Seniorenrat Dietikon

Dig[iT]reff 3-2023

Online-Sicherheit

3

Programm 22.2.2023

- Welche sozialen Medien kennt ihr?
- Risiken und Gefahren im Internet
- Digitaler Fussabdruck
- Sicherheit und Privatsphäre in Facebook
- Sicherheit und Privatsphäre in Instagram
- Konten und Spuren im Internet löschen
- Phishing und gefährliche E-Mails und Nachrichten
- Passwörter: Sichere Passwörter wählen und speichern

6

Rolle des Internets und sozialer Medien heute

Das Internet wird immer wichtiger in unserer Gesellschaft, immer mehr Menschen nutzen und soziale Medien und Online-Angebote jeder Art für ...

- Information
- Vernetzung / Freundschaften
- Dienstleistungen

Wegen der steigenden Wichtigkeit müssen wir wissen, welche Folgen und Risiken unsere Online-Aktivitäten haben können.

7

8

9

Risiken und Gefahren von Online-Aktivitäten

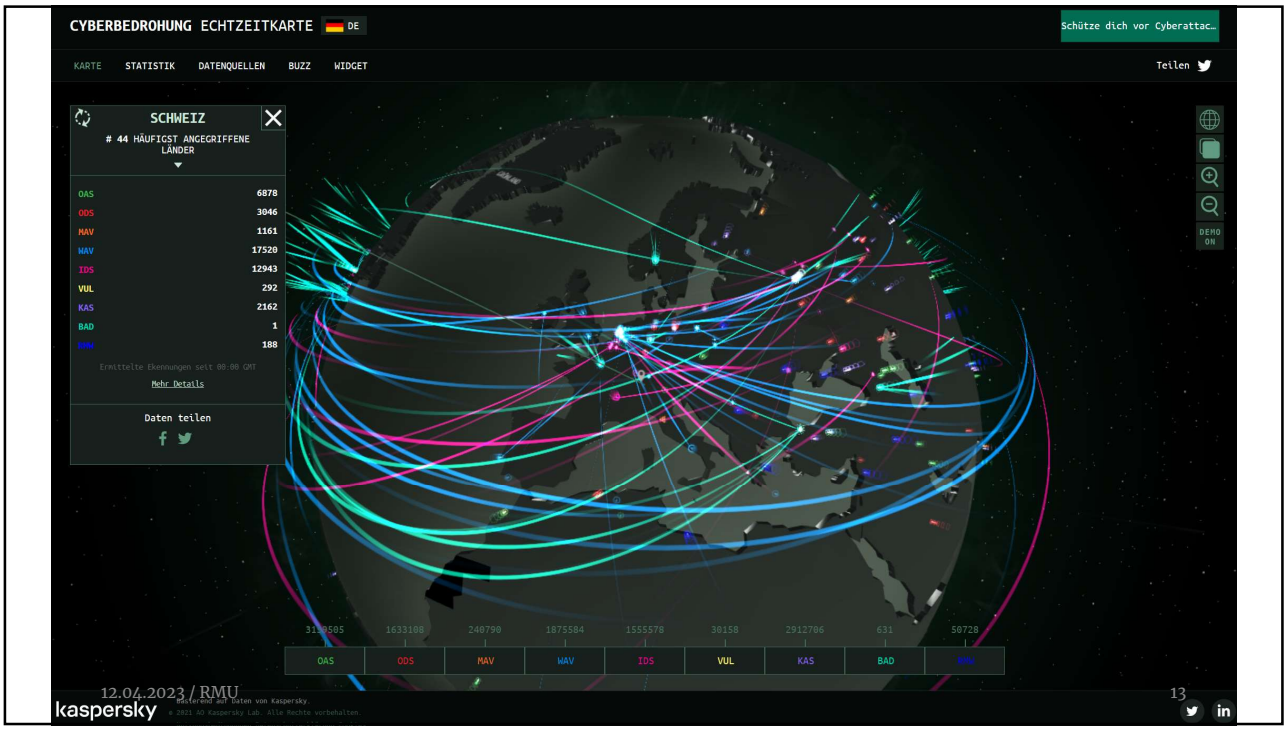
10

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!

