Checkliste für die digitale Selbstverteidigung

IT-Sicherheit

☑ **Ich habe sichere Passwörter für alle relevanten Accounts (insbesondere E-Mail-Accounts!)**
Was ein sicheres Passwort ist und worauf du achtest musst, hat das BSI hier zusammengefasst: gruenlink.de/1zvy

☑ **Ich nutze einen Passwortmanager**
Passwortmanager verwalten deine Passwörter für dich. Hier findest du alles, was du wissen musst: gruenlink.de/2bvr

☑ **Ich habe relevante Accounts mit einer Zwei-Faktor-Authentifizierung (2FA) geschützt**
Mit der zweistufigen Authentisierung wirst du jedes Mal aufgefordert, einen Sicherheitscode einzugeben oder die Anmeldung zu bestätigen, wenn du dich mit deinem Passwort bei einem deiner Accounts anmeldest. So kannst du verhindern, dass sich jemand Unbekanntes zum Beispiel in deine Accounts auf den Sozialen Plattformen einloggt und Schaden anrichtet. Schaue in den Benutzereinstellungen deiner Accounts nach, wie du die 2FA einstellen kannst. In unserer Broschüre „Grün und Sicher im Netz" findest du weitere Infos: gruenlink.de/266d

☑ **Ich habe überprüft, ob meine E-Mail-Adresse im Netz geleakt wurde**
Es gibt mehrere Dienstleister*innen im Internet, mit denen du prüfen kannst, ob du von einem Passwort-Leak betroffen bist. Diese Dienstleister*innen bieten teilweise ein Abonnement an, sodass du über neue Leaks informiert wirst und dadurch zeitnah das betroffene Passwort ändern kannst. Vertrauenswürdige Dienstleister*innen sind beispielsweise:

- Hasso Plattner-Institut: gruenlink.de/22wz
- Mozilla Firefox: gruenlink.de/22x1
- Have I Been Pwned: gruenlink.de/22x2

☑ **Ich melde mich nur in sicheren WLAN-Netzen an**
Öffentliche WLAN-Hotspot sind oft unverschlüsselt. Dass unverschlüsselte Netzwerke Gefahren bergen und was du tun kannst, zeigt dieses kurze Video vom BSI: bsi.bund.de/SharedDocs/Videos/DE/BSI/VerbraucherInnen/WLAN.html

☑ **Ich gehe sparsam mit sensiblen Daten um**
Das Prinzip der Datensparsamkeit bedeutet, dass du achtsam mit persönlichen Daten wie z.B. deiner Mobilfunknummer oder der privaten Anschrift umgehst. Ein paar wichtige Punkte dazu werden in „Grün und sicher im Netz" erläutert: gruenlink.de/266d

☑ **Ich weiß, was Phishing bedeutet und wie ich damit umgehe**
Wäge gut ab, auf welche Links du im Netz klickst. Phishing per E-Mail oder SMS ist eine bekannte Methode von Hacker*innen, um an deine Daten zu kommen. Das Landeskriminalamt Niedersachsen hat hierzu wichtige Punkte zusammengefasst: polizei-praevention.de/themen-und-tipps/straftaten-im-netz/phishing

☑ **Ich halte meine Endgeräte, Software und Apps immer auf dem aktuellsten Stand (mache Updates)**
Software und Apps, die du nicht nutzt, solltest du deinstallieren, um die Angriffsmöglichkeiten zu reduzieren. Die Software, die du weiterhin nutzt, sollte sich automatisch updaten. Wie du das einstellen kannst und weitere Tipps findest du hier: gruenlink.de/2cqu

Soziale Plattformen

☑ **Ich habe öffentliche Seiten auf Sozialen Plattformen angelegt und trenne diese von meinen privaten Accounts**

Bei Facebook kannst du eine „Seite" erstellen, die du ausschließlich für die öffentliche Kommunikation nutzt. Auf anderen Plattformen musst du dafür einen weiteren Account anlegen. Die privaten Accounts solltest du ausmisten, damit wirklich nur Menschen an private Informationen und Bilder von dir und deinen Nächsten kommen, denen du vertraust.
Weitere Infos zum Thema findest du in „Grün und Sicher im Netz" auf Seite 19.

☑ **Ich habe die Privatsphäre meiner Accounts auf den Sozialen Plattformen überprüft**

Sorge über die Einstellungen dafür, dass deine privaten Accounts nichts öffentlich posten und stelle auch alte Posts auf privat. Bei Facebook kannst du beispielsweise einen Privatsphäre-Check durchführen:
facebook.com/privacy/checkup/?source=settings_and_privacy

Weitere Infos zum Thema findest du in „Grün und Sicher im Netz" ab Seite 20.

