TERZO DIETIKON

Dig[iT]reff

20.8.2026

Sicher vor Betrug im Internet

Referent: René Müller

3

4

Risiken und Gefahren von Online-Aktivitäten

5

Risiken und Gefahren im Internet

- **Suchtgefahr**: Online-Angebote, soziale Medien und Surfen an sich können süchtig machen.
- **Cyber-Mobbing und Stalking**: andere können uns über das Internet und die sozialen Medien verfolgen und belästigen.
- **Datendiebstahl**: Andere Personen können unsere Daten stehlen, und unsere Identität annehmen und auch unsere Kreditkarten oder Bankkonten nutzen.
- **Reputationsschäden**: Andere Personen können unseren Ruf schädigen mit Lügen oder Gerüchten – oder auch mit Sachen, die wir tatsächlich machen – das kann bei der Stellensuche ein grosses Problem sein!

6

Risiken und Gefahren im Internet

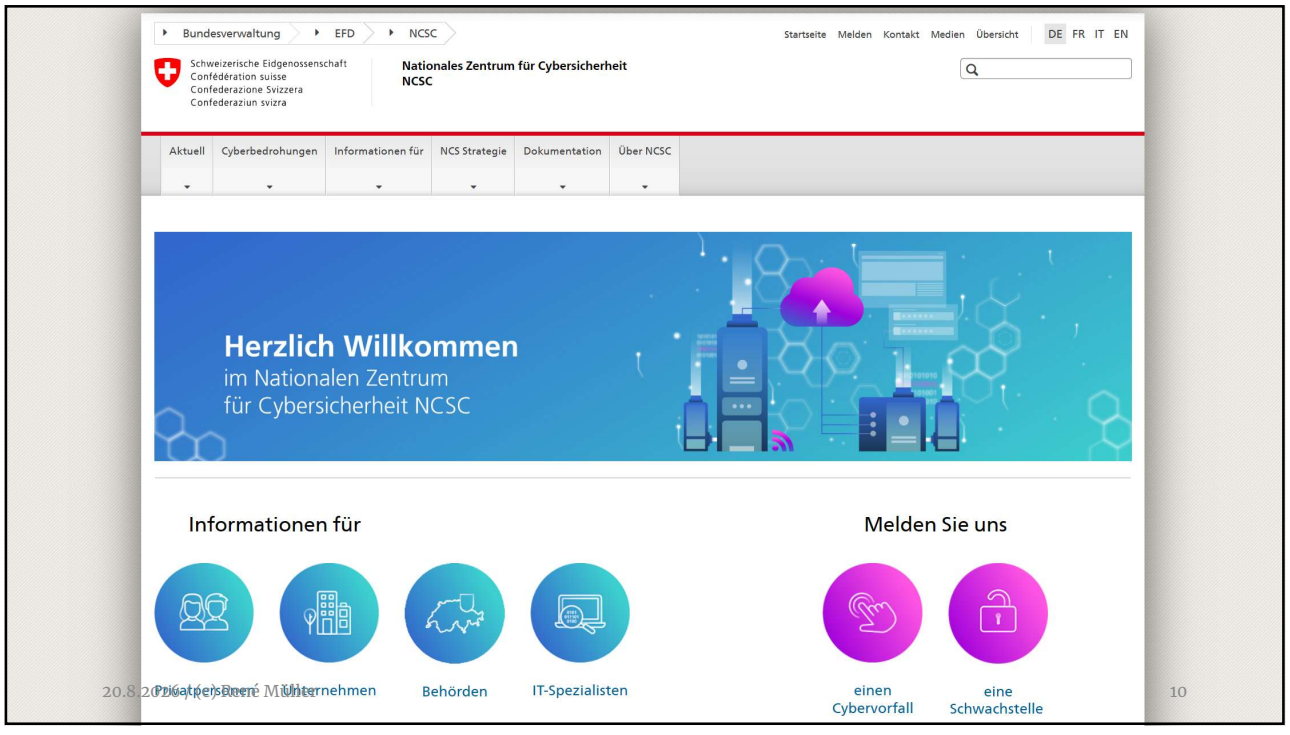
- **Zuverlässigkeit der Informationen:** Viele Personen, vor allem auf Social Media verkaufen ihre Information als Wahrheit. Als User muss man aber sehr kritisch sein, und sich genau fragen: Woher kommt diese Information? Gibt es «Beweise»?
- **Manipulation:** Viele User werden durch Webseiten und soziale Medien gesteuert. Sie denken und machen deswegen Dinge, die sie ohne diese Steuerung nicht tun würden (z.B. etwas kaufen)
- **Siehe auch** Online-Shops, weiter unten

7

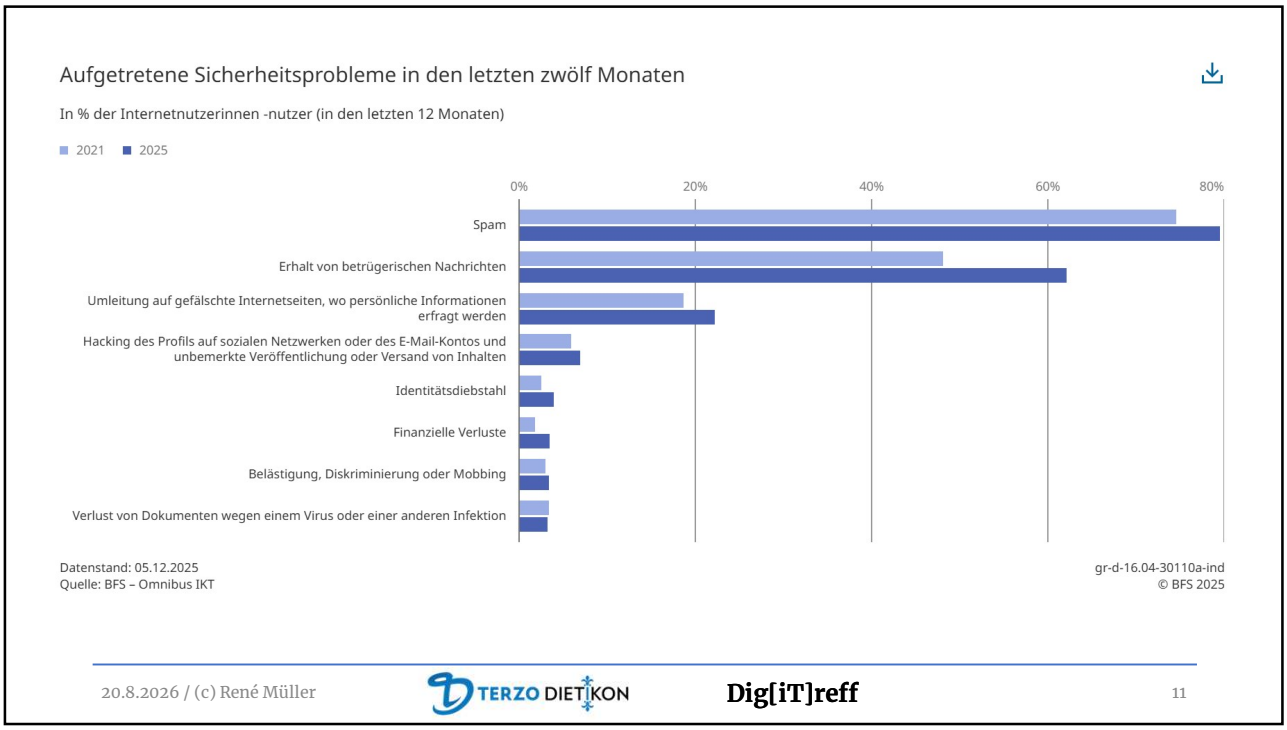
8


[X] NEW ATTACK: FROM [THAILAND] TO [INDIA]
[X] NEW ATTACK: FROM [UNITED STATES] TO [TAIWAN]
[X] NEW ATTACK: FROM [ALGERIA] TO [SAUDI ARABIA]
LOCAL TIME
11:39:43
ATTACKS TODAY
354,685
FIREEYE CYBER THREAT MAP
PORTUGAL
UNITED STATES
ALGERIA
SAUDI ARABIA
INDIA
THAILAND
TAIWAN
ATTACKERS
TOP COUNTRIES
(PAST 30 DAYS)
Powered by FireEye Labs
TOP 5 REPORTED INDUSTRIES (PAST 30 DAYS)
FINANCIAL SERVICES
SERVICES/CONSULTING
TELECOM
MANUFACTURING
INSURANCE
VIEW FULL SCREEN
The "FireEye Cyber Threat Map" is based on a subset of real attack data, which is optimized for better visual presentation. Customer information has been removed for privacy
20.8.2026 / (c) René Müller
9

