Digitale Schutzmaßnahmen für Privatanwender

Dieses Dokument vereint die kleine Serie von technischen Artikeln, mit dem Ziel dein digitales Leben sicher und leicht zu machen.

Wir beleuchten die Grundlagen des Internets und Maßnahmen zur Sicherheit deiner Systeme und Daten.

Bitte beachte den Disclaimer am Ende und dass alle genannten Tipps Hinweise sind und keine konkrete Handlungsanweisung enthalten und damit keine direkte Anleitung zur Umsetzung. Wähle aus, in welchem Bereich du aktiv werden möchtest oder solltest und suche dir dann die entsprechende Anleitung zur Umsetzung im Internet.

Eine großartige und professionelle Checkliste findest du hier: https://heise.de/-4886712

Inhaltsverzeichnis

Die "Internets"

Das Internet ermöglicht uns Dinge, die früher nicht einmal denkbar gewesen wären. Von der Automatisierung von Rechenoperationen für die Raumfahrt, die erste Kommunikation zwischen Universitäten bis zum ersten lokalen Netzwerk in einer Firma. Heute haben wir diese Technik in der Tasche und jederzeit verfügbar.

Warum ist das Internet nicht so sicher?

Das Internet wurde entwickelt in einem kleinen, recht vertrauten Umfeld und der Aspekt der Sicherheit wurde damals nicht mit bedacht. Das Internet besteht aus einer gemeinsamen, einheitlichen Sprache, die keine Geografie, keine Rasse und keinen Glauben kennt. Die Grundlage ist eine technische Basis (Internetprotokolle und Hardware) und eine große Portion Vertrauen. Und so gern, wie die eine Seite erschafft, gibt es Herausforderer, die das System optimieren. So entsteht der massive Fortschritt, der das digitale Zeitalter erst möglich macht. Und dort gibt es immer wieder schwarze Schafe und ein regelrechtes Wettrüsten.

Welche "Ebenen" hat das Internet, und ist es gefährlich?

Das Internet lässt sich grob in drei Kategorien einteilen: die Oberfläche (Surface Web, Clearnet, Clear Web), den privaten Teil (Deep Web, Deepnet, Hidden Internet, Invisible Web) und das medial aufgebauschte Darknet.

Das **Surface Web** kennen wir gut, es ist durchsuchbar mit Suchmaschinen und die Inhalte sind indexiert und zumeist für jeden verfügbar. Von Webseiten, Blogs, Nachrichten und Katzenvideos über Online Shops bis Social Media. Das macht jedoch nur den kleinsten Teil des Internets aus.

Dahinter steht das **Deep Web**, das sind zugangsbeschränkte Inhalte wie Datenbanken von medizinischen oder lehrenden Einrichtungen, Unternehmensdaten, Backups, WebMail, Banking, Foren, etc. Oder Inhalte hinter PayWalls (bezahlte Inhalte) wie (Hör-)Bücher, Serien, Filme, usw. Die Inhalte sind nicht indiziert oder direkt per Suchmaschine auffindbar, die Webseiten an sich schon.

Das **Darknet** verkauft sich als Bösewicht in den Medien wie von selbst und ja, es gibt einen guten Teil an zwielichtigen Inhalten (Illegaler Handel, Pornografie, Daten, usw.). Die Webseiten und Dienste sind nirgends aufgelistet und verschlüsselt, es wird ein besonderer Browser für den Zugriff benötigt (Tor). Der Sinn dahinter ist jedoch der Schutz der Teilnehmer vor Zensur und Überwachung. Das hat Vor- und Nachteile, genau wie in der analogen Welt. Wo einerseits Menschen geschützt und anonym kommunizieren können, gibt es natürlich auch schwarze Schafe. Als Analogie könnte man eine dunkle Straße nehmen, diese kann dich vor Verfolgung schützen, und gleichzeitig werden dort Drogen angeboten (ohne Zwang). Hier gibt es also nicht nur Kriminelle, sondern vor Allem Journalisten, Menschenrechtler, Whistle Blower, usw. Was wir wirklich bekämpfen sollten sind nicht nur

Unternehmungen (oder Personen), die illegale Webseiten hosten - sondern auch Unternehmungen (Personen, Firmen) die der Umwelt schaden und z.B. giftige Substanzen herstellen von Drogen, über Chemikalien, bis zum Billigfleisch und weiteren Artikeln, die der Umwelt und Menschheit schaden.