☑ **Ich habe meine Google-Einträge gecheckt und ggf. Löschanträge gestellt**

Google dich selbst! In manchen Fällen lassen sich die Einträge in Suchmaschinen über eigene Accounts etwa in den Einstellungen bei LinkedIn, XING, Facebook und Co. entfernen. Ist das nicht möglich, versuch es mit Googles Antragsformular zur Entfernung personenbezogener Daten:
gruenlink.de/1zwq

HateAid unterstützt dich auch bei der Entfernung von Google-Einträgen.

☑ **Ich habe einen Notfallplan für rechte Angriffe und Shitstorms (und mögliche Vertrauenspersonen)**

Überlege dir, wie du im Notfall reagieren möchtest und wen du wann kontaktierst – erstelle einen Notfallplan. Was ist überhaupt ein Notfall für dich und ab wann ist ein Shitstorm ein Shitstorm?
Als Kandidat*in oder Mandatsträger*in kannst du dir ein kleines Team aus Unterstützer*innen zusammenstellen. Kläre, wer deine Accounts auf den Sozialen Plattformen übernehmen kann, solltest du im Netz attackiert werden. Stelle dir eine Sammlung von wichtigen Kontakten und Notfallnummern zusammen.

☑ **Ich habe auf meinen Seiten auf den Sozialen Plattformen Wortfilter eingerichtet**

Stelle auf deinen Accounts Wortfilter ein und bewirke, dass Hasskommentare zuerst ausgegraut erscheinen, bevor du entscheidest, ob sie öffentlich zu sehen sein sollen. Wie du das einrichtest, findest du ebenfalls in „Grün und Sicher im Netz" ab Seite 20.

☑ **Ich habe eine Netiquette auf meinen Seiten auf den Sozialen Plattformen und setze sie konsequent durch**

Für deine öffentlichen Accounts empfehlen wir dir eine Netiquette zu veröffentlichen, auf die du dich beziehen kannst, wenn du Pöbler*innen blockierst oder ihre Kommentare löschst.
Als Inspiration findest du hier den Vorschlag des Bundesverbands, den du gerne kopieren darfst:
gruene.de/artikel/8-regeln-fuer-eine-demokratische-diskussionskultur-1

Sicherheit vor Ort

☑ **Ich habe eine Auskunftssperre und / oder Übermittlungssperre beantragt, weil ich im Wahlkampf besonders gefährdet bin**
Eine Auskunftsperre verhindert, dass die Meldebehörde deine Privatanschrift herausgeben darf. Informiere dich im Netz oder vor Ort bei deiner Meldebehörde, was du für den Antrag benötigst. Screenshots von Hassnachrichten und Drohungen können oft unterstützend eingereicht werden.

☑ **Meine Adresse und private Telefonnummer sind nicht im Netz zu finden (etwa im Impressum meiner Webseite)**
Verzichte darauf, deine personenbezogenen Daten digital zu verschicken oder zu veröffentlichen. Wende dich an beratung@hateaid.org und frage nach einem Privatsphäre-Check. So erfährst du, wie leicht man im Netz an deine persönlichen Daten kommt. Oft steht die private Anschrift im Impressum von grünen Websites. Ersetze diese durch die Anschrift deiner Geschäftsstelle.

☑ **Meine Sprechzeiten bekommen Interessent*innen nur auf Nachfrage / nach Anmeldung**
Auch deine Sprechzeiten sollten nicht auf einer grünen Website zu finden sein. Verschicke diese nur auf Nachfrage an Bürger*innen, die dir nicht schaden wollen.

Weitere Informationen und nützliche Tipps:

- Allgemeine Tiipps: netzpolitik.org/2018/kleines-ein-maleins-der-digitalen-selbstverteidigung/
- Hier findest du auch andere Plattformen wie Tiktok oder Snapchat: klicksafe.de/service/schule-und-unterricht/leitfaeden/
- Infobroschüre für Mandatsträger*innen: verband-brg.de/wp-content/uploads/2021/04/Drohungen_gg_Politik_Verwaltung_DS_WEB.pdf

Notfallkontakte

In Notfällen und akuten Bedrohungslagen bitte umgehend die Polizei (110) kontaktieren!
Oder wende dich an deine zuständige Polizeidienststelle:
polizei.de/Polizei/DE/Home/home_node.html

Bei IT-Notfällen (Hackerangriff, Datenklau usw.) findet ihr hier die Notfallnummer vom CERT der Netzbegrünung: cert.netzbegruenung.de/NB-CERT-Notfallkarte.pdf
(für einen Rückruf unbedingt auf AB sprechen!)

Bei einem aufziehenden Shitstorm lohnt es sich die grüne Netzfeuerwehr als Unterstützung zu aktivieren: gruene.de/aktionen/mach-mit-bei-unserer-netzfeuerwehr

Hateaid bei digitaler Gewalt: hateaid.org

Opferberatungsstellen: verband-brg.de/beratung/#beratungsstellen

Mobile Beratungsstellen gegen Rechtsextremismus: bundesverband-mobile-beratung.de/angebote/vor-ort

Unsere hauseigene Anlaufstelle gegen Rechts vom Bundesverband: Mail an anlaufstelle@gruene.de