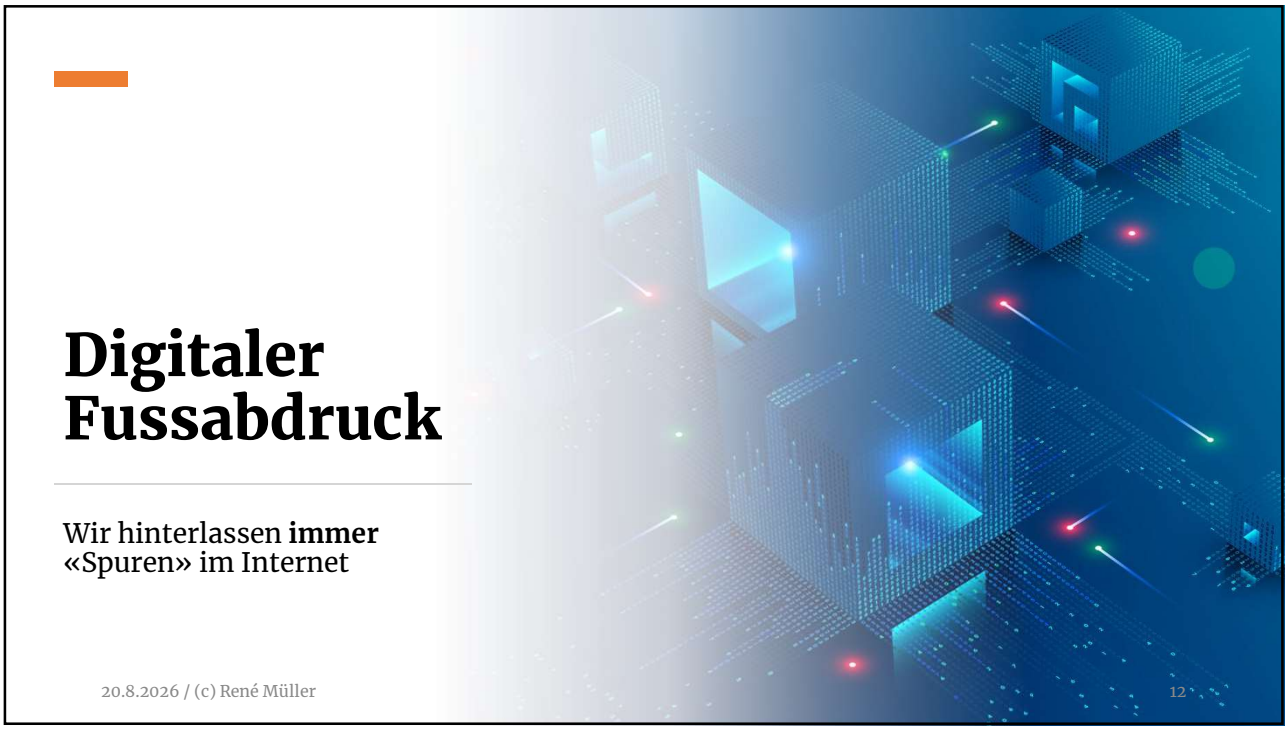
9


Bundesverwaltung
EFD
NCSC
Startseite Melden Kontakt Medien Übersicht
DE FR IT EN
Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra
Nationales Zentrum für Cybersicherheit
NCSC
Aktuell
Cyberbedrohungen
Informationen für
NCS Strategie
Dokumentation
Über NCSC
Herzlich Willkommen
im Nationalen Zentrum
für Cybersicherheit NCSC
Informationen für
Melden Sie uns
Private
Unternehmen
Behörden
IT-Spezialisten
einen Cybervorfall
eine Schwachstelle
20.8.2026 / (c) René Müller
10

10


Aufgetretene Sicherheitsprobleme in den letzten zwölf Monaten
In % der Internetnutzerinnen -nutzer (in den letzten 12 Monaten)
2021
2025
0%
20%
40%
60%
80%
Spam
Erhalt von betrügerischen Nachrichten
Umleitung auf gefälschte Internetseiten, wo persönliche Informationen erfragt werden
Hacking des Profils auf sozialen Netzwerken oder des E-Mail-Kontos und unbemerkte Veröffentlichung oder Versand von Inhalten
Identitätsdiebstahl
Finanzielle Verluste
Belästigung, Diskriminierung oder Mobbing
Verlust von Dokumenten wegen einem Virus oder einer anderen Infektion
Datenstand: 05.12.2025
Quelle: BFS – Omnibus IKT
gr-d-16.04-30110a-ind
© BFS 2025
20.8.2026 / (c) René Müller
TERZO DIETIKON
Dig[iT]reff
11

11


Digitaler Fussabdruck
Wir hinterlassen immer «Spuren» im Internet
20.8.2026 / (c) René Müller
12

12

Digitaler Fussabdruck

Der digitale Fussabdruck sind alle Spuren, die wir im Internet hinterlassen, also unsere «Geschichte» im Internet:

- **Aktivitäten und Aktionen** (z.B. Einkäufe, Suchen auf Google, Hotel buchen etc.)
- **Beiträge** (z.B. Posts auf Facebook, Bilder teilen, Einträge in Foren etc.)
- **Kommunikation** (z.B. WhatsApp, E-Mails an Kollegen, etc.)

Was sie mit dem Browser machen, wird mit Hilfe von «**Cookies**» gespeichert. Andere Aktivitäten werden in Datenbanken gespeichert.

13

Digitaler Fussabdruck

- **Passiver Fussabdruck:** Daten, die gesammelt gespeichert und analysiert werden, ohne dass wir es wissen (Präferenzen, gekaufte Produkte, Standort, etc.)
- **Aktiver Fussabdruck: Informationen oder Daten, die bewusst von uns eingegeben oder verbreitet werden** (z.B. Posts auf Facebook, Einträge in Foren, Angaben in Benutzer-Accounts etc.)

14

Digitaler Fussabdruck: Cookies

- **Cookies** verfolgen unsere Aktivitäten im Internet und die so gesammelten Informationen werden gespeichert und analysiert. Es gibt verschiedene Arten von Cookies
- **Session-Cookies:** Sind nur aktiv, wenn eine Person gerade auf einer Website etwas macht. Werden danach gelöscht
- **Authentifizierungs-Cookies:** Sie verfolgen, ob ein Benutzer gerade angemeldet ist, und unter welchem Namen
- **Tracking-Cookies:** Sie sammeln langfristig Daten über eine Person (erkennbar über die IP-Adresse und/oder Authentifizierungs-Cookies) über mehrere Besuche auf einer Webseite

15

Digitaler Fussabdruck: Webseiten und Shops

Online Händler verfolgen mit Cookies, was ich kaufe, was ich auf die Merkliste legen, was ich im Warenkorb habe und auch, auf welche Website ich als nächstes gehe.

Mit der Zeit entsteht ein klares Bild von mir und dem was ich gerne kaufe. Diese Daten werden genutzt, um gezielt Werbung zu machen.

16

Digitaler Fussabdruck: Webseiten und Shops

Beispiel:

- Letzte Woche wollte ich eine Waage kaufen, und habe auf verschiedenen Websites gesucht. Seitdem sehe ich Werbung für Waagen auf vielen Webseiten, die ich besuche. Warum? Weil diese Webseiten mich erkennen, und weil mein Fussabdruck sagt: René will eine Waage kaufen!

