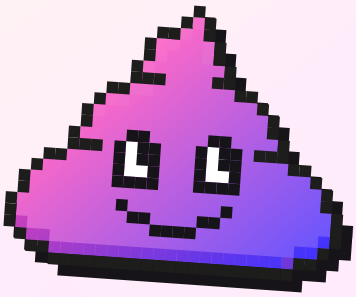
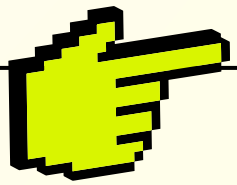


Cybersecurity BS-Bingo

Beim Thema digitale Sicherheit hörst du lieber weg? Das ungute Gefühl von „eigentlich ist es super wichtig“ steht dem „irgendwie finde ich keine Zeit dafür“ entgegen, und du verschiebst es immer weiter. Mit der Zeit wird das Thema immer unangenehmer und peinlicher, weil du dich „eigentlich schon vorgestern hättest einlesen sollen“.
Wir kennen das alle! Dazu kommen unterschiedliche, teils widersprüchliche Ratschläge und Guidelines online und offline. Wir haben ein paar davon gesammelt und beleuchten sie mal genauer!

Ich habe nichts zu verbergen	Ich beschäftige micht nicht mit Sicherheit, weil ich davon überwältigt bin und mensch es eh nicht richtig machen kann	Apps hören mit, was ich sage, und zeigen mir dementsprechend Werbung	WhatsApp ist jetzt auch Ende zu Ende verschlüselt
Selber schuld, wenn du Nudes schickst	E2E – was ist das, warum ist das wichtig?	*Fehler, die deine Mutter / Oma / weiblich gelesene Person macht*	Kein Backup, kein Mitleid
Telegram ist ein sicherer Messenger	Ich muss mir mein Passwort ja merken können	Für sensible Kommunikation nutze ich kein Smartphone	Antiviren-programme gibt’s ja auch kostenlos
Biometrische Entsperrung von Geräten ist viel praktischer	Das TOR-Netzwerk wird von Miss-brauchsdarstel-lungen, Militär und weiterer Gewalt dominiert	Betrugsmails erkennt man (NICHT) an der Rechtschreibung	Open-Source-Tools sind weniger sicher als bezahlte Tools



HEINRICH BÖLL STIFTUNG
Gunda Werner Institut

„Ich habe nichts zu verbergen“

Wir alle haben etwas zu verbergen, Privatsphäre ist ein wichtiger Teil unserer Meinungs- und Persönlichkeitsbildung. Dass es etwas Schlechtes sei, „etwas zu verbergen“ zu haben, kommt aus dem Trend der letzten Jahrzehnte, in denen staatliche und unternehmerische Massenüberwachung zur neuen Normalsituation gemacht wurden. Firmen brauchen all deine Daten, um Profile so genau wie möglich anzulegen und zu verkaufen. Vor dem Staat musst du durch Gläsernheit beweisen, dass du nicht kriminell bist. Privatsphäre und ein Recht auf Geheimnisse zu haben und dafür zu kämpfen, wird ein immer wichtiger werdender politischer Konflikt.

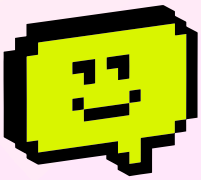
„Ich beschäftige mich nicht mit Sicherheit, weil ich davon überwältigt bin und mensch es eh nicht richtig machen kann“

(Cyber-)Security ist ein weites Feld, und es ist leicht, sich in Details und den vielen (manchmal auch gegensätzlichen) Meinungen zu verlieren und dann einfach aufzugeben. Das Zauberwort ist hier: durchhalten und geduldig mit dir selbst sein! Wir reden oft von „Security is a process“ (Sicherheit ist ein Prozess). Dazu gehört, neue Dinge zu lernen, aber vor allem alte Gewohnheiten zu verlernen. Und das braucht einfach Zeit. Versuche nicht, dein ganzes digitales Verhalten auf einmal umzustellen, das führt nur zu Frustration. Such dir ein Werkzeug aus und baue es in deinen Alltag ein, bis du dich daran gewöhnt hast, dann geh zum nächsten über.

„Apps hören mit, was ich sage, und zeigen mir dementsprechend Werbung“

Viele berichten davon: gerade mit Freund*innen über Produkt XYZ geredet, schon erscheint Werbung dafür in deinem Social-Media-Stream oder in der Seitenspalte einer Website. Haben die Apps bei eurem Gespräch direkt mitgehört? Das ist unter normalen Umständen nicht üblich (es gibt aber Ausnahmen, z. B. durch #stalkerware). Was du hier erlebst, ist die Macht des Werbetrackings und der Metadaten.