Risiken und Gefahren im Internet

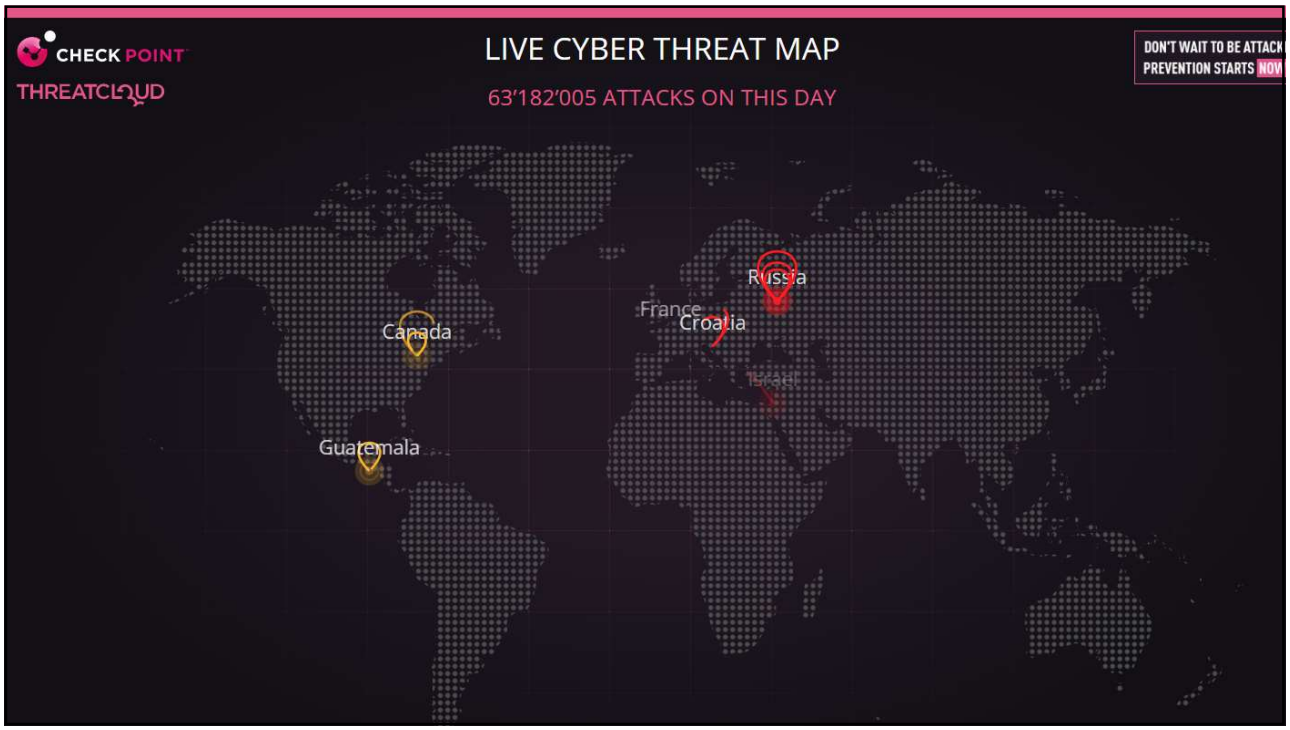
- **Zuverlässigkeit der Informationen:** Viele Personen, vor allem auf Social Media verkaufen ihre Information als Wahrheit. Als User muss man aber sehr kritisch sein, und sich genau fragen: Woher kommt diese Information? Gibt es «Beweise»?
- **Manipulation:** Viele User werden durch Webseiten und soziale 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


CYBERBEDROHUNG ECHTZEITKARTE
DE
Schütze dich vor Cyberattac…
KARTE
STATISTIK
DATENQUELLEN
BUZZ
WIDGET
Teilen
SCHWEIZ
44 HÄUFIGST ANGEGRIFFENE LÄNDER
OAS 6878
ODS 3046
MAV 1161
WAV 17520
IDS 12943
VUL 292
KAS 2162
BAD 1
RMW 188
Ermittelte Ekennungen seit 00:00 GMT
Mehr Details
Daten teilen
DEMO ON
3133505
1633108
240790
1875584
1555578
30158
2912706
631
50728
OAS
ODS
MAV
WAV
IDS
VUL
KAS
BAD
RMW
12.04.2023 / RMU
13
kaspersky
Basierend auf Daten von Kaspersky.
© 2021 AO Kaspersky Lab. Alle Rechte vorbehalten.

