen, Gewinne, Bewerbungen, Bestellungen usw. vor
- Schadsoftware (z. B. Emotet) führt vorherige Kommunikation mittels Bot fort
- Keine sensiblen Daten (z.B. Kontodaten, Ausweiskopie) zurücksenden!
- Onlineshops, Zahlungsdienstleister, Banken, Provider und andere Unternehmen fordern nie zur Herausgabe von Account-/Kontodaten auf.

Alternativen

Alternatives Mailprogramm:

- Mozilla Thunderbird

Alternative mobile Mailprogramme:

- K9 Mail
- FairEMail
- pEp Mail

Alternative Mailanbieter:

- Posteo
- Mailbox.org
- Tutanota
- Protonmail
- StartMail

Clouddienste

- Alle großen Cloud-Anbieter scannen die Daten der Nutzer
- Wo werden meine Daten physikalisch gespeichert? Wo steht der / stehen die Server?
- Welches Recht gilt bei der Nutzung von Cloud-Speichern?
- Sind meine Daten verschlüsselt, wenn ja, wie?

Alternative Cloud-Dienste

- pCloud
- Tresorit
- Luckycloud (ausschließlich deutscher Anbieter)
- Mega (zweifelhafter Ruf)
- Dropbox

- Nextcloud
- Owncloud

- Eigenes Cloud-Hosting mit Nextcloud oder Owncloud

Sichere Passwörter

Das beliebteste Passwort ist

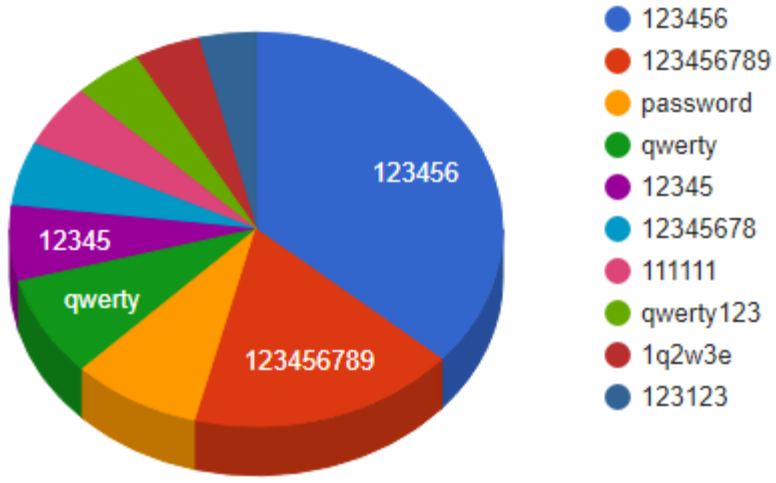
Sichere Passwörter

Das beliebteste Passwort ist

123456

Schon seit Jahren…

(Un)Sichere Passwörter



	Passwort	Häufigkeit
1	123456	8,01‰
2	123456789	3,84‰
3	password	1,87‰
4	qwerty	1,82‰
5	12345	1,36‰
6	12345678	1,15‰
7	111111	1,14‰
8	qwerty123	1,00‰
9	1q2w3e	0,95‰
10	123123	0,84‰

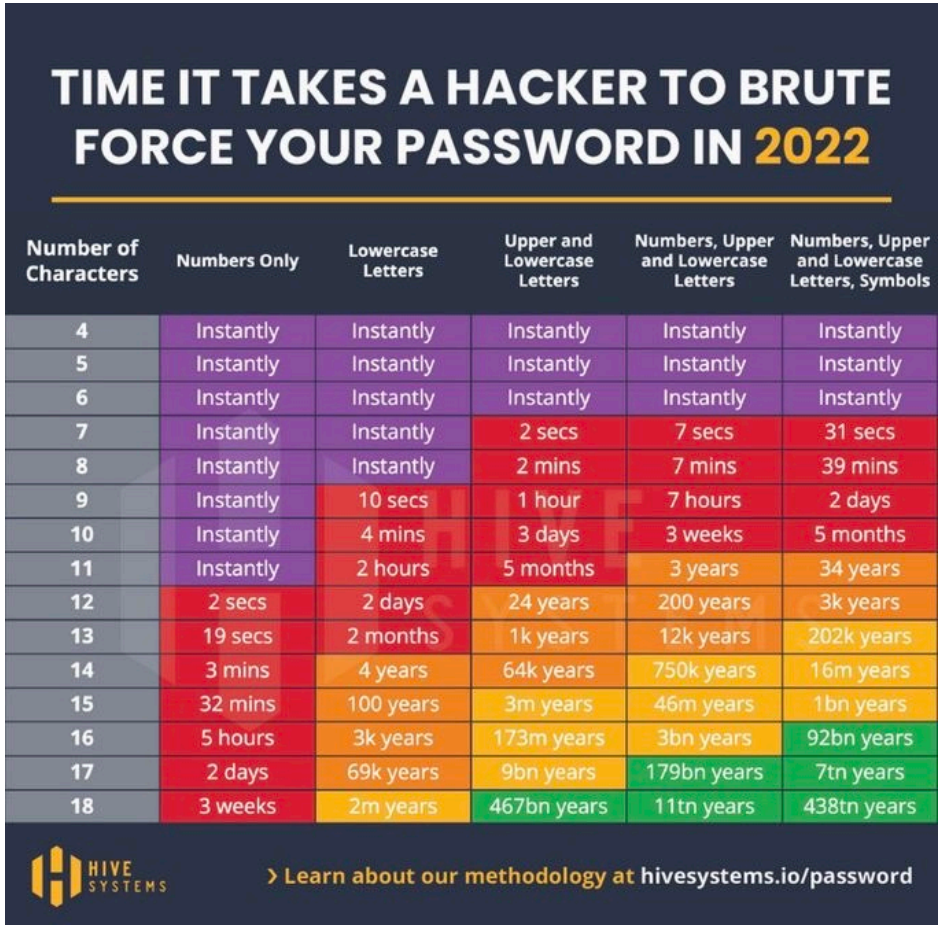
Quelle: https://sec.hpi.de/ilc/statistics