Ist das Darknet per se böse?

Weil Verschlüsselung und Anonymität verhindern, dass kontrolliert, verfolgt und überwacht werden kann, ist das Darknet natürlich eine riesige "Gefahr" (hier folgt ganz viel Interpretationsspielraum). Genauso ist es generell mit der Verschlüsselung von Kommunikation. Unter dem Deckmantel der Sicherheit lassen sich viele Gründe finden, doch noch ein Hintertürchen zum Abhören bereit zu stellen. Und dementsprechend erfordern all diese Maßnahmen etwas Arbeit.

Was du für deinen digitalen Schutz tun kannst, folgt im nächsten Blog-Post!

Sollte das Thema dich interessieren sind hier ein paar nette Dokumentationen:

Zusammenfassung in 4 Minuten

So sollte es nicht laufen (Doku)

10 Mythen über das Darknet

Ted Talks zum Thema (EN)

35C3 - Du kannst alles hacken – du darfst dich nur nicht erwischen lassen.

Teil 1 - Grundlagen

Zuerst zu den **Grundlagen**,
wie du dich - bzw. deine digitalen Identitäten - absichern kannst.

Mit jedem (technischen) System, welches du nutzt, hinterlässt du automatisch Spuren. Das ist teilweise notwendig, da sonst einige Dienste nicht funktionieren würden (Mobilfunk, Internetzugang), teilweise gibt es jedoch eine reine Sammelwut des Anbieters. Diese Tipps sind nur Anhaltspunkte und enthalten meine eigene Erfahrung und Empfehlung. Mit jedem Punkt kannst du dich auch mehrere Minuten bis Stunden auseinandersetzen. Anleitungen zu den einzelnen Optionen gibt es im Internet, insofern ich die konkreten Anleitungen finde, verlinke ich diese. Zu den Motivationen und Fällen, die du und wir vermeiden möchten, will ich nicht zu ausführlich berichten. Wenn du das brauchst, findest du in den Nachrichten genug Mangel, Angst und Panikmache. Ich möchte hier nur über die Absicherung berichten.

Grundlegend gilt für Online-Dienste: Wenn der Dienst kostenlos ist, bist du das Produkt (bzw. deine Daten sind die Bezahlung und/oder du wirst mit Werbung beworfen).

Einige Anbieter sagen "OK, du hast unsere Geräte bezahlt, damit ist alles abgeglichen" und andere Anbieter sind der Meinung "Ach, wir nehmen dein Geld und dazu noch deine Daten."

Die **Zusammenfassung** zuerst:

- Richte sichere Passwörter ein. Verwahre diese in einem gut geschützten Ort - am besten einem (Offline) Passwortmanager. Mit diesem kannst du direkt sichere Passwörter erzeugen!
  - Verwende keine ähnlichen/gleichen Passwörter für verschiedene Dienste.
  - Erneuere Passwörter, die Jahre alt sind oder zu einfach.
- Für alle wichtigen Konten nutze einen zweiten Faktor bei der Anmeldung (MFA – Multi Faktor Authentifizierung).
- Reduziere die Erzeugung von unwichtigen oder gefährlichen Daten.
- Vermeide nicht benutzte Konten und Programme. Optimiere deine Social Media Nutzung bis hin zum Zahlungsanbieter.
- Verschlüssele deine Kommunikation (Mail, Daten).
- Richte automatische Updates ein bei: Betriebssystem, Programmen und Apps.
- Wichtige Daten brauchen ein regelmäßiges Backup! Persönliche Daten, Fotos und wichtige Dokumente (Mails, etc.) sollten regelmäßig gesichert werden.