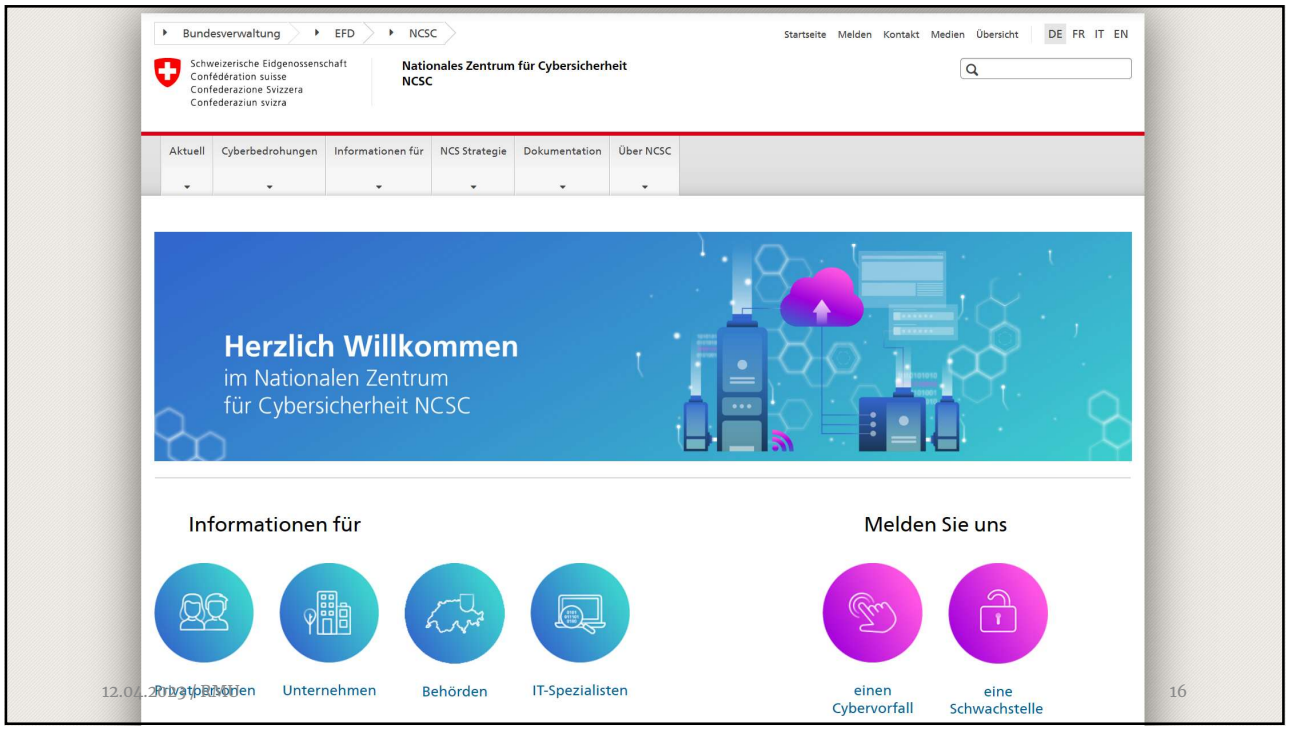
13


[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
12.04.2023 / RMU
14
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

14


CHECK POINT
THREATCLOUD
LIVE CYBER THREAT MAP
63'182'005 ATTACKS ON THIS DAY
DON'T WAIT TO BE ATTACK
PREVENTION STARTS NOW
Russia
France
Croatia
Canada
Guatemala

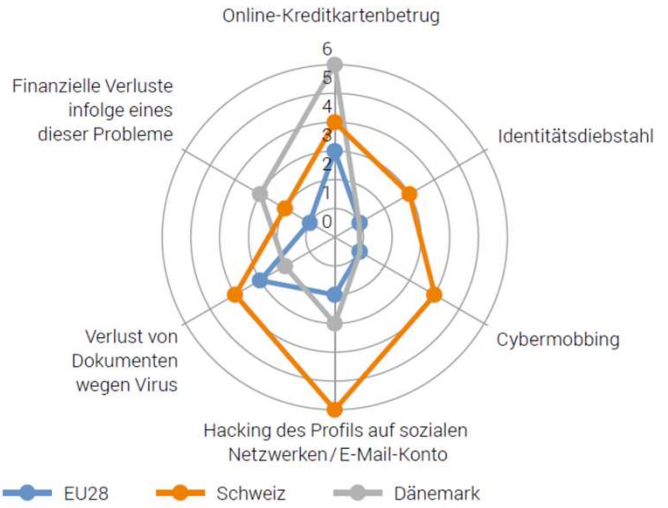
15


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
Unternehmen
Behörden
IT-Spezialisten
einen Cybervorfall
eine Schwachstelle

16

Internetsicherheitsprobleme in den letzten zwölf Monaten, 2019

In % der Bevölkerung (16 – 74 Jahre) G1

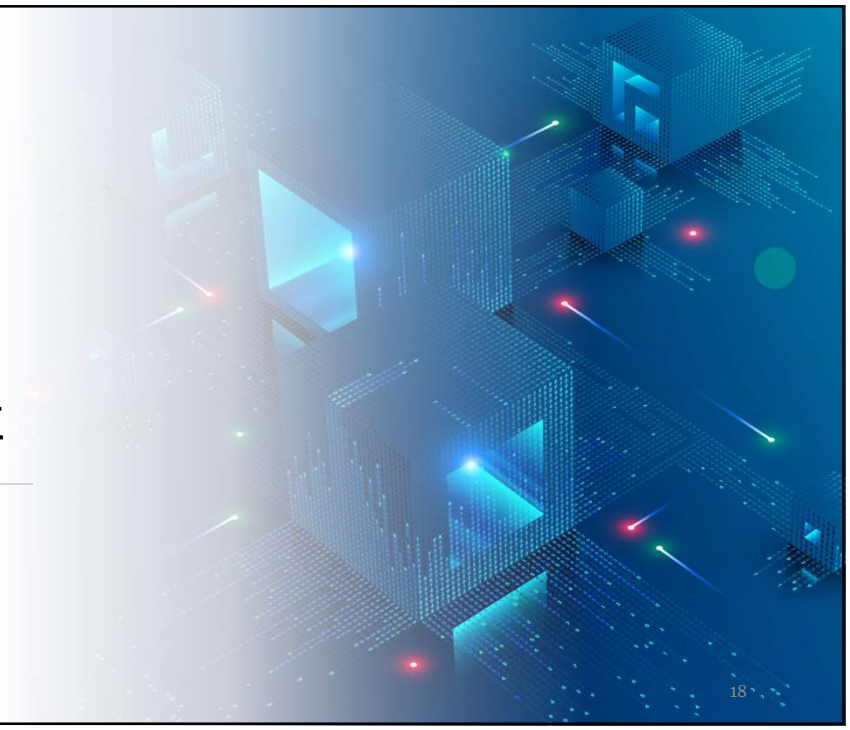


Quellen: BFS – Omnibus IKT, Eurostat

17

Digitaler Fussabdruck

Wir hinterlassen **immer** «Spuren» im Internet



18

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.

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.)

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

21

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.