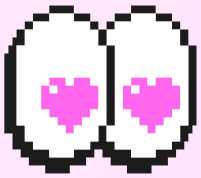
Tracker sind nicht nur in Social-Media-Apps, sondern laufen im Hintergrund von fast allen Websites im Internet. Beim „targeted advertising“ (zielgerichtete Werbung) wird den Werbekund*innen ein Platz in deinem Social-Media-Stream verkauft. Die Werbenetzwerke wissen aufgrund deines bisherigen Verhaltens – und des Verhaltens deiner Freundinnen und wiederum deren Freund*innen – was gerade gern angeklickt bzw. gekauft wird. Passen die Profile gerade gut zusammen, bekommst du auch die Werbung. Es fällt dir nur stärker auf, weil ihr gerade darüber geredet habt. Bei vielen anderen Produkten denkst du anders oder gar nicht darüber nach.



„WhatsApp ist jetzt auch Ende-zu-Ende-verschlüsselt“

Stimmt! Aber das ist nicht die ganze Geschichte, und wie immer geht es ums Detail. WhatsApp verschlüsselt den eigentlichen Inhalt deiner Nachrichten, aber nicht die Metadaten. Metadaten sind Infos wie: wem du wann die Nachricht schreibst, wie lang die Nachricht ist, ob sie einen Anhang hat etc. Aus diesen Metadaten lassen sich Muster erkennen, die viel über dein Verhältnis zu dieser Person verraten – gerade, wenn mensch diese Muster mit denen anderer vergleicht. So kann WhatsApp bzw. Meta dann, ohne die eigentlichen Nachrichten zu kennen, ziemlich genau sagen, mit wem du wann schreibst.

Das muss aber nicht so sein: Der Messenger Signal, zum Beispiel, verschlüsselt ebenfalls Ende-zu-Ende und speichert erst gar keine Metadaten!



„Selber schuld, wenn du Nudes schickst“

Hier kommt klassisches, patriarchales Victim-Blaming: Du bist als Opfer schuld, wenn du selbstbestimmt mit deinem Körper umgegangen bist, analog zu: „Die ist doch selbst schuld, wenn sie sich so anzieht“. Natürlich weißt du vorher nicht, ob sich Chatpartner*innen irgendwann als Creeps oder Arschlöcher herausstellen. Das heißt aber nicht, dass Cybersecurity ohne Nudes auskommen muss!

Coding Rights hat schon vor Jahren ein Mini-Zine mit Tipps herausgegeben und die sind immer noch aktuell. [1]

„E2E – was ist das, warum ist das wichtig?“

E2E ist die Abkürzung für Ende-zu-Ende-Verschlüsselung. Konkret beschreibt sie das Konzept, dass eine Nachricht, die du an eine andere Person schickst, auch nur von euch beiden (bzw. euren Endgeräten, also Smartphone, Laptop etc.) gelesen werden kann. Dabei ist es egal, welche Infrastruktur die Nachricht auf ihrem Weg durchquert oder auf welchen Servern in welchen Ländern sie zwischengespeichert wird – die Verschlüsselung sorgt dafür, dass der Inhalt zwischen euch privat bleibt.

Dieses Konzept ist mehr und mehr staatlichen Akteuren ein Dorn im Auge, denn sie wollen wissen, worüber sich die Bevölkerung unterhält, oft unter dem Vorwand der Terrorprävention. Medial wird hier von Chatkontrolle

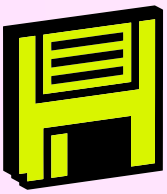
geredet und im Diskurs der Schutz von Minderjährigen instrumentalisiert. Gemeint ist aber, dass Softwarefirmen mit Absicht Hintertüren in die Verschlüsselung einbauen sollen, damit Polizei & Co. tiefgreifenderen Zugriff auf private Inhalte bekommen und der staatliche Überwachungsapparat weiter ausgebaut werden kann.

Fehler, die deine Mutter/Oma/weiblich gelesene Person macht

Eigentlich klar, aber es lohnt sich, es immer wieder zu sagen: Frauen und weiblich sozialisierte Menschen – egal welchen Alters – sind nicht automatisch schlechter im Umgang mit Technologien. Es sind strukturelle Unterdrückungsmechanismen, die dafür gesorgt haben, dass sich Generationen von Frauen weniger mit Technologie auseinandergesetzt haben und ihnen schlichtweg der Zugang verweigert wurde.