17

Digitaler Fussabdruck: Webseiten und Shops

Beispiel 2:

- Gruselig: Wenn es Amazon schon vor dir weiss, wenn du schwanger bist
- «Von wegen Datenschutz – Amazon kann mehrere hundert Millionen Menschen weltweit gleichzeitig beobachten, analysieren, vergleichen. Und nutzt dieses Können schonungslos aus.»
- Schwangere Frauen kaufen anders – Amazon weiss dies und schlägt ihnen die «passenden» Produkte vor
- Dokumentation auf Youtube:
  Alexa: Wie mächtig ist Amazon? | WDR Doku

18

Digitaler Fussabdruck: Soziale Medien

- Alles was ich irgendwo auf Facebook, Instagram, TikTook schreibe, teile, like (auch wenn es privat ist) hinterlässt eine Spur. Auch wenn ich etwas lösche, und nicht mehr sehe, ist es nicht verschwunden, nur versteckt!
- Es ist darum sehr wichtig, in sozialen Medien die richtigen Privatsphäre-Einstellungen zu kennen und zu wählen.

19

Digitaler Fussabdruck: Geräte

- Viele Websites erkennen und speichern, mit welchen Geräten ich eine Website besuche.
- Über den Standort können Websites ziemlich lückenlos nachvollziehen, wo ich gerade bin, und auch wann ich meistens zu Hause oder bei der Arbeit bin.
- Vorteile: Wenn z.B. Google merkt, dass ich mich von einem Gerät einlogge, das Google noch nicht «kennt», bekomme ich eine Warnung.
- Nachteile: Nichts mehr ist «privat» oder «geheim»

20

Digitaler Fussabdruck: Nutzung

Der Fussabdruck wird von verschiedenen Gruppen für verschiedene Zwecke verwendet:

- von Strafverfolgungsbehörden: zur Lieferung von Informationen, z.B. Standort, Präferenzen, Kontakte
- Von Marketingabteilungen: um herauszufinden, an welchen Produkten ein Benutzer interessiert ist, oder um sein Interesse an einem bestimmten Produkt aufgrund ähnlicher Interessen zu wecken.
- von Personalverantwortlichen (HR): Interviewer könnten Bewerber auf der Grundlage ihrer Online-Aktivitäten recherchieren
- Siehe Google Search Console (►Beispiel)

21

Daten im Internet löschen: Historie

- Die Historie (Verlauf) zeigt, welche Seiten Sie im Internet besucht haben.
- Im Browser (►Einstellungen):

→ Hauptmenü (3 Punkte in der oberen rechten Ecke)

→ Einstellungen

→ Datenschutz, Suche und Dienste

→ Privater Modus:

Wenn Sie im privaten Modus browsen wird die Historie gelöscht, sobald sie das Fenster schliessen.

23

Cookies und Browserverlauf löschen

- Edge

1. Drei Punkte oben rechts → Einstellungen → Datenschutz… → Browserdaten löschen

- Google Chrome

1. Bei der Menüleiste oben auf Verlauf klicken → Gesamtverlauf anzeigen
2. Browserverlauf, Cookies und andere Webseitendaten auswählen und löschen

- Safari

1. Bei der Menüleiste oben auf Verlauf klicken → Verlauf löschen

Privates Surfen

Falls Sie nicht möchten, dass ihre Aktivitäten gespeichert werden:

- Edge

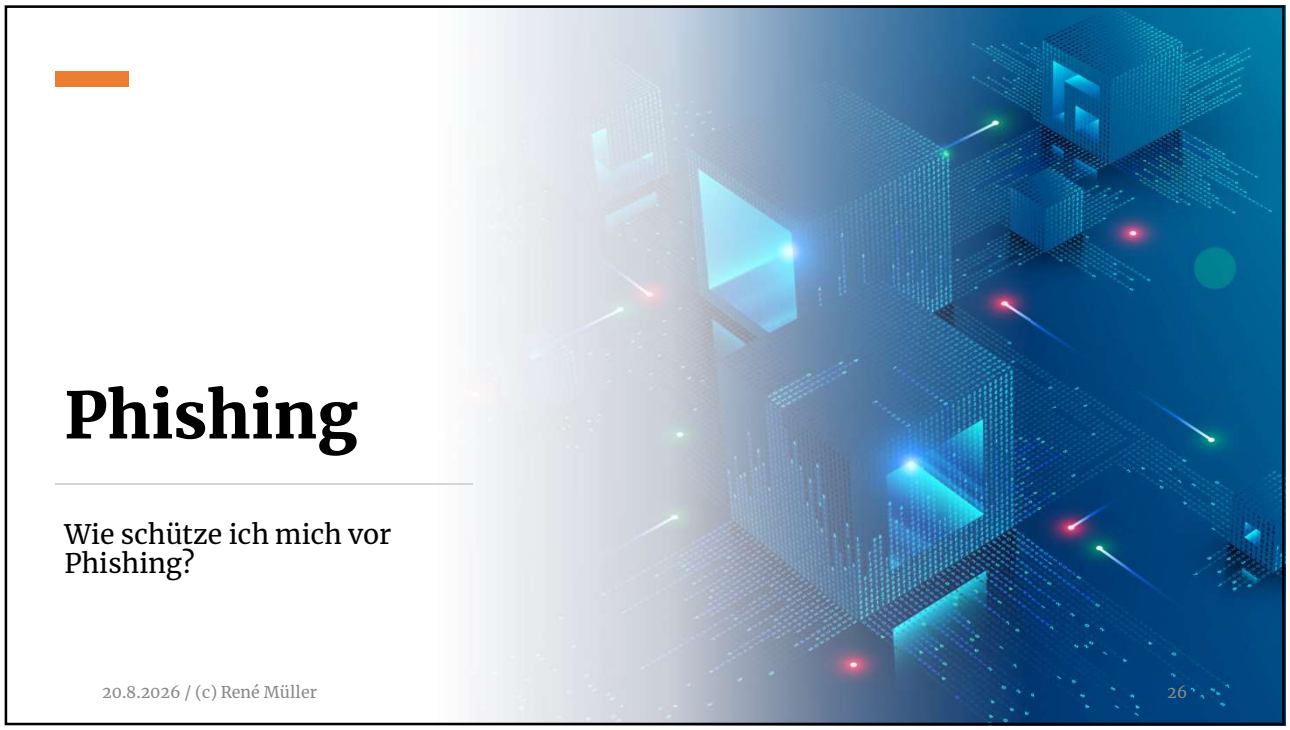
Oben rechts drei Punkte → Neues InPrivate-Fenster

- Google Chrome

Klicken Sie rechts oben auf das Dreipunkt-Menü → Neues Inkognitofenster → Ein neues Fenster wird geöffnet. Links oben befindet sich das Inkognitosymbol

- Safari

→ Ablage → Neues Privates Fenster



26

Was ist Phishing?