22

Digitaler Fussabdruck: Webseiten und Shops

Beispiel:

- Ich habe keine Kinder, ich kaufe nie Windeln, Kinderkleider etc. Ich bekomme nie Werbung für solche Sachen.
- Aber 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!

Digitaler Fussabdruck: Webseiten und Shops

Beispiel 2:

- Gruselig: Wenn es Amazon schon vor dir weiss, wenn du schwanger bist
- «Von wegen Datenschutz – Amazon kann 300 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

Digitaler Fussabdruck: Soziale Medien

- Alles was ich irgendwo auf Facebook 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.

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»

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 Cyber-Vetting

Digitaler Fussabdruck: Cyber-Vetting

Cyber-Vetting bedeutet, dass Arbeitgeber ihre Soziale-Medien-Profile überprüfen.

Wichtigste Plattformen sind:

- LinkedIn
- Facebook
- Twitter

Cyber-Vetting betreiben die Arbeitgeber für folgende Informationen:

- Was sie im Leben und im Beruf schon gemacht haben (sekundärer Lebenslauf)
- Ihre Interessen und Hobbies
- Ihre politischen Ansichten

Digitaler Fussabdruck: Cyber-Vetting

Negative Spuren

- Unkorrekte Äusserungen, z.B. politisch oder rassistisch aber auch Reklamationen über frühere Arbeitgeber (negativ bei der Bewerbung)
- Fotos oder andere Spuren von Parties, Drogen, Sex etc.
- Kein Profil (vielleicht wollen Sie etwas verstecken?)
- **Achtung**: Auch gelöschte Aktivitäten sind vielleicht noch zu sehen, z.B. wenn man mit Google sucht

Digitaler Fussabdruck: Cyber-Vetting

Liste von negativen Spuren

- Posten von provokativen oder unangemessenen Fotos, Videos oder Informationen
- Diskriminierende Bemerkungen in Bezug auf Rasse, Geschlecht, Religion usw. zu machen.
- Mit kriminellem Verhalten in Verbindung stehen.
- Lügen über ihre Qualifikationen oder eine Abwesenheit.
- Schlechte Kommunikationsfähigkeiten.
- Negative Aussagen über ihr früheres Unternehmen oder ihre früheren Mitarbeiter.
- Unprofessioneller Benutzername
- Weitergabe vertraulicher Informationen von früheren Arbeitgebern.

Digitaler Fussabdruck: Cyber-Vetting

Tipps zum Umgang mit Cyber-Vetting:

Achten Sie auf einen positiven Fussabdruck.

Man kann zwei Profile machen: Ein privates, mit einem erfundenen Namen und ein professionelles mit dem eigenen Namen. Auf dem professionellen Profil teilen Sie nur Informationen, die sie als guten und interessierten Arbeiter zeigen. Dieses ist eher öffentlich, der Zugriff auf das private Profil sollte stark beschränkt sein (siehe Privatsphäre).

31

Digitaler Fussabdruck: Cyber-Vetting

Tipps zum Umgang mit Cyber-Vetting:

So können Sie prüfen und sicherstellen, dass ihr Fussabdruck positiv ist:

- Recherchieren Sie sich selbst: So können sie selber sehen, welche Informationen Teil ihres digitalen Fussabdrucks sind.
- Denken Sie nach, bevor Sie etwas posten: Dies gibt Zeit, um zu überlegen, ob dies etwas ist, das Teil des eigenen digitalen Fussabdrucks sein sollte oder nicht.
- Betonen Sie attraktive Eigenschaften und Qualitäten: Auf diese Weise werden in den Augen potenzieller Arbeitgeber positiv gesehen.

32

Digitaler Fussabdruck: Privatsphäre

Um einen positiven Fussabdruck zu bekommen, ist es wichtig, dass man kontrollieren kann, welche persönlichen Informationen im Internet und auf sozialen Medien in Umlauf kommen.
Dies kann man mit den Privatsphäre-Einstellungen machen.

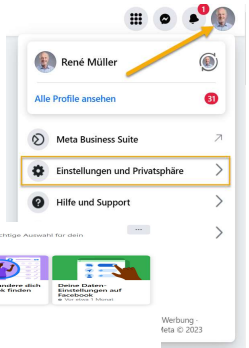
Ihr bekommt eine Schritt-für-Schritt-Anleitung für:
- Facebook
- Instagram

Privatsphäre-Check Facebook

So gelangen Sie zum Privatsphäre-Check auf dem PC:

1. Klicken Sie auf Facebook oben rechts auf ihr Bild

2. Klicken Sie auf Einstellungen und Privatsphäre > Privatsphäre-Check



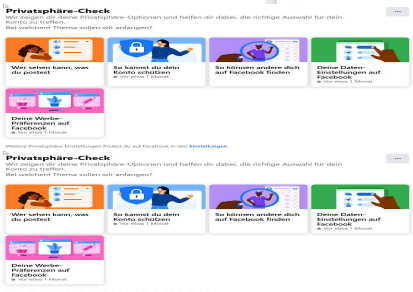
Folgendes können Sie im Privatsphäre-Check überprüfen

Wer sehen kann was Sie posten

Wie Sie Ihr Konto schützen können

Wie andere Sie auf Facebook finden können

Ihre Daten-Einstellungen auf Facebook



Privatsphäre-Check Instagram

- So gelangen Sie zum Privatsphäre-Check auf dem Handy:
- 1. Klicken Sie auf Instagram unten rechts auf
- 2. Dann oben rechts auf ☰ → ⚙ Einstellungen → 🔒 Privatsphäre

- Kontrollieren Sie und passen Sie evtl. Ihre Einstellungen an

1. Sichtbarkeit: Wer kann mein Konto sehen? Evtl. Konto auf Privat setzen
2. Aktivitätsstatus: Wer sieht wann ich online bin?
3. Kommentare: Wer kann meine Beiträge kommentieren?
4. Erwähnungen: Wer kann mich auf Beiträgen markieren?
5. Kontakte: Wer hat Zugriff auf meine Kontakte?