Gerade auch deswegen sehen wir heute immer noch Technologien als Tools für systematische Unterdrückung von Frauen und Gender-Minderheiten; wir reden von geschlechtsspezifischer digitaler Gewalt. Wissensteilung und Aneignung von Technologien sind deswegen die wichtigsten feministischen Praxen des 21. Jahrhunderts.

„Kein Backup, kein Mitleid“



Ein Kommentar, der noch keiner Person geholfen hat. Wichtig ist: Stell sicher, dass du von Daten, die dir wichtig sind, regelmäßig eine Kopie machst. Im ersten Schritt ist es wichtig, dass du überhaupt Kopien erstellst und das entweder zur Gewohnheit machst oder – idealerweise – automatisierst.

Kopien kannst du auf physischen Datenträgern oder in Clouds speichern, auch ein verschlüsseltes Backup ist möglich. Denk aber auch daran, wie du wieder an die Daten kommst bzw. im Fall eines Festplattenausfalls oder verlorenen Telefons die Daten wiederherstellst.

„Telegram ist ein sicherer Messenger“

Telegram-Chats sind standardmäßig nicht Ende-zu-Ende-verschlüsselt. Nur sogenannte „geheime Chats“ verschlüsseln die verschickten Inhalte. Eine Verschlüsselung von Gruppenchats ist gar nicht möglich. Alle unverschlüsselten Inhalte liegen auf den Servern von Telegram. Seit 2022 gibt es Hinweise, dass ukrainische/russische Aktivist*innen in Schwierigkeiten gerieten. [2, 3]

„Ich muss mir mein Passwort ja merken können“

Jein. Es gibt Hilfsmittel – sogenannte Passwortmanager. Diese verwalten für dich lange, komplexe und vor allem individuelle Passwörter. Passwörter, die wir uns einfach merken können, sind häufig Passwörter, die leicht zu knacken sind. Dazu gehören alle bekannten Wörter und Namen, auch wenn sie mit Ziffern am Ende oder Ersetzungen (wie der 4 für ein A) benutzt werden.

Alternativ zu komplexen Passwörtern kannst du auch lange sogenannte Passphrasen verwenden. Dabei kombinierst du mindestens fünf wahllos gewählte Worte. Aber ja: Du wirst dir mindestens noch ein Passwort merken müssen, um dein Gerät zu entsperren, und je nach Einstellungen noch eins für deinen Passwortmanager. Alle anderen Passwörter kannst du beruhigt vergessen.

„Für sensible Kommunikation nutze ich kein Smartphone“

Häufig ist direkte verbale Kommunikation vor Ort tatsächlich eine gute Wahl, aber das ist ja nicht immer möglich. Smartphones bieten im Gegensatz zu einem Festnetzanschluss oder einem alten Tastenhandy die Möglichkeit, verschlüsselte Messenger zu verwenden. Auch die 4G- und 5G-Netze bieten höhere Sicherheitsstandards als die älteren Netze. Klassische SMS werden unverschlüsselt verschickt.

E-Mails können je nach Anbieter des E-Mail-Kontos ganz unterschiedliche Sicherheitsstandards haben, aber in der Regel werden sie standardmäßig nicht versendet, wenn der minimale Sicherheitsstandard nicht erreicht ist.

„Antivirenprogramme gibt’s ja auch kostenlos“

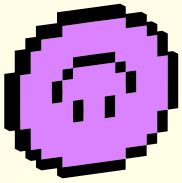
Diese Aussage bezieht sich vor allem auf Windows-Nutzende. Wenige Antivirenprogramme schützen hier wirklich. Einige verkaufen auch Lücken bzw. Zugang zum System, auf dem sie installiert wurden, z. B. für Werbung. Zusätzlich verlangsamen sie Rechner, weil ihre Prozesse konstant im Hintergrund laufen.

In den meisten Fällen reicht es, Windows Defender (kommt schon mit Windows, nicht zu verwechseln mit ähnlich genannter Software!) laufen zu lassen und regelmäßig System- und Sicherheitsupdates zu machen.

„Biometrische Entsperrung von Geräten ist viel praktischer“

Eigene Geräte mit PINs oder Passcodes zu (ent-)sperren, ist ein wichtiger Schritt der physischen Gerätesicherheit. Seit mehreren Jahren können auch biometrische Marker wie Fingerabdruck oder Gesichtserkennung dafür genutzt werden und machen das Prozedere oft angenehmer.