- Phishing ist eine Form des Online-Betrugs, bei der Angreifer versuchen, vertrauliche Informationen wie Passwörter, Kreditkarteninformationen oder Bankdaten von Internetnutzern zu erlangen.
- Sie tun dies in der Regel, indem sie sich als vertrauenswürdige Personen oder Unternehmen ausgeben, z.B. als Bankmitarbeiter oder auch als Online-Shop und bitten die Nutzer in E-Mails oder über Soziale Netzwerke um diese Informationen.
- Oft enthalten diese Nachrichten Links, die auf gefälschte Websites führen, die so gestaltet sind, dass sie täuschend echt aussehen und die Nutzer dazu verleiten, ihre Informationen einzugeben.
- **Es ist wichtig, dass man niemals auf solche Links klickt und auf solche Anfragen nicht reagiert, um sich vor Phishing-Angriffen zu schützen.**

28

Keine seriöse Institution würde von Ihnen (per Mail, SMS oder Telefon) folgende Informationen verlangen:

- Kreditkartennummer
- Kontonummer
- Ausweisnummer
- Passwort
- vollständiger Name

(Quelle: Stadtpolizei Zürich)

29

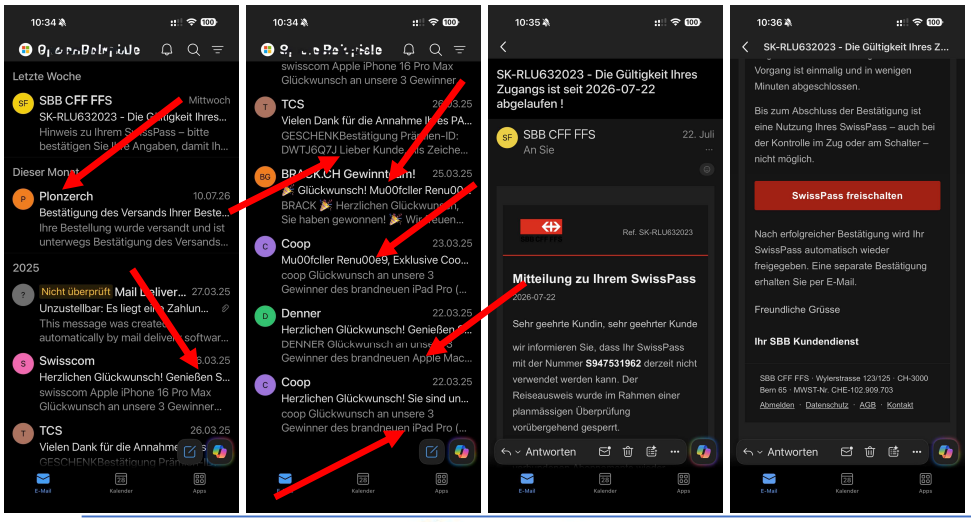
Warnsignale: Das sollte Sie stutzig machen

- Begrüssung: Steht nur «sehr geehrter Kunde» oder werden Sie persönlich mit Namen angesprochen?
- Vortäuschen von Dringlichkeit: Wird in der Nachricht mit einer Kontosperrung oder ähnlichem gedroht, falls Sie nicht sofort reagieren?
- Links: Ist der Link verdächtig? Erscheint eine andere URL anstelle des Links, wenn Sie mit der Maus darauf fahren? Achtung: Nicht klicken.
- Sprache: Hat es grammatikalische und orthografische Fehler im Text?

(Quelle: Stadtpolizei Zürich)

30

Phishing -Beispiele



31

Phishing -Beispiele

32

Was schützt Sie vor Phishing?

- Seien Sie misstrauisch.
- Antworten Sie auf keinen Fall auf eine verdächtig erscheinende Nachricht.
- Klicken Sie auf keine verdächtigen Links, öffnen Sie keine verdächtigen Anhänge. Am besten löschen Sie die Nachricht gleich.
- Geben Sie niemals vertrauliche Daten per Mail, via Websites/Online-Formulare oder telefonisch bekannt.
- Kontrollieren Sie regelmässig Ihre Kreditkartenabrechnungen und Bankauszüge.
- Schützen Sie Ihren Computer mit Antiviren-Programmen und mit regelmässigen Updates (auch Handy)
- Bei Verdacht auf Betrug wenden Sie sich an die Polizei oder an BACS, dem Bundesamt für Cybersicherheit.

33

Phishing (LINDA)

34

LINDA

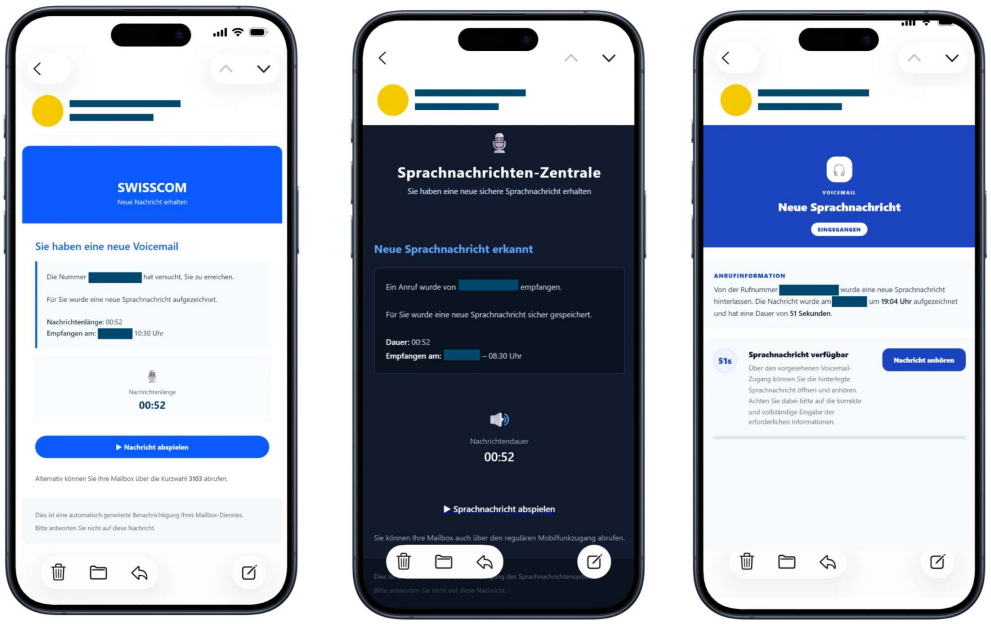
L = Links und Anhängen misstrauen
I = Inhalte kritisch prüfen
N = Neutrale Anrede anzweifeln
D = Dringlichkeit hinterfragen
A = Absender überprüfen

35

E-Mail «Neue Sprachnachricht» ist Phishing

- Betrüger versenden E-Mails, in denen sie behaupten, dass eine neue Sprachnachricht bereitstehe. Damit versuchen sie, an Zugangsdaten von persönlichen Benutzerkonten zu gelangen.
- Die E-Mails geben vor, von Swisscom oder einem Mailbox-Dienst zu stammen, und informieren über eine angeblich neue Sprachnachricht. Um diese anzuhören, sollen die Empfänger auf Schaltflächen wie «Nachricht abspielen», «Nachricht anhören», «Sprachnachricht abspielen» oder «Mitteilung öffnen» klicken

38



39

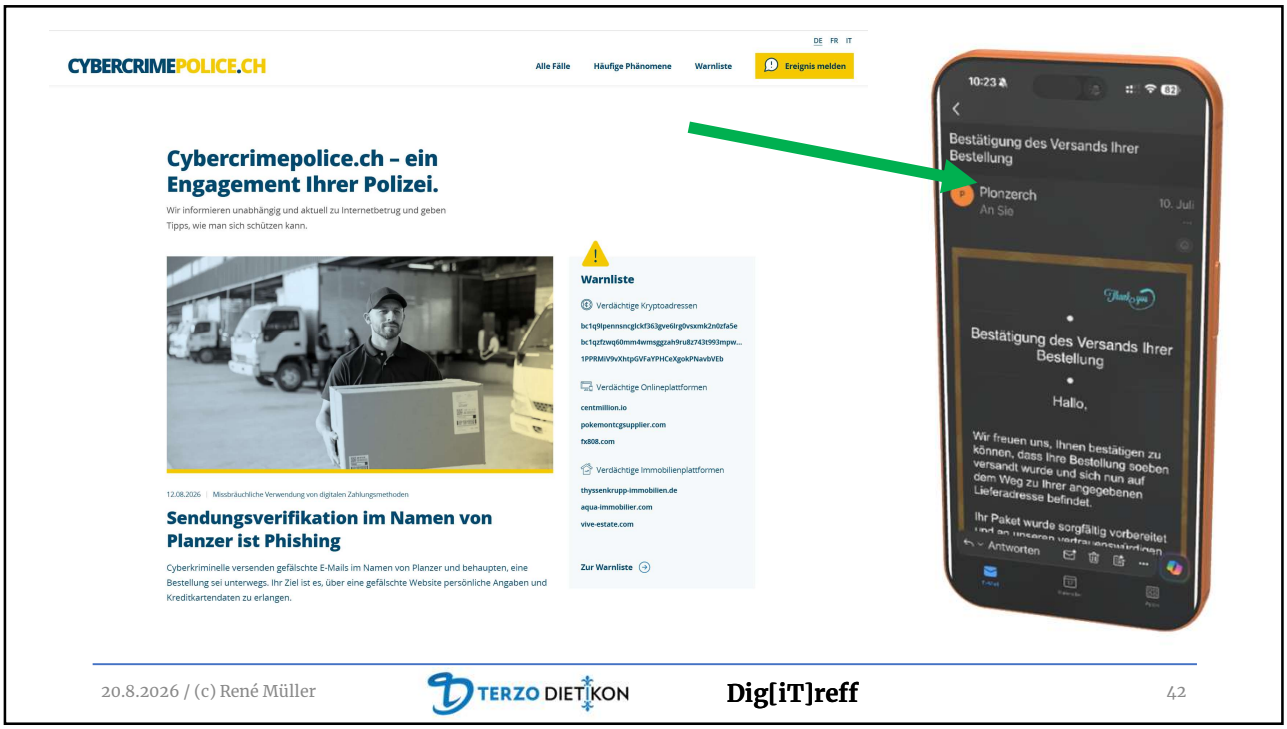
E-Mail «Neue Sprachnachricht» ist Phishing