Daten im Internet löschen: Facebook

Deaktivieren: Ihr Account bleibt bestehen, aber Personen können sie nicht finden und ihre Posts und Inhalte nicht sehen.

Löschen: Ihr Account wird ganz gelöscht, aber erst nach 30 Tagen. Wenn Sie innerhalb dieser 30 Tage ins Facebook gehen, wird die Löschung annuliert.

Daten sichern bei Löschung: Sie können ihre Daten mit dem Browser (nicht mit dem App) herunterladen und speichern: Im Menü oben rechts auf «Kopie ihrer Facebook-Daten herunterladen» klicken

Daten im Internet löschen: Instagram

Deaktivieren: Ihr Account bleibt bestehen, aber Personen können sie nicht finden und ihre Posts und Inhalte nicht sehen.

Löschen: Ihr Account wird ganz gelöscht, und zwar sofort. Das ist nur möglich über diesen Link:
https://instagram.com/accounts/remove/request/permanent

Daten sichern bei Löschung: Sie können ihre Daten mit dem Browser (nicht mit dem App) herunterladen und speichern: Im Menü «Download anfordern» klicken.

HTTPS vs. VPN

- HTTPS: Hypertext Transfer Protocol Secure
- VPN: Virtual Private Network
- HTTPS verschlüsselt Ihre Daten, während sie übertragen werden, während VPNs Ihre Daten verschlüsseln, während sie ruhen. Darüber hinaus schützt HTTPS nur die Daten, die zwischen Ihrem Computer und der von Ihnen besuchten Website gesendet werden, während VPNs den gesamten Datenverkehr auf Ihrem Gerät schützen können.

Vorteile eines VPN

Dies sind die wichtigsten Vorteile eines VPNs:

- Umgehen von Inhaltssperren und Zensur
- Sicheres Online-Shopping und –Banking
- Anzeigen konsistenter Preise
- Einrichten einer sicheren Verbindung
- Gewährleisten von Anonymität (IP-Verschlüsselung)
- Kein Tracking durch Internetdienstanbieter und Schutz Ihrer Daten
- Streaming von Filmen (Umgehung Geoblocking)

Daten im Internet : Cookies

Was sind Cookies?

- Cookies sind kleine Textdateien, die von einer Website auf Ihrem Computer oder Mobilgerät gespeichert werden, wenn Sie die Website besuchen.
- Sie dienen dazu, das Browsererlebnis zu verbessern, indem sie dem Browser Informationen zur Verfügung stellen, die er benötigt, um die Website richtig anzuzeigen, und es dem Website-Betreiber ermöglichen, die Nutzung der Website zu verfolgen.
- Cookies können auch verwendet werden, um Informationen wie Ihre Präferenzen zu speichern und Ihnen personalisierte Inhalte anzuzeigen.

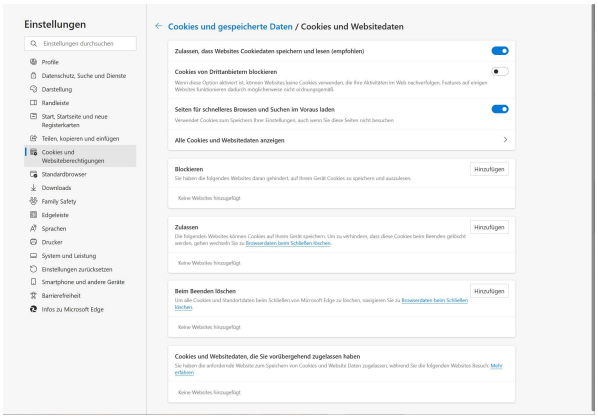
Daten im Internet löschen: Cookies

- **Im Browser**:
  - → Hauptmenü (3 Punkte in der oberen rechten Ecke)
  - → Verlauf
  - → 3 Punkte oben
  - → Browserdaten löschen
- **Privater Modus:**

  Wenn Sie im privaten Modus browsen werden die Cookies gelöscht, sobald sie das Fenster schliessen.