Der große **Haken**:

Die grundlegende Absicherung deiner Daten und Geräte ist etwas Aufwand, wenn du alle deine Geräte eingerichtet hast, läuft es weitestgehend pflege-frei, manchmal sind es nur wenige Klicks. Sicherheit geht aktuell noch zu Lasten des Komforts, an der Stelle ist deine eigene Risiko-Einschätzung gefragt. Um es richtig gut zu machen, sind einige Kenntnisse und etwas Zeit gefragt. Dafür bist du vor brenzligen Situationen bewahrt und wirst nicht einmal merken, wie kritisch und belastend diese sein könnten.

Die **Wahrheit**:

Viele Dienste möchten Einnahmen erzeugen (z.B. durch Werbung, In-App-Käufe) oder einfach nur deine Zeit und Aufmerksamkeit. Andere arbeiten mit deinen Daten und nutzen diese zur Analyse oder Weitergabe. Im optimalen Fall verbessert das Systeme, wie z.B. die Bild- und Spracherkennung.

Die größere Gefahr ist, dass deine persönlichen Daten ins Internet geraten, zum Beispiel deine Kreditkartendaten, Adresse, usw. Oder sogar über ein paar Daten / einzelnes Konto hinaus, dass deine Daten zusammengestellt und damit Profile erzeugt werden. So können anhand von Ausgaben Rückschlüsse gezogen werden auf deine aktuelle Situation, zum Beispiel könnte eine Schwangerschaft erkannt werden, bevor du es selbst erkennst. Kritisch wird es, wenn Gesundheit und Finanzen zusammengebracht werden, um Bewertungen vor zu nehmen.

Was kannst du also für die Sicherheit deiner Daten und deiner digitalen Identitäten tun?

Ein wichtiger Punkt ist Aufmerksamkeit! Nimm' dir einen Moment, wenn etwas komisch aussieht und Frage lieber einmal Zuviel nach. Wenn etwas bedrohlich ist, bleib' ruhig und handle nicht gewissenhaft!

Bevor wir zum Schutz deiner Konten, Daten und Geräte kommen,
hier ein paar **konkrete** Punkte:

- Überprüfe heruntergeladene Dateien und mehr:
  https://www.virustotal.com/gui/home/upload
- Lade nur Programme aus vertrauenswürdigen Quellen herunter:
  https://www.heise.de/download/
  (auf dem Smartphone NUR Apps aus dem offiziellen Store!)
- Nutze Passwort-Manager:
  Offline-Manager wie **KeePass** oder KeepassXC
  Auch sind Online-Passwortmanager heute recht sicher und ersparen dir Backups. Meine aktuelle Empfehlung ist **Dashlane**, funktioniert auch mobil und synchronisiert sich.
  https://www.dashlane.com/de/
- Browser – meine aktuelle Empfehlung ist der Brave Browser https://brave.com/de/
- Dienste, die Sicherheitsprobleme haben oder hatten:
  https://haveibeenpwned.com/PwnedWebsites
- prüfe deine Mail-Adresse: DE: https://sec.hpi.de/ilc/ / EN: https://haveibeenpwned.com/
- Überprüfe dein Passwort: https://haveibeenpwned.com/Passwords
  prüft dein Passwort gegen die öffentlichen Listen, bekannter (geleakter) Passwörter.
- Wergwerf-Mail-Adressen:
  https://www.teltarif.de/internet/email-wegwerf-einmal-adressen.html
- Verantwortungsvolles Online-Shopping:
  - Spenden beim Shoppen:
    https://www.boost-project.com/de
    https://www.wecanhelp.de/
  - Grüne Produkte:
    https://smoothpanda.de/product-category/alle-produkte/
    https://gopandoo.de/collections/plastikfrei-zero-waste-shop
  - Amazon-Alternative:
    https://www.genialokal.de/
  - Gebrauchte Produkte:
    ebay-kleinanzeigen.de, medimops.de / rebuy.de
- Dateien verschlüsseln mit VeraCrypt:
  https://www.heise.de/download/product/veracrypt-95747

Teil 2 - Daten & Konten

So schützt du deine digitalen Identitäten und Konten. Und worauf du verzichten solltest.