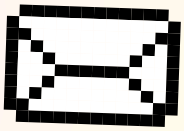
Je nach deiner Situation oder (aktivistischer) Arbeit sind die Entsperrmethoden aber rechtlich unterschiedlich: Die Polizei kann dich nicht dazu zwingen, ein Passwort oder einen -code einzugeben, aber sie darf (nach aktuellem Stand) deinen Finger auf den Scanner legen oder das Telefon zum Entsperren vor dein Gesicht halten.



„Das TOR-Netzwerk wird von Missbrauchsdarstellungen, Militär und weiterer Gewalt dominiert“

Das TOR-Netzwerk, medial auch gern „Darknet“ genannt, wird oft im schlimmsten Sinne als rechtsfreier Raum dargestellt. Aber das ist eine einseitige Darstellung, die oft aus dem gleichen Lager wie die #chatkontrolle kommt. Beim TOR-Netzwerk handelt es sich erstmal um Internet-Infrastruktur, die es dir ermöglicht, anonym auf Inhalte zuzugreifen. Das unterstützt auch journalistische, aktivistische und forschende Arbeit von Menschen, die in Ländern mit Internetzensur leben oder überwacht werden.

Aber es stimmt auch, dass dort eine große Menge Missbrauchsdarstellungen – vor allem von Kindern und FLINTA* – zugänglich sind.



„Betrugsmails erkennt man (NICHT) an der Rechtschreibung“

Betrugs- oder Phishingmails werden häufig von Nicht-Muttersprachler*innen als Teil einer größeren Struktur geschrieben und waren deswegen oft sprachlich nicht korrekt. In Zeiten von KI-Sprachmodellen ist dieses Merkmal allein aber längst nicht mehr tauglich.

Viel besser eignet sich ein genauer Blick auf die Absenderadresse (häufig hinter einem falschen Klarnamen versteckt) und die vermeintliche Dringlichkeit der Nachricht („jetzt klicken oder der Account wird gesperrt!“). Nicht sicher, ob Phishing oder nicht? Auf gar keinen Fall direkt auf Links in der Mail klicken! Lieber den Linktext auswählen und manuell kopieren, um den sichtbaren Link zu nutzen, nicht den unsichtbaren HTML-Teil. Oder, noch besser: Dich separat in den Account, um den es gehen soll, einloggen und nachsehen.

Du hast die Mail an deine Arbeitsadresse bekommen? Leite sie an die IT-Abteilung (falls vorhanden) weiter – vielleicht haben Andere in der Organisation die gleiche bekommen, und sie können eine Warnung rausgeben.

„Open-Source-Tools sind weniger sicher als bezahlte Tools“

Open Source bezeichnet (unter anderem) die Offenlegung des Quellcodes eines Programms. Das erlaubt es Menschen, zu sehen und zu lernen, wie das Programm funktioniert, aber auch Fehler und Sicherheitslücken zu entdecken und ggf. auszubeuten. Manche denken deswegen, dass Open-Source-Software unsicherer sei als ihre geschlossenen Gegenstücke. Das ist aber nicht zwangsläufig der Fall!

Denn wenn viele Augen auf den Code schauen, fallen Lücken viel früher auf und werden schnell geschlossen – oder es wird zumindest öffentlich darüber geredet, und Betroffene können sich informieren. Bei geschlossener Software reden wir dagegen gern von „security through obscurity“ (Sicherheit durch Verschleierung): Software wird als sicher wahrgenommen und verkauft, weil die Lücken nicht bekannt gemacht werden. Gerade diese Lücken werden dann aber oft in Viren, Ransomware, Spyware oder Staatstrojanern ausgenutzt!

1 Coding Rights, 2016: Safer Nudes (Quelle: https://codingrights.org/en/project-item/safer-nudes-2/, letzter Zugang am 27.11.2025)

2 Roman Anin, Nikita Kondratyev, 2025: Telegram, the FSB, and the Man in the Middle (Quelle: https://istories.media/en/stories/2025/06/10/telegram-fsb/, letzter Zugang am 27.11.2025)

3 Fabian Sommavilla, Fabian Schmid 2024: Telegram, das „letzte Fenster nach Moskau“, genutzt von Propagandisten und Regimekritikern. der Standard (Quelle: https://www.derstandard.de/story/3000000223060/telegram-das-letzte-fenster-nach-moskau-genutzt-von-propagandisten-und-regimekritikern, letzter Zugang am 27.11.2025)

Mehr Infos zum Thema feministische Cybersecurity in unserer Einführung:

https://www.gwi-boell.de/2024/08/30/was-bedeutet-feministische-cybersecurity