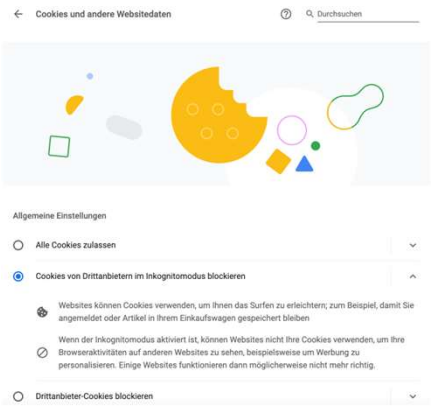
Cookie-Einstellungen Edge

- Oben rechts drei Punkte → Einstellungen → Cookies und Website-berechtigungen → Verwalten und Löschen von Cookies
- Shift+Ctrl+I zeigt Cookies unter dem Reiter Anwendung



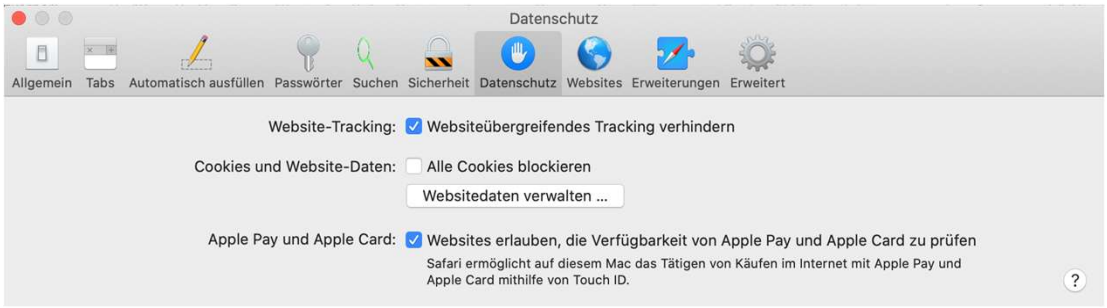
Cookie-Einstellungen Chrome

- 1. Menüleiste Chrome → Einstellungen → Datenschutz und Sicherheit



Cookie-Einstellungen Safari

- 1. Menüleiste Safari → Einstellungen → Datenschutz



Daten im Internet löschen: Historie

- Die Historie zeigt, welche Seiten Sie im Internet besucht haben.
- Im Browser:

→ Hauptmenü (3 Punkte in der oberen rechten Ecke)

→ Einstellungen

→ Datenschutz und Sicherheit

- Privater Modus:

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

46

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

47

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

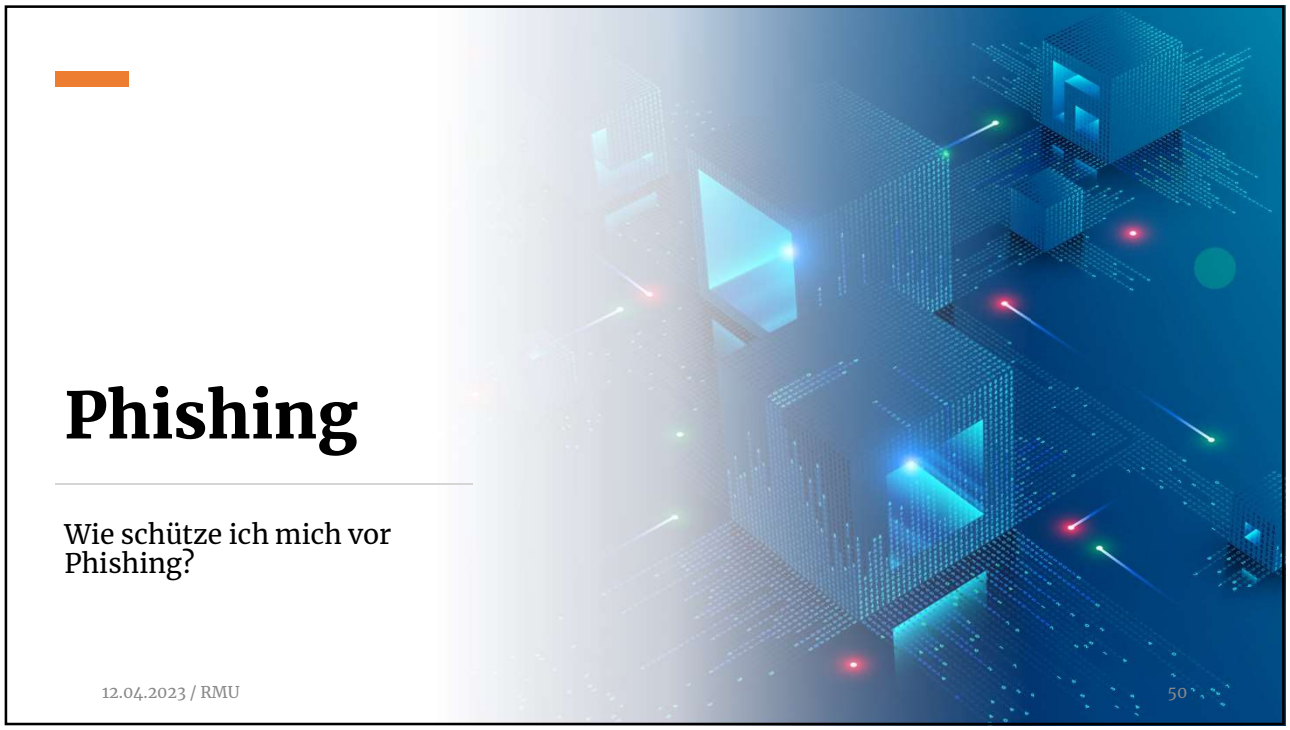
Daten im Internet löschen: Privates browsen

Folgende Browser haben einen privaten Modus

- Google Chrome: Incognito Mode.
- Microsoft Internet Explorer & Edge: InPrivate Browsing Mode.
- Mozilla Firefox: Private Browsing Mode.
- Opera: Private Browsing Mode.
- Safari: Privates Fenster.

