Politik und Wirtschaft unterrichten

WOCHENSCHAU

Checkheft Sek. I

DATENSCHUTZ

Checklisten und Infos zu

- Sozialen Netzwerken
- Cybermobbing
- Privatsphäre im Internet
- AGB und Passwörtern

WOCHEN SCHAU VERLAG

Liebe Schüler*innen,

ein Leben ohne Smartphone und Internet könnt ihr euch vermutlich nicht vorstellen. Beides bietet unglaublich viele Möglichkeiten: Das Handy ist Kamera, MP3-Player, Telefon, Fernseher und Computer in einem. Über Chatdienste kommuniziert ihr mit euren Freund*innen, Naviagationssysteme zeigen euch, wo es langgeht und mit Spielen vertreibt ihr die Langeweile.

Doch was weiß das Netz über euch? Mit diesem Checkheft könnt ihr prüfen, wie es um die Sicherheit eurer Daten bestellt ist.

Auf den folgenden Seiten findet ihr Tipps, wie ihr euch und eure Daten im Internet schützen könnt. Schritt für Schritt überprüft ihr, ob ihr euch sicher im Netz bewegt und wo ihr vorsichtiger sein solltet.

Datenschutz

Dieses Symbol wird euch im Checkheft häufiger begegnen. Die Zahl hinter dem kleinen Buch verrät euch, auf welchen Seiten ihr im WOCHENSCHAU-Schülerheft mehr über das Thema erfahrt.

Das Checkheft ist eine Sonderbeilage zum WOCHENSCHAU-Themenheft „Datenschutz" (2015). Die digitale Version des Checkhefts (2020) wurde leicht überarbeitet.

Datenschutz – dein Checkheft

Sichere Passwörter – so geht's!

Checkliste 1 Passwort

- ☐ Denk dir für jeden Account ein eigenes Passwort aus.
- ☐ Jedes Passwort hat mindestens acht Stellen.
- ☐ Dein Passwort besteht aus Groß- und Kleinbuchstaben, Zahlen und Sonderzeichen (z. B. ?!%$&), die sich abwechseln (z. B. 2oSTer?hASe7).
- ☐ Verwende keine Namen oder Daten, die mit dir zu tun haben (z. B. Namen von Freunden, Familienmitgliedern, Haustieren, deinen Geburtstag etc.).
- ☐ Dein Passwort steht in keinem Wörterbuch.
- ☐ Merk dir dein Passwort mithilfe eines Satzes:
  S&d7Zsi3! = Schneewittchen und die sieben Zwerge springen im Dreieck!
- ☐ Verrate niemandem deine Passwörter.
- ☐ Du willst ein Passwort aufschreiben? Dann bewahre die Notiz sicher auf.
- ☐ Ändere deine Passwörter regelmäßig.

Soziale Netzwerke und Chatrooms 4–5, 14–16

Checkliste 2 Privatsphäre und Datensparsamkeit

- ☐ Achte darauf, dass dein Profil nicht öffentlich ist und somit nur Personen Zugang dazu haben, die mit dir verlinkt sind bzw. mit denen du befreundet bist. In sozialen Netzwerken kannst du das über die Privatsphäreeinstellungen regeln.

- ☐ Gib keine persönlichen Daten an (z. B. Adresse, Telefonnummