CHECKLISTE FÜR MEHR SICHERHEIT IM INTERNET

1. HARDWARE UND SOFTWARE SCHÜTZEN

+/- Regemäßige Updates für die Software herunterladen

- Überprüfen, ob das Gerät auf dem neusten Stand ist und ob die Software richtig und gut geschützt ist
- Alte Modelle, die man nicht mehr updaten kann, sind unsicher und sollten daher nicht datenbezogen verwendet werden.

+/- Regelmäßige Backups

- Wenn trotz aller Sicherheitsmaßnahmen mal Daten verloren gehen, kann Du diese durch ein Backup einfach wieder herstellen.

+/- Standartbenutzer zusätzlich zum Admin-Account

- Der erste Account bei den meisten Softwares ist ein Admin-Account. Wird der Admin-Account angegriffen, gehen die Daten dort verloren. Indem man sich einen Standartbenutzeraccount ohne Administratorenrechte anlegt, kann man die Daten schützen. (Man kann sich die Administratorenrechte kurzzeitig durch Eingabe eines Passwort erlangen.)

+/- Interne und Externe Speichermedien schützen

- Wenn man z.B. einen unverschlüsselten USB-Stick verliert kann jeder einfach auf die enthaltenen Daten zugreifen. Deshalb sollte jeder seine externe Speichermedien zu mindestens mit einem Passwort schützen.
- Genauso kann man auch Dateien besonders auf dem Computer schützen
- Programme, wie z.B. Veracrypt, entsprechen dann einem Tresor auf dem PC/USB-Stick/Festplatte/… , der durch ein Passwort geöffnet werden

+/- Virenschutz

- Schütze dich vor jeglichen Befall von Viren mit Virenblockern

2. Passwörter und Authentifizierung

+/- Sichere Passwörter haben: mind. 16 Zeichen, Groß- und Kleinschreibung, Zahlen, Sonderzeichen, Umlaute, beinhalten keine privaten Daten und es sollte inhaltlich keinen Sinn ergeben

- Hier kannst du Passwörter ausprobieren (benutze nicht dein Eigenes):Passwort-Sicherheit-Check: Wie sicher ist mein Passwort? (checkdeinpasswort.de)

+/- Für jeden Account ein anderes Passwort benutzen

- Sonst kann man mit einem Passwort gleich mehrere Accounts knacken
- Zum Merken kannst du Passwort-Manager benutzen, z.B.: Keepasstwo(android), sticky password, Bitwarden

+/- 2-Faktor-Authentifizierung

- So kannst du deinen Account extra sicher machen.
- Nach dem Du dein Passwort auf der Webseite/etc. eingegeben hast, wird ein SMS an dein Handy geschickt. Erst wenn Du auf deinem Handy bestätigt hast, dass es wirklich Du bist, der die anfrage gestellt hat, wird Dir der Zutritt zur Webseite erlaubt.
- Programme hierfür sind, z.B.: google authenticator, authy

3. Sicher unterwegs im Internet

+/- Sichere Suchmaschinen benutzen

- Viele Suchmaschinen sammeln deine Daten, auch wenn Du es nicht merkst. (z.B.: Google, Ecosia, bing, yahoo, ...)
- Sicherer sind z.B.: Startpage.com, duckduckgo.com

+/- Datenschutzerklärungen lesen

- Dort gibt es viele wichtige Informationen, aber man ist meistens zu faul die Erklärung zu lesen und bestätigt sie einfach, weil sie viel zu lang ist. Lies es!
- Eine Kurzfassung zu der Datenschutzerklärung vieler Webseiten und Programme findest du bei tosdr.org

+/- Nur sichere Verbindungen benutzen

- http-Seiten sind unsicher und veraltet: Du solltest dort keine persönlichen Daten angeben oder

  sie am besten ganz meiden
- Das s in https steht für Secure und ist demzufolge auch sicherer, achte auch bei anderen Programmen auf ein S am Ende, z.B. POP3s

+/- Cookies ablehnen/ nur essenzielle Cookies zulassen

- Das Annehmen von Cookies erlaubt dem Webseitenbetreiber persönliche Daten über Dich zu sammeln.

+/- Add-/Tracker-Blocker verwenden

- Werbungen sind nicht nur nervig, sondern sammeln auch Informationen über Dich.
- Ein Beispiel-Programm ist.: Blockada

+/- VPN-Dienste benutzen

- Durch solche Dienste wird deine “Spur” im Internet verschleiert.

+/- Sichere Messenger-Dienste benutzen

- Sie sollten mit End-zu-End-Verschlüsselung ausgestattet sein und auch sonst keine Daten sammeln.
- Beispiele sind : Signal, Threema

+/- Achte auf verdächtige Mails/SMS/...

- Offensichtlich verdächtig sind Mails von Prinz xy, der um Geld bittet, aber auch andere Mails, wie Gewinnspiele, etc. Können gefährlich sein.
- Generell solltest Du nicht auf Links klicken, die Du nicht geprüft hast

4. Fake News

+/- Es gibt viele Fake News im Internet, deshalb solltest Du die Webseite (Impressum, Autor,...) und die Informationen gegen checken

+/- Prüfe deine Medienkompetenz mit dem bpb Newstest

+/- Spiele zum Thema:

- Fake News selber erstellen (am besten erst ab 15): getbadnews.de, fakeittomakeit.de
- Fake News erkennen: swrfakefinder.de