Mehr Informationen:

- Auf dieser Seite sehen Sie, was man alles löschen kann und wie:
https://us.norton.com/internetsecurity-privacy-how-to-clear-cookies.html



Phishing

Wie schütze ich mich vor Phishing?

50

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.**

51

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

- Kreditkartennummer
- Kontonummer
- Ausweisnummer
- Passwort
- vollständiger Name

(Quelle: Stadtpolizei Zürich)

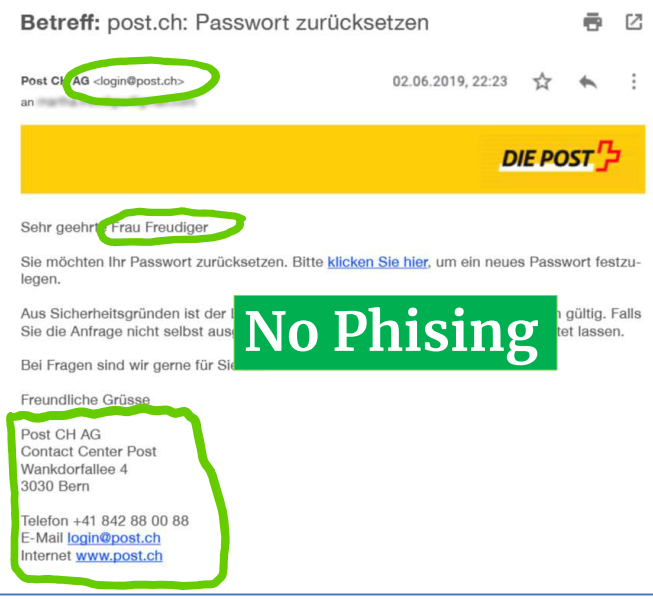
52

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)

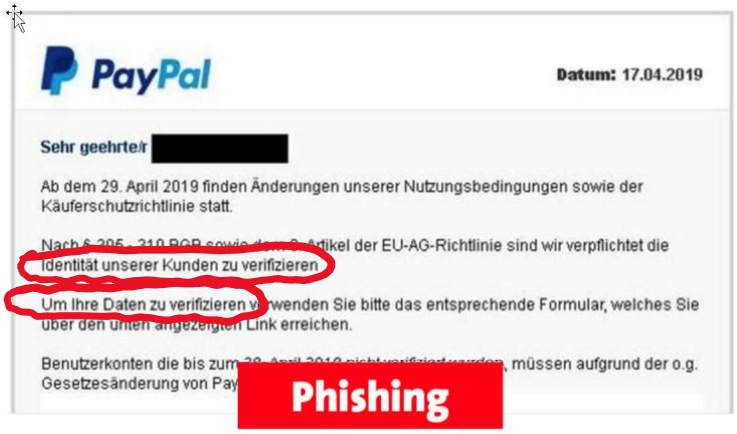
53


Betreff: post.ch: Passwort zurücksetzen
AG <login@post.ch>
02.06.2019, 22:23
DIE POST
Sehr geehrte Frau Freudiger
Sie möchten Ihr Passwort zurücksetzen. Bitte klicken Sie hier, um ein neues Passwort festzulegen.
Aus Sicherheitsgründen ist der
gültig. Falls Sie die Anfrage nicht selbst aus
tet lassen.
Bei Fragen sind wir gerne für Si
Freundliche Grüsse
Post CH AG
Contact Center Post
Wankdorfallee 4
3030 Bern
Telefon +41 842 88 00 88
E-Mail login@post.ch
Internet www.post.ch
No Phising

54


italienische rezepte
ALLE
BILDER
SHOPPING
VIDEOS
NEWS
Anzeige
www.golbani.ch/
Italienische Rezepte | Galbanis beste Kochrezepte |
Ob Pizza, Capre
präsentiert dir die besten Rezepte. Einfach. Schnell. Lecker. Spezialitäten aus Italien. Rezepte zum Nachkochen. Nr. 1 in Italien.
Schnell & einfach kochen
Phising

55



PayPal

Datum: 17.04.2019

Sehr geehrte/r [redacted]

Ab dem 29. April 2019 finden Änderungen unserer Nutzungsbedingungen sowie der Käuferschutzrichtlinie statt.

Nach § 305 - 310 BGB sowie dem 9. Artikel der EU-AG-Richtlinie sind wir verpflichtet die Identität unserer Kunden zu verifizieren

Um Ihre Daten zu verifizieren verwenden Sie bitte das entsprechende Formular, welches Sie über den unten angezeigten Link erreichen.

Benutzerkonten die bis zum 29. April 2019 nicht verifiziert wurden, müssen aufgrund der o.g. Gesetzesänderung von Pay

Phishing

Von: "RAIFFEISEN BANK AG"<info@Raiffeisen.ch>
Datum: 7. Mai 2013 09:22:43 MESZ
Betreff: Raiffeisen Kundendienst.