Deine persönlichen Daten und Konten

- **Passwörter** sollten komplex sein und nicht aus ableitbaren Fakten bestehen (Name der Mutter, des Hundes, Lieblings-Automarke, etc.). Zur Verwaltung kannst du diese in einem Passwortmanager speichern, dann brauchst du dir nur ein sicheres Passwort merken.
- Die Strategie der ständigen **Passwortänderung** ist veraltet, aktuell ist es "in" ein komplexeres Passwort zu nutzen und die zweite Stufe (MFA) einzurichten.
- Die wichtigste aktuelle Option ist "**MFA**" - der Multi- oder zweite Faktor zur Anmeldung. Das heißt, du wirst nicht nur nach einem Benutzernamen und Passwort gefragt (Wissen) sondern auch nach zum Beispiel einem Einmal-Code oder biometrischen Merkmal (z.B. Fingerabdruck) gefragt (Besitz).
  So kannst du zum Beispiel deine Telefonnummer bei einem Dienst hinterlegen und bekommst **Einmalpasswörter** per SMS zugesendet. Ich empfehle lieber einen "**Authenticator**" als App oder auch als Schlüsselanhänger (FIDO2 z.B. von Yubico). Dann solltest du beim Wechsel des Smartphones unbedingt an diese App denken oder am besten schon vorher Vorkehrungen treffen (Backup). SMS & Telefon sind veraltete Methoden.
- Für unwichtige Dienste kannst du **Wegwerf**-**Mail**-Adressen verwenden.
- Für wichtige Dienste solltest du verschiedene Mail-Adressen nutzen. Nutze nicht bei allen Konten die gleiche Anmeldung / Mail-Adresse und nicht ein ähnliches Passwort.
- Deine sensiblen Daten bitte **verschlüsseln**, zum Beispiel auf deinem Computer mit VeraCrypt, E-Mails mit PGP/MIME.
- Auf Webseiten darauf achten, dass **HTTPS** benutzt wird, vor Allem wenn Daten übertragen werden (bei Anmeldung mit Passwort, beim Einkauf, etc.). Die aktuellen Browser sind recht empfindlich und weisen dich darauf hin, wenn kein Zertifikat vorhanden ist.