- Wer dem Link folgt, gelangt nicht zu einer echten Swisscom-Seite, sondern auf eine betrügerische Webseite. Dort werden meist Zugangsdaten für E-Mail-Konten oder andere Online-Dienste abgefragt. In einem weiteren Schritt versuchen die Betrüger zudem, den Zwei-Faktor-Authentifizierungscode (2FA-Code) abzufangen, um die Konten zu übernehmen.

40


antiphishing.ch
Startseite
Informationen
Kontakt
Haben Sie eine Phishing-Seite gefunden?
Melden Sie Phishing-Seiten via Web-Formular:
URL ...
MELDEN
Haben Sie ein Phishing E-Mail erhalten?
Leiten Sie Phishing E-Mails weiter an
reports@antiphishing.ch
Achtung: Diese Mailbox wird nicht gelesen sondern maschinell verarbeitet. Falls Sie eine Anfrage haben und / oder eine Antwort des Bundesamt für Cybersicherheit (BACS) wünschen, wenden Sie sich bitte an incidents@ncsc.ch oder verwenden Sie das BACS Meldeformular.
rund eine Million Meldungen pro Jahr
20.8.2026 / (c) René Müller
TERZO DIETIKON
Dig[iT]reff
41

41


CYBERCRIMEPOLICE.CH
Alle Fälle
Häufige Phänomene
Warnliste
Ereignis melden
Cybercrimepolice.ch – ein Engagement Ihrer Polizei.
Wir informieren unabhängig und aktuell zu Internetbetrug und geben Tipps, wie man sich schützen kann.
Warnliste
Verdächtige Kryptoadressen
Verdächtige Onlineplattformen
centmillion.io
pokemontcgsupplier.com
fx808.com
Verdächtige Immobilienplattformen
thyssenkrupp-immobilien.de
aqua-immobilier.com
vive-estate.com
Zur Warnliste
12.08.2026 | Missbräuchliche Verwendung von digitalen Zahlungsmethoden
Sendungsverifikation im Namen von Planzer ist Phishing
Cyberkriminelle versenden gefälschte E-Mails im Namen von Planzer und behaupten, eine Bestellung sei unterwegs. Ihr Ziel ist es, über eine gefälschte Website persönliche Angaben und Kreditkartendaten zu erlangen.
Bestätigung des Versands Ihrer Bestellung
Plonzerch
An Sie
Bestätigung des Versands Ihrer Bestellung
Hallo,
Wir freuen uns, Ihnen bestätigen zu können, dass Ihre Bestellung soeben versandt wurde und sich nun auf dem Weg zu Ihrer angegebenen Lieferadresse befindet.
Ihr Paket wurde sorgfältig vorbereitet
Antworten
20.8.2026 / (c) René Müller
TERZO DIETIKON
Dig[iT]reff
42

42

Falscher Support-Anruf

- Wer einen Anruf von einem technischen Support erhält, sollte vorsichtig sein. Immer öfter geben sich Betrüger als Mitarbeitende eines Kunden_ dienstes aus und bieten ihre Hilfe an. Wer nicht aufpasst, verliert die Kontrolle über den Computer und die Bankkonten.
- Häufig geben sie sich beispielsweise als Mitarbeiter einer IT-Firma aus und erklären, dass der Computer von Viren befallen sei und repariert werden müsse. Oder sie behaupten, beim Kundendienst einer Bank zu arbeiten und verdächtige Transaktionen festgestellt zu haben.

43

Falscher Support-Anruf

Wie funktioniert der Betrug?

- Die Betrüger versuchen ihre Opfer dazu zu bringen, ein Programm herunterzuladen, damit sie mittels Fernzugriff die Kontrolle über den Computer übernehmen können. Sobald das Programm installiert ist, erhalten die Angreifer direkten Zugriff auf das Gerät und können es manipulieren. So können sie etwa Passwörter abfangen oder Daten herunterladen.
- Besonders dreist: Sie erklären, dass ihre Hilfe kostenpflichtig sei. Danach wollen sie ihren Opfern eine Software-Lizenz oder eine Dienstleistung verkaufen. Dazu fragen sie nach den Kreditkarteninformationen. Auch diese Kreditkartendaten werden anschliessend missbraucht.

44

Falscher Support-Anruf

Wieso sind die Betrüger erfolgreich?

- Die Angreifer lösen mit ihrem Anruf und ihren sicherheitsrelevanten Behauptungen eine Stresssituation aus. Sie treten ruhig und professionell auf, drängen auf sofortiges Handeln – und bieten eine prompte Lösung für das Problem an.
- Dank technischer Manipulation (Spoofing) erscheint auf dem Display der Opfer zudem meist eine scheinbar offizielle und unverdächtige Schweizer Telefonnummer oder sogar der Name der Bank oder des IT-Anbieters. Das schafft Vertrauen – zu Unrecht.

45

Falscher Support-Anruf

Wie kann man sich schützen?

- Grundsätzlich gilt: Niemand ruft unangemeldet und unaufgefordert an, um Computerprobleme zu beheben. Brechen Sie solche Anrufe sofort ab. Wichtig: Sie können der angezeigten Telefonnummer nicht trauen.
- Lassen Sie niemanden auf Ihren Computer zugreifen.
- Geben Sie keine persönlichen Daten wie Passwörter oder Kreditkartennummern an andere Personen weiter.

46

Fake-Shops

Wie schütze ich mich vor falschen Online-Shops?

47

Schutz vor Fake-Shops

Die meisten Fake-Shop-Fälle weisen ähnliche Warnsignale auf, die Verbraucher vor dem Kauf überprüfen können:

- **Übertriebene Rabatte:** Produkte, die deutlich unter Marktpreis angeboten werden, sind fast immer ein Risiko.
- **Webadresse und Impressum:** Oft sind die Webadressen leicht verschlüsselt, etwa durch Tippfehler oder Zusätze (-*switzerland*, -*zurich*). Das Impressum fehlt oder ist unvollständig – etwa ohne Adresse oder Kontakt.

48

Schutz vor Fake-Shops

- **Zahlungsmethoden:** Nur Vorauszahlung per Kreditkarte oder Banküberweisung möglich, kein PayPal, keine Käuferschutzsysteme.
- **Bewertungslage:** Fehlende oder gefälschte Nutzerbewertungen; häufig nur positive Rezensionen, die auf Plattformen wie Trustpilot entlarvt werden können.