Sehr geehrter Kunde,

Kürzlich, laut unseren Unterla[redacted]nt ein unbefugter Dritter hat versucht, in Ihr Konto einlogg[redacted] Hauptanliegen, so haben wir beschlossen, Beschränken Sie [redacted]l. Für den vollen Zugriff auf Ihr Konto, müssen Sie Ihre Daten wiederherstellen, um das zu bestätigen Link:
WWW.RAIFFEISEN.COM

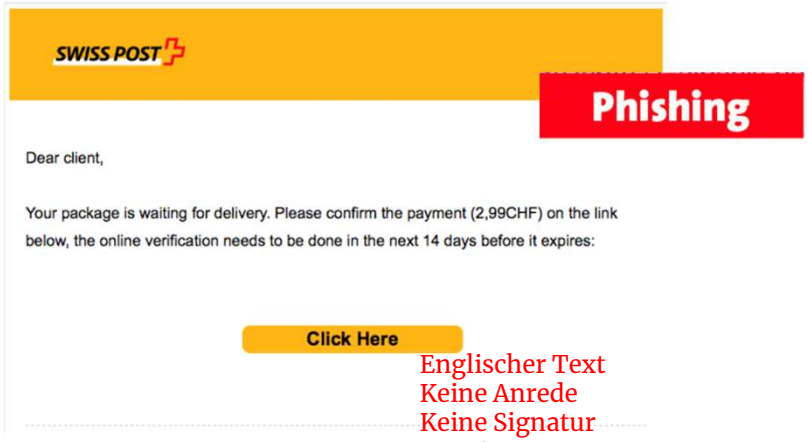
Sobald Ihre Daten von uns überprüft wurden und bestätigt, einer unserer personal wird Sie innerhalb von 48 Stunden per Telefon vollständig aktivieren Sie Ihr Konto und alle Zugang zu Ihrem Konto wird vollständig wiederhergestellt werden.

Vielen Dank für Ihre Mitarbeit.

Mit freundlichen Grüßen,
RAIFFEISEN Bank AG Angelegenheiten Security Department.

Phishing

Voller Schreibfehler, merkwürdige Formulierungen und Zeichen



Englischer Text
Keine Anrede
Keine Signatur
2,99CHF

58

Keine persönliche Anrede
Keine vollständige
Signatur
Sicherheitsupdate
Scharfes «S»

59

Absender: Viseca Card Services <do_not_replay@viseca.com>

Schützen Sie Ihre Kreditkarte

Bitte klicken Sie auf folgende URL, um die Anmeldung zu aktivieren. Dies muss innerhalb der nächsten 2 Tage erfolgen.

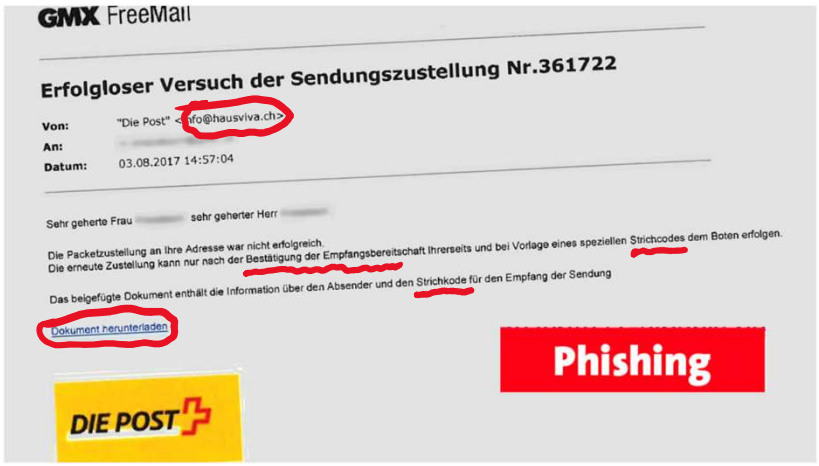
Aktivieren 3-D Secure

3-D Secure ist ein international anerkannter Sicherheitsstandard für Kreditkartenzahlungen im Internet. Bei einem Online-Einkauf geben Sie zusät… Ihnen bekannt ist.Sie identifizieren sich damit ähnlich wie mit dem PIN… e direkt im MyAccount für 3-D Secure anmelden.

Phishing

© 2013 Viseca Card Services SA

60



Ein betrügerisches E-Mail mit einem gefälschten Post-Logo verunsichert Kunden. Im E-Mail heisst es: *Die Paketzustellung an Ihre Adresse war nicht erfolgreich. Die erneute Zustellung kann nur nach der Bestätigung der Empfangsbereitschaft Ihrerseits und bei Vorlage eines speziellen Strichcodes dem Boten erfolgen. Das beigefügte Dokument enthält die Information über den Absender und den Strichkode für den Empfang der Sendung. Dokument herunterladen.*
Auf diesen Link sollte man unter keinen Umständen klicken: Das Mail stammt von Betrügern und bringt einem kein Paket nach Hause, sondern unter Umständen einen Virus auf den Computer.

61

Was schützt Sie vor Phishing?

- Seien Sie misstrauisch.
- Antworten Sie auf keinen Fall auf eine verdächtig erscheinende Nachricht.
- Klicken Sie auf keine Links, öffnen Sie keine 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.
- Bei Verdacht auf Betrug wenden Sie sich an die Polizei oder an KOBIK, die Schweizerische Koordinationsstelle zur Bekämpfung der Internetkriminalität.

(Quelle: Stadtpolizei Zürich)

62

Passwörter

Wie schütze ich meine Zugangsdaten?

63

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

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

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)