Sichere Passwörter

- Komplexität
  - Kombination aus großen und kleinen Buchstaben, Zahlen, Sonderzeichen
  - Nicht im Wörterbuch zu finden
- Länge
  - Lange Passwörter (15 Zeichen oder mehr)
- Länge schlägt Komplexität

- Keine zusammenhängenden / erschließbaren Wörter
- Regelmäßig (bei Bedarf) ändern
- Für jeden Dienst ein eigenes, neues Passwort, kein Recycling der Passwörter
- Nicht im Computer speichern (Ausnahme: Passworttresor)
- Keine Weitergabe an Dritte
- Besonders wichtig für Mailpostfach und mobile Geräte

Sichere Passwörter



TIME IT TAKES A HACKER TO BRUTE FORCE YOUR PASSWORD IN 2022

Number of Characters	Numbers Only	Lowercase Letters	Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters, Symbols
4	Instantly	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	Instantly	Instantly	Instantly
6	Instantly	Instantly	Instantly	Instantly	Instantly
7	Instantly	Instantly	2 secs	7 secs	31 secs
8	Instantly	Instantly	2 mins	7 mins	39 mins
9	Instantly	10 secs	1 hour	7 hours	2 days
10	Instantly	4 mins	3 days	3 weeks	5 months
11	Instantly	2 hours	5 months	3 years	34 years
12	2 secs	2 days	24 years	200 years	3k years
13	19 secs	2 months	1k years	12k years	202k years
14	3 mins	4 years	64k years	750k years	16m years
15	32 mins	100 years	3m years	46m years	1bn years
16	5 hours	3k years	173m years	3bn years	92bn years
17	2 days	69k years	9bn years	179bn years	7tn years
18	3 weeks	2m years	467bn years	11tn years	438tn years

HIVE SYSTEMS

› Learn about our methodology at hivesystems.io/password

Quelle: https://www.hivesystems.io/blog/are-your-passwords-in-the-green

Sichere Passwörter

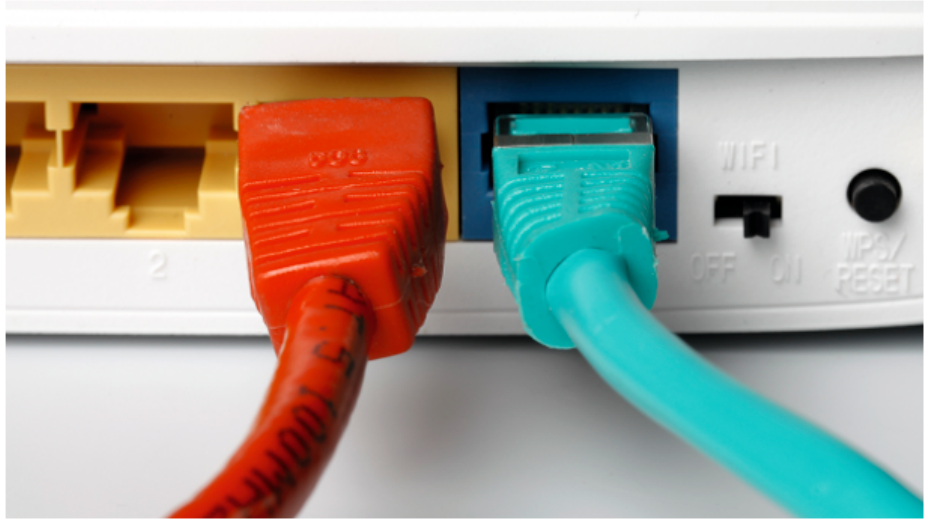
- 2 – Faktor – Authentifizierung
- Passwortsafes

Das eigene Netzwerk schützen!