49

Prüfen vor dem Bestellen

Webadresse prüfen: Betrüger versuchen oft, die Webadresse/den Domainnamen zu verschlüsseln, mit sogenannten Subdomains. Etwa die Webadresse ***www.TERZO-Dietikon.ch.fakeshop.to*** oder hätte mit TERZO nichts zu tun, sondern würde zu *fakeshop.to* führen, da dies das eigentliche Ziel wäre. Die Webadresse ist oft so lang (*Tolle.Artikel.auf.pctipp.ch.kaufen.fakeshop.to)*, dass Nutzer das Ende in der Adresszeile nicht lesen können. Klicken Sie im Browser daher bei der Adresszeile die *Webseiteninformationen* an. Im Fenster, das sich nun aufklappt, wird das eigentliche Ziel angezeigt.

50

Prüfen vor dem Bestellen

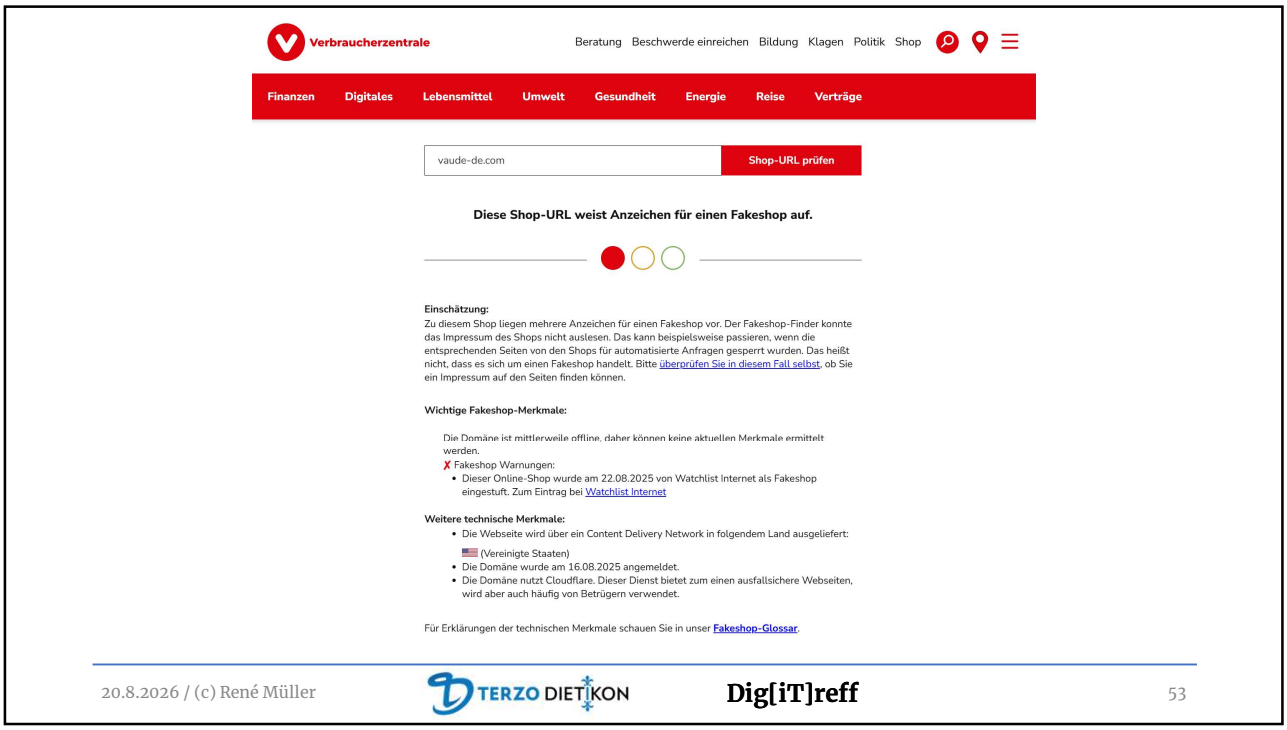
- **Bewertungen und Kundenmeinungen:** Fragen Sie die Google-Suche nach dem Shop und prüfen Sie Erfahrungsberichte auf Portalen wie Trustpilot (de.trustpilot.com) oder in den Google-Rezensionen, die in der Google-Suche bei vielen Anbietern auftauchen. Meist reicht die Suche nach **fakeshopadresse**
- **Erfahrungen Meinungen**. Nicht jeder Shop hat immer Einträge bei Trustpilot oder anderen Portalen. Aber meistens wird man so am schnellsten fündig,

51

Prüfen vor dem Bestellen

- **CH-Firmencheck bei Zefix.ch:** Der zentrale Firmenindex zefix.ch zeigt Ihnen schnell, ob es ein im Impressum genanntes Unternehmen gibt oder nicht. Aber Achtung: Bei gefälschten Web-Stores ist das Impressum auch oft von einem Originalmarkenshop kopiert.
- **Hören Sie auf Ihr Bauchgefühl:** Sehr oft finden Nutzer eine Seite seltsam, die Preise sind verlockend niedrig und es wird alles getan, um das Geschäft so schnell wie möglich abzuschliessen. Vertrauen Sie auf Ihre Instinkte.
- **Probieren Sie den Fakeshop-Finder der Verbraucherzentrale.de:** Der Finder unter verbraucherzentrale.de/fakeshopfinder arbeitet im Hintergrund mit KI und kennt sehr viele gefälschte Shops. Geben Sie dort einfach die Internetadresse des Shops ein und die Adresse wird analysiert.

52



53

Prüfen vor dem Bestellen

- **Auch Watchlist-Internet.at ist gut:** Auf dem Service watchlist-Internet.at lassen sich Adressen von Shops prüfen. Alle aktuellen Fake-Shops zeigt das Tool in einer Liste an. Pro Tag kommen hier mal schnell 100 Warnungen zusammen. Oft ist es ein Fake-Shop, der gleich fünf oder sechs Varianten einer Webadresse ausnutz.

54


Watchlist Internet
Internet-Betrug, Fallen und Fakes im Blick
Internetfalle melden
Warnungen & Tipps
Unseriöse Webseiten
Services & Tools
Über uns
Ich suche nach ...
Suchen
Startseite / Unseriöse Webseiten / Betrügerische Online-Shops
Liste Fake-Shops/betrügerische Online-Shops
Jeden Tag tauchen zahlreiche neue Fake-Shops auf. Wer dort bestellt, erhält trotz Bezahlung nichts oder etwas, das nicht dem beworbenen Produkt entspricht. So schützen Sie sich vor Fake-Shops.
Die Liste wird laufend aktualisiert. Es gelten die Nutzungsbedingungen der Watchlist Internet. Sind Sie auf einen Fake-Shop gestoßen, der hier nicht auftaucht? Informieren Sie uns über das Meldeformular.
Geben Sie einen Suchbegriff ein.
Suche
Suchen Sie nach einem Online-Shop, um herauszufinden, ob wir vor diesem warnen.
24365 Treffer
beckludwig.com
bestwassertechnik.com
baumaterialstore.com
Seit 03.08.2026 gelistet
Betrügerische Shops
Mehr Infos
20.8.2026 / (c) René Müller
TERZO DIETIKON
Dig[iT]reff
55

55


Diverse Betrügereien
Auf was kann oder soll ich auch noch achten?
20.8.2026 / (c) René Müller
56

56

Manipulierte QR-Codes an Schweizer Parkuhren

Die Betrüger nutzen die Tatsache aus, dass viele Menschen heutzutage Parkgebühren lieber mit dem Handy als mit Bargeld bezahlen. Um die Autofahrer gezielt zu täuschen und finanziell auszubeuten, überkleben sie die QR-Codes auf den Parkuhren mit gefälschten Codes, die zu betrügerischen Bezahlseiten führen. Diese manipulierten QR-Codes sind den offiziellen Designs täuschend ähnlich und optisch so gut nachgemacht, dass sie auf den ersten Blick kaum von den Originalen zu unterscheiden sind.

57

Öffentliches WLAN

- So offen ein WLAN ist, so offen sind beim Surfen
- auch Ihre persönlichen Daten.
- Öffentliche WLANs sind häufig unverschlüsselt und kaum geschützt. Das nutzen Cyberkriminelle gezielt aus und greifen darauf zu.
- Ist das WLAN unverschlüsselt, sind Ihre Daten für andere Personen im gleichen Netz sichtbar. So können Kriminelle relativ einfach Ihre Passwörter, Kreditkartendaten und persönliche Nachrichten mitlesen.