- Wieder die Grundlage #1: Ist der Dienst kostenlos, bist du wahrscheinlich das Produkt. Es gibt jedoch auch viele, recht sichere Plattformen. Wichtig ist es, etwas auf den **Ruf** zu achten und nicht nur einen Dienst zu nutzen, weil das "alle nutzen". Hilfreich dabei können Rezensionen im Store sein, kritische Stimmen können immer hilfreich sein. Es wurden einige **Dienste** sehr prominent oder sogar mehrfach als unsicher bekannt gemacht. Alle ungenutzten Accounts löschen (lassen). Dabei hilft oft die E-Mail-Adresse datenschutz@***.** des jeweiligen Anbieters weiter und eine kurze Mail mit dem Hinweis auf die DSGVO.
- Bei Diensten und Apps im Internet solltest du auf deren Ruf und Umgang mit dem Datenschutz achten. Zum Beispiel sollten Daten in Deutschland oder einem rechtlich ähnlich gelagerten Land verarbeitet werden. Wenn deine Daten alle direkt nach China oder in die USA gelangen, solltest du dir gut überlegen dort z.B. Videos von deiner Familie und Freunde hoch zu laden.
- **Bezahldienste** - sammeln ebenfalls umfangreiche Daten (Meta-Daten), und alles in Richtung Finanzen kann bedenklich sein. Es gibt z.B. einige Optionen bei PayPal, die dringend deaktiviert werden sollten. Schau in deine Einstellungen, es gibt eine Option für Anbieter, dass diese eine Art Freifahrtsschein bekommen, abzubuchen wonach Ihnen ist. Schalte auch die "**OneClick**" Funktionen aus, Paypal und Amazon.
- "**Cloud**" ist in und komfortabel, z.B. alle Fotos vom Smartphone gehen direkt ins Netz. Wenn das sein muss, dann bitte das entsprechende Konto gut absichern.
- Dazu zählen auch **Fitnesstracker** und **Smartwatches** - die Daten werden zum Großteil erst auf dem Server erst verarbeitet, einige Anbieter betreiben dies jedoch vorbildlicher als andere.
- Recht bedenklich sind auch **Assistenten** wie Alexa und Google Assistant - diese hören doch recht viel mit und daher sollte bei Nutzung die Datenübertragung weitestgehend eingeschränkt werden.
- Generell die ganze Geschichte mit dem **Smarthome** von der Heizungssteuerung, über den Kühlschrank bis zur einfachen, "smarten" Glühbirne. Alles kann einen schnellen Weg in dein Heim-Netzwerk bedeuten. Möchtest du so etwas nutzen, kaufe bitte bei großen Anbietern und setze die Produkte in einem eignen WLAN ein, am besten ohne Internetzugriff. Die beliebten DNA-Tests sind in den USA sehr umfangreich ausgewertet, in Deutschland leider nicht und das sind die absolut kritischsten Daten über die eigene Person, die es gibt - inkl. Vererbung von Krankheiten bis Stammbäume. Da werden in Zukunft noch einige Schlagzeilen folgen, **lieber Finger weg!**

Teil 3 - Smartphone

Heute geht es um das Smartphone. Wie schützt du dieses kleine Kästchen, das dein ganzes Leben beinhalten kann?

- Starte dein Smartphone regelmäßig (mindestens wöchentlich) **neu**.
- Richte dir eine **PIN** ein und z.B. einen Fingerabdruck.
- **Updates**. Halte alle APPs und das Betriebssystem auf dem aktuellen Stand, das lässt sich z.B. automatisch einstellen, sobald du im WLAN bist.
  Sehr alte Betriebssysteme, älter als Android Version 9, sollten vermieden werden, vor Allem so etwas wie Android 4 oder 5.
- Auf dem Smartphone solltest du nur **notwendige APPs** installieren, und nur aus dem offiziellen Store. Die Option zur Installation von Nicht-Store-Apps ausschalten.
- **Verschlüssele** deine Speicherkarte, so dass Sie bei Verlust des Smartphones keine Daten preisgibt (ohne Handy-Entsperrung oder in einem anderen Gerät).
- Achte auf die **Berechtigungen**, die eine App haben möchte. Viele davon sind nicht notwendig, leider jedoch manchmal sehr umfassend.
- Google hat zum Beispiel einen Standard eingeführt namens "**Google Play Protect**" - prüfe, ob das bei dir aktiv ist.
- Es gibt es die Option einen **Notfallkontakt** anzeigen zu lassen und stelle sicher, dass du aktiviert hast, dass du das Telefon bei **Verlust** löschen kannst, am besten auch **Orten**.
- Weitere Maßnahmen sind nicht zwingend notwendig, wenn du keine APPs aus fremden Quellen installierst.
- Es gibt natürlich noch APPs die steuern können, welcher Dienst wann Zugriff auf das Internet hat - eine Art **Firewall** (ich teste da gerade NetGuard) und eine **AntiVirus**-Lösung (Lookout). Generell hatte ich sowas noch nicht und bisher ist nie etwas passiert, und trotzdem kann es ein gutes Gefühl vermitteln.
- **Downloads / Mails + Dateien** - nur aus sicheren Quellen ausführen / öffnen. Zum Beispiel keine APPs oder App-Installations-Dateien öffnen, die nicht aus dem offiziellen Store sind.
- **Fotos** - auch diese können viele Daten preisgeben (EXIF-Daten) von deinem Handy-Modell über Datum und Zeit bis zu GPS-Daten.