Gehackte Router als Bot-Netz

Das Bot-Netz, das an Weihnachten die Spielenetzwerke von Sony und Microsoft lahmlegte, bestand einer Analyse des Sicherheitsexperten Brian Krebs zufolge zum Großteil aus gehackten Heimroutern.

Lesezeit: 2 Min. In Pocket speichern 159



Quelle: https://www.heise.de/newsticker/meldung/Gehackte-Router-als-Bot-Netz-2515682.html

Das eigene Netzwerk schützen!

- Den Router gegen unbefugte Zugriffe von Außen und Innen absichern
- Update der Firmware
- Änderung der Passwörter im Administratorkonto und WLAN
- Sicherung des WLAN (mindestens WPA2), besser WPA3 (aber Vorsicht: nicht alle Geräte können den Standard nutzen)
- Für fortgeschrittene Nutzer:
  - WLAN (SSID) umbenennen und unsichtbar machen
  - MAC-Adressenfilterung
  - WPS deaktivieren

Datensicherung

Quelle: https://upload.wikimedia.org/wikipedia/commons/4/4f/%EA%B0%90%EC%97%BC%EC%82%AC%EC%A7%84.png

Quelle: https://www.myitplanet.de/wp-content/uploads/2019/08/datenrettung-kosten-1024x682.jpeg.webp