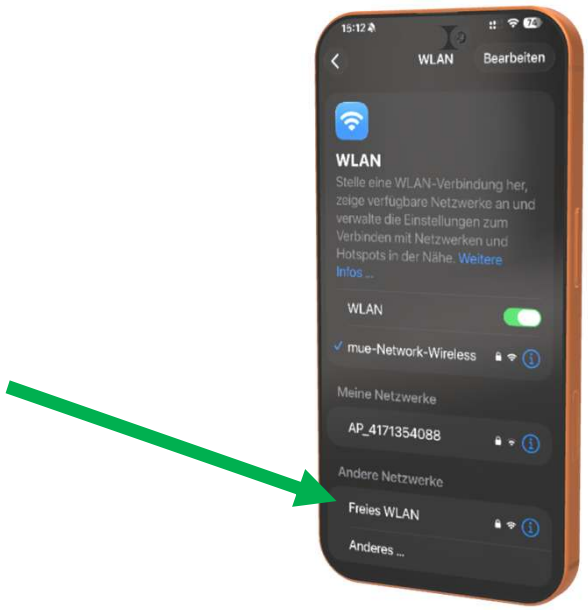
58

Tipps fürs Surfen im öffentlichen WLAN

- Verbinden Sie sich nur mit einem öffentlichen WLAN, wenn Sie den Anbieter kennen und dieser vertrauenswürdig ist. Fragen Sie im Zweifel vor Ort nach dem offiziellen WLAN.
- Verbinden Sie sich keinesfalls mit einem WLAN, wenn Sie den Anbieter nicht kennen.
- Verzichten Sie darauf, über das öffentliche WLAN sensible Dienste wie Online-Banking zu nutzen.
- Nutzen Sie für sensible Dienste besser Daten (Mobilfunknetz) als öffentliches WLAN.
- Aktualisieren Sie die Software Ihrer Geräte regelmässig, damit die neuesten Sicherheitsstandards aktiv sind.

Wirklich sicher sind Sie in öffentlichen WLANs nur, wenn Sie Ihre Daten selbst verschlüsseln. Die sicherste Lösung: Verschlüsseln Sie Ihre Daten mit VPN

59



60

Öffentliche USB-Ladestationen

- Meiden Sie öffentliche USB-Ladestationen. Manipulierte oder defekte Stecker können Geräte beschädigen oder mit Schadsoftware infizieren (Juice Jacking). Verwenden Sie besser Ihr eigenes Ladegerät – idealerweise in Kombination mit einer Powerbank. Das ist eine grosse Batterie, mit der Sie beispielsweise Ihr Smartphone aufladen können.
- Smartphone - USB-Ladestationen: Gefahr aus der Dose - News - SRF

61

Passwörter

Wie schütze ich meine Zugangsdaten?

62

Passwort wählen

- Variante 1: Sie können sich mit ihrem Google Konto oder Ihrer Apple-ID registrieren → Es braucht kein neues Passwort
  -> dann tracken diese Firmen aber ihre Aktivitäten !!!
- Variante 2: Lassen Sie ihren Browser (Firefox, Chrome) oder ihr System ein automatisches Passwort generieren
  -> lässt sich meistens nicht leicht merken !!!
- Variante 3: Wählen Sie selber ein Passwort → Speichern Sie das Passwort in ihrem Browser oder schreiben Sie es auf.
  -> ist jedoch beides nicht sicher und nicht zu empfehlen -> siehe später
- Passwort-Feld ist immer unsichtbar (....), kann aber angezeigt werden Beim Wiederholen hilfreich

63

Wie wählt man ein starkes Passwort?

- Länge: Ein Passwort sollte aus mind. 10 Zeichen bestehen.
- Verwenden Sie Ziffern, Buchstaben und Sonderzeichen.
- Verwenden Sie Klein- und Grossschreibung.
- Um ein starkes (und somit schwer zu merkendes) Passwort nicht zu vergessen, bauen Sie sich am besten eine Eselsbrücke.
- Beispiel: Passwort:
  Eselsbrücke: Mein Hund heisst Bello und ist 3 Jahre alt. MHhB&i3Ja
- Oder: XyzHansMuster1954$ erste 3 Buchstaben=Firma, fixer Teil

  z.B. MigHansMuster1954$ bei Migros.ch
  CopHansMuster1954$ bei Coop.ch
  UbsHansMuster1954$ bei Ubs.ch

64

Wenn Sie selber ein Passwort wählen, was ist wichtig?

- Wählen Sie sichere Passwörter.
- Halten Sie Ihre Passwörter geheim. Geben Sie diese nie einer anderen Person bekannt.
- Passwörter sollten regelmässig geändert werden.
- Schreiben Sie Ihre Passwörter nicht auf und speichern Sie sie auch nicht unverschlüsselt.

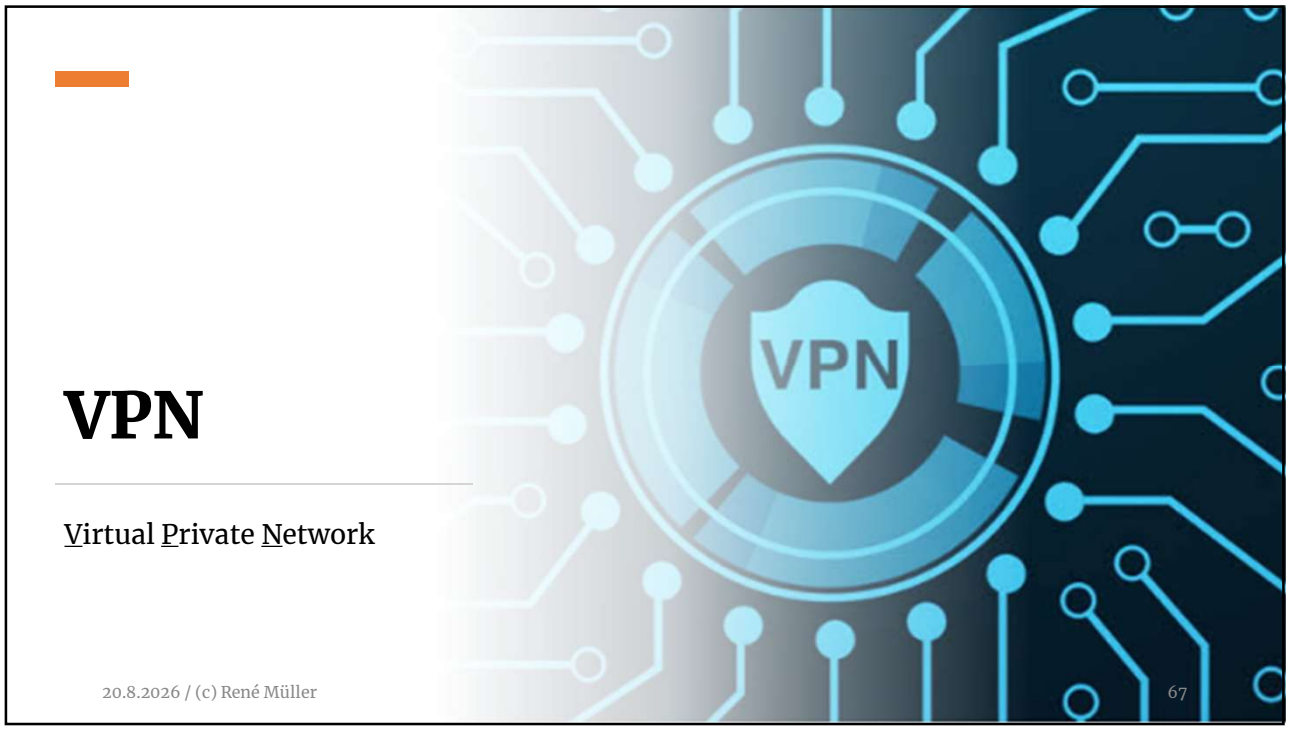
(Quelle: Stadtpolizei Zürich)

65

Oder sie nutzen einen Passwort-Manager

- Wir empfehlen Ihnen den «Proton Pass»
- Kostenlos und ohne Werbung
- Sehr einfach auf mehreren Plattformen nutzbar
- CH-Firma
  - Hinter Proton Pass steckt die Proton AG, ein Schweizer Unternehmen mit Sitz in Plan-les-Ouates bei Genf. Die Firma wurde 2014 von einem Team aus Wissenschaftlern gegründet, die sich am CERN kennengelernt hatten. Bekannt ist das Unternehmen vor allem für seinen sicheren E-Mail-Dienst Proton Mail sowie Proton VPN.
- Siehe auch weiter unten bei VPN

66



VPN

Virtual Private Network

67

VPN – ein «privater Tunnel» durchs Internet

Stell dir vor, du sitzt in einem Café und benutzt das öffentliche WLAN.