Weg Damit!

Also konkret, wovon sollen wir die Finger lassen bzw. sehr gut auf unsere Daten aufpassen?

- Aus den aktuellen Meldungen sollte unbedingt vermieden werden: TikTok, Snapchat, …
- Weniger ein Datenschutz-Bedenken, gleichzeitig sehr bedenklich sind Riesen wie Amazon. Weiche bitte auf verantwortungsvolle Händler aus.
- Generell würde ich von Facebook und WhatsApp abraten, eventuell auch Instagram. Es gibt gute Alternativen für Messenger, ich stelle gerade auf SIGNAL um. Es gibt gute kostenlose Alternativen die auch viele Teilnehmer haben.
- Bekannte Dienste vermeiden, die bereits bekannt sind für Ihre Unsicherheit bzw. MySpace, usw.
- QR-Codes, die überall kleben, nur abfotografieren und anklicken, wenn du der Quelle vertraust!

Sehr spannend sind Menschen, die Datenschutz-Bedenken über WhatsApp oder Facebook verbreiten. WhatsApp ist viel bedenklicher, als ein Großteil der anderen Apps die man so nutzen könnte :)

Teil 4 - Computer & Laptop

Der vorerst letzte Teil der Serie "digitale Schutzmaßnahmen" - dein Computer, Laptop und alles drumherum.

Computer

- Mache regelmäßige **Backups** deiner Daten auf einem Datenträger, der nicht ständig verbunden ist. (Grund: sogenannte Ransomware verschlüsselt alle Daten, und selbst wenn du dich "freikaufst" ist das keine Garantie).
- Dein **Betriebssystem** und die darauf laufenden **Programme** immer **aktuell** halten, am Besten automatisch aktualisieren / updaten lassen.
- Du solltest eine Firewall und Antivirenschutz nutzen, als Grundausstattung genügen die Windows-Vorrichtungen (Firewall, Defender, etc.).
- Die **Festplatte** sollte verschlüsselt sein (z.B. Bitlocker). Das funktioniert sogar ohne Eingabe eines Passwortes und ist ein minimaler Schutz bei Verlust des Gerätes. Sehr kritische Daten sollten gesondert gespeichert werden, am besten auf einem Gerät/einer Festplatte die nicht immer am Rechner angeschlossen ist.
- Nutze keine fremden (oder gefundenen) Datenträger.
- Installiere **Software** nur auch vertrauenswürdigen Quellen oder vom Hersteller direkt.
- Nutze einen (Offline) **Passwortmanager** mit einem komplexen Passwort.
- **Passwörter** gehören nicht (im Klartext) neben, an, in oder auf den Computer :)

Heim-Netzwerk

- Richte dir ein sicheres **WLAN** ein mit der aktuellen **Verschlüsselung** WPA2 (optimal: AES mit CCMP) und einem guten Passwort. Und falls schon verfügbar, nimm' "WPA3". Beim Passwort bitte auch hier etwas leicht komplexes mit mindestens Zahlen und Buchstaben, nicht sowas wie "WirliebenunserHaustier".
- Dein WLAN solltest du neutral und selbst benennen (der WLAN Name ist die "SSID"), der Name darf kein Hinweis auf das Passwort sein! Und wenn du dich bereits auf deinem Modem (FritzBox, etc.) angemeldet hast:
- Ändere die Zugangsdaten zu diesem Gerät. Das Standard-**Passwort**, welches auf der Rückseite des Gerätes steht ist nicht das Optimum, die Anmeldedaten sollten jedoch auch nicht "admin" + "admin" lauten.
- Wenn es viel Besuch gibt, kann ein Gast-WLAN mit einem eigenen Passwort Sinn machen.
- Es wäre gut, wenn sich dein Internet-Modem nicht über das WLAN konfigurieren lässt.
- Deaktiviere bitte "WPS" - das ist das Knöpfchen zum schnellen Verbinden des WLAN direkt am Gerät.
- Auch der Router / das Modem braucht **Updates** - hier kannst du einstellen, dass dies automatisch passieren soll. Auch ein automatischer Neustart (mindestens einmal die Woche) macht technisch Sinn, am Besten Nachts, dann gibt es tagsüber keine Unterbrechungen.