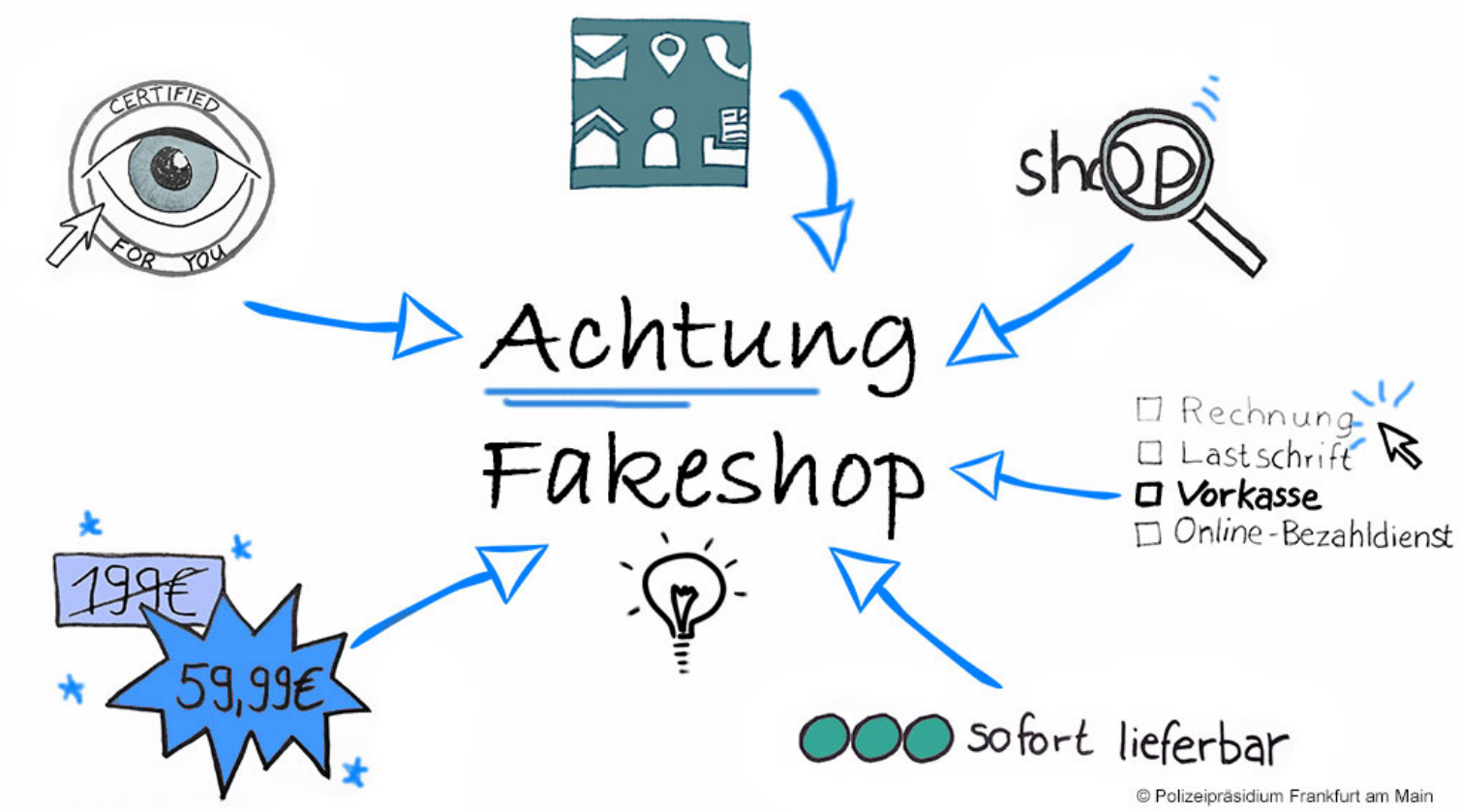
Datensicherung

- Regelmäßig (wöchentlich, ggf. auch täglich, je nach Wichtigkeit der Daten)
- Auf externe Datenträger
- Externe Datenträger sofort nach dem Backup trennen
- Antivirenprüfung auch auf externen Datenträgern
- Ggf. mehrere Nutzer auf einem Rechner beachten
- Gilt für alle Endgeräte (PC, Smartphone usw.)

Datensicherung

Quelle: https://www.apfelwerk.de/2014/09/das-tao-des-backups/kein-backup-kein-mitleid/

Online-Shopping



Quelle: https://www.polizei.hessen.de/icc/internetzentral/nav/c35/broker.jsp?uCon=c8960769-9c27-2261-0e01-f9e70517fe34&uTem=bff71055-bb1d-50f1-2860-72700266cb59&uMen=c3570ee1-825a-f6f8-6373-a91bbcb63046#uCon_c8960769-9c27-2261-0e01-f9e70517fe34

Online-Shopping

- Achtung bei vermeintlichen Schnäppchen! Häufig ist der Preis zu gut, um wahr zu sein.
- Vor der Bestellung Recherche zum Shop / Anbieter
- Überprüfung der Adresszeile im Browser
- Nutzung sicherer Zahlungswege, keine Vorkasse / Nachnahme bei unbekannten Shops
- Vorsicht bei der Herausgabe von eigenen Konto- oder Zahlungsdaten
- Nutzung seriöser Shops / Anbieter (z.B. seriöse Gütesiegelanbieter mit Gegenkontrolle)

Online-Shopping

Quelle: https://www.avira.com/de/blog/internet-shops-diese-guetesiegel-muessen-sie-kennen-teil-3

Online-Banking

- Eigener Benutzer am Rechner (kein „Surfprofil“)
- Vorsicht bei ungewöhnlichen Aufforderungen / Meldungen, bei Zweifeln Vorgang besser abbrechen!
- Kontoauszüge zeitnah / sofort überprüfen
- Nur auf „sauberem“ / aktuellem Computer
  - besser: Computer von DVD / CD starten
- 2-Faktor-Authentifizierung (SMS, Zweitgerät, USB-Stick) ist zwingend vorgeschrieben
- Notruf: 116 116 oder eigene Bankhotline

Sicherheit unterwegs

- Vorsicht in allen fremden Netzwerken
- Kein sensibler Datenverkehr in fremden Netzwerken
- Vorsicht bei unbekannten / unverschlüsselten Hotspots
- Vorsicht auch bei vermeintlich bekannten Hotspots
- Nutzung von VPN (Virtuelles Privates Netzwerk)
- Kein Anschluss eigener Hardware an fremde Geräte (z.B. USB-Stick oder Speicherkarte an PC im Internetcafe / Hotel)
- Installation von Ortungssoftware / Fernsperre / Fernlöschung für Mobilgeräte

Welche weiteren Themen sind aktuell in der Diskussion?

- Vorratsdatenspeicherung
- Chat-Kontrolle
- Künstliche Intelligenz

Wo bekomme ich weitere Informationen?

- Ratgeber Internetkriminalität
  https://www.polizei-praevention.de/
- Bundesamt für Sicherheit in der Informationstechnik
  https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/verbraucherinnen-und-verbraucher_node.html
- Initiative klicksafe (Information zur Sicherheit in sozialen Medien, Schwerpunkt auf Kinder und Jugendliche)
  https://www.klicksafe.de/
- Initiative „Deutschland sicher im Netz“
  https://www.sicher-im-netz.de/
- … und viele andere: Fragen Sie die Suchmaschine Ihres Vertrauens!

Zeit für Fragen / Diskussion