- **Ohne VPN:**
  - **iPhone/PC → Café-WLAN → Internet → Webseite**
  - Deine Internetverbindung läuft dabei über den Internetanbieter bzw. das verwendete Netzwerk. Die besuchte Webseite sieht normalerweise auch die **öffentliche IP-Adresse**, über die du ins Internet gehst.
- **Mit VPN:**
  - **iPhone/PC → 🔒 verschlüsselter VPN-Tunnel → VPN-Server → Internet → Webseite**
  - Das VPN – **Virtual Private Network** – baut also zunächst eine verschlüsselte Verbindung zu einem VPN-Anbieter auf. Erst von dort geht es weiter zur gewünschten Webseite.
- Der wichtige Punkt dabei: **VPN bedeutet nicht anonym und auch nicht automatisch sicher.** Man verschiebt einen Teil des Vertrauens vom Internetanbieter bzw. lokalen Netzwerk zum VPN-Anbieter.

68

Was bringt mir das konkret?

- 🔐 **Verschlüsselung:** Der Datenverkehr zwischen deinem Gerät und dem VPN-Server wird verschlüsselt.
- 🧿 **Unterwegs:** Gerade in fremden oder öffentlichen Netzwerken kann ein VPN eine zusätzliche Schutzschicht bieten.
- 🌍 **Andere IP-Adresse:** Webseiten sehen grundsätzlich die IP-Adresse des VPN-Servers statt deiner normalen öffentlichen IP-Adresse.
- 🏠 **Zugriff nach Hause oder in eine Firma:** VPN-Technik kann auch verwendet werden, um von unterwegs sicher auf ein Heim- oder Firmennetzwerk zuzugreifen.
- 📺 **Virtueller Standort:** Bei manchen Diensten kann ein VPN-Server in einem anderen Land den Eindruck erwecken, dass der Internetzugriff von dort erfolgt. Streaminganbieter können VPNs allerdings erkennen oder blockieren.

69

«Schützt mich ein VPN vor Betrügern, Phishing und Viren?»

- Die Antwort lautet: **Nein.**
- Wenn ich auf eine gefälschte Bankseite gehe und dort mein Passwort eingebe, kann die Verbindung dorthin wunderbar verschlüsselt sein – **ich habe mein Passwort trotzdem dem Betrüger gegeben.**
- Ein VPN ersetzt deshalb weder gesunden Menschenverstand noch Updates, Virenschutz, sichere Passwörter oder Zwei-Faktor-Authentifizierung.

70

Brauche ich als Privatperson überhaupt ein VPN?

- Zu Hause im eigenen, ordentlich abgesicherten WLAN ist ein kommerzielles VPN für viele Menschen **nicht zwingend notwendig**. Moderne Webseiten und Apps verwenden ohnehin überwiegend HTTPS und verschlüsseln damit bereits die Kommunikation.
- Ein VPN kann aber sinnvoll sein, wenn man **häufig fremde WLANs verwendet, seine öffentliche IP-Adresse gegenüber Webseiten verbergen möchte, einen bestimmten VPN-Standort benötigt oder sicher auf ein privates Netzwerk zugreifen will.**

VPN macht aus dem Internet keinen sicheren Ort.
Es macht den Weg zwischen meinem Gerät und dem VPN-Server zu einem verschlüsselten Tunnel.

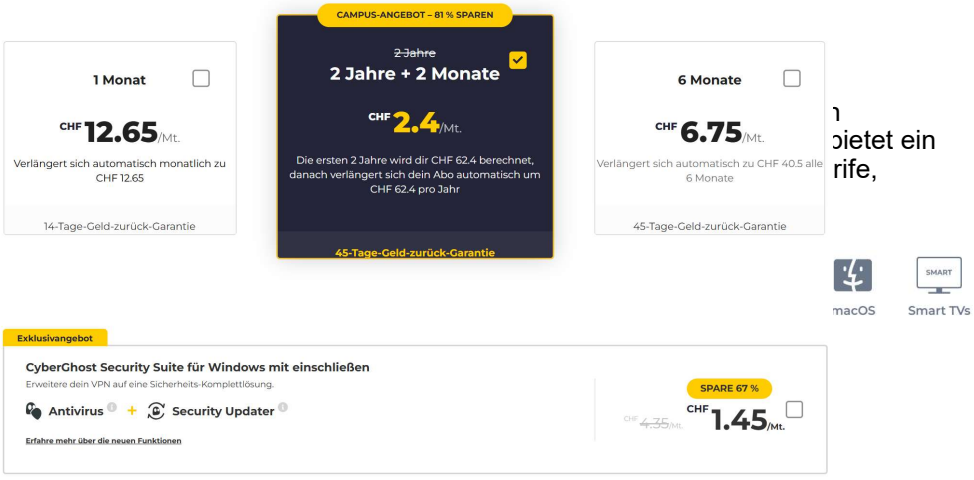
https://WhatIsMyIPAddress.com/

71

Ich n

VPN für mehr Privatsphäre kaufen: 2 Jahre für CHF 2.4 /Monat

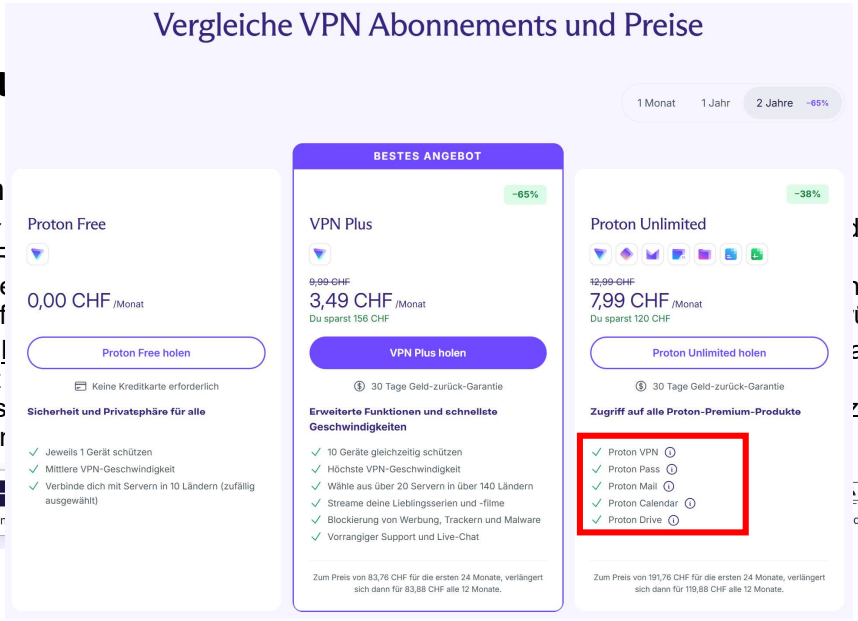
- Cyber
  - Cyb
    unk
    ries
    sch
    Sich



72

Ich nu

- Proton
  - Der CER Date Surf
  - Ja, I gibt Ges Prer



de von

ürdig.

an. Es

zahlenden

d TV Fire TV

73