- Was du nicht brauchst, **deaktivieren**. Heute ist einiges an Schi Schi mit diesen Geräten möglich (Dateifreigabe, am besten noch über Internet, Druckerfreigabe, FTP, Medienserver, etc.).

Browser

- Installiere dir einen Browser deiner Wahl (z.B. Firefox / Chrome) und dazu einen **AdBlocker**, denn schon Werbeanzeigen können gefährlich sein.
- Oder du nutzt den neuen **Brave Browser** – dort wird sehr viel ohne weitere Einstellung herausgefiltert. Er spart Daten und unterdrückt, was nicht sicher ist.
- In den Einstellungen solltest du mindestens Third-Party **Cookies** blockieren. Du kannst dazu noch eine "**DoNoTrack**"-Anforderung einstellen, das wird jedoch nicht verlässlich befolgt.
- Das "**NoScript**" AddOn zum Verbot von Java Script sollte zusätzlich vorhanden sein und nur auf vertrauenswürdigen Seiten aktiviert werden.
- Sehr Sicher bist du mit dem **Tor Browser** - dieser leitet deine Anfragen an das Internet mehrfach weiter, sodass die Nachverfolgung recht schwer ist. Alternativ das Thema "VPN" (virtueller, privater Kanal), dort muss dann dem jeweiligen Anbieter vertraut werden.

Dateien und E-Mails

- Öffne keine **Dateien** aus nicht vertraulichen Quellen, du kannst Dateien auch überprüfen lassen oder in einer **sicheren Umgebung** öffnen (z.B. Windows Sandbox).
- Du kannst deine Mail-Adresse(n) bei verschiedenen Diensten überprüfen lassen, ob diese Daten im Netz gelandet sind.
- Alles, was in dir **Emotionen** erzeugt, solltest du **langsam** angehen.
    - Egal ob Social Media, Mail oder Anruf, wenn jemand etwas ganz Dringendes haben will - immer kurz inne halten und erst nachdenken.
    - Kein Dienst wird dich, z.B. per Mail, nach deinem Passwort fragen.
    - Beispiel: Wenn deine Bank dich anmailt, dass dein Konto gesperrt ist - immer direkt die Bank kontaktieren oder die Adresse der Webseite selbst eingeben. Als Kurzfassung kannst du bei suspekten Anfragen auf die Sprache achten, auf die angegebenen Adressen (Link, Absender, …) und ob das Anliegen überhaupt passt. Ganz einfach: wenn du kein Auto hast, lösche die Mail mit der Rechnung des Reifenwechsels ;)

Disclaimer

Diese Sammlung an Tipps stammt von einer Privatperson und stellen keine Garantie auf sichere Systeme und Online-Konten da. Alle Maßnahmen können im Fehler- oder Angriffsfall sehr hilfreich sein und größere Schäden (Kosten, Image, Zeitaufwand) verhindern. Es besteht kein Anspruch auf Fehlerfreiheit, Vollständigkeit und/oder vollständigen Schutz. Diese Liste entstand aus vielen Jahren eigener IT-Erfahrung und ist selbst erstellt.

Deine Sicherheit liegt vollständig in deiner eigenen Verantwortung, daher:

Bleib sicher!

Blog | Facebook | Twitter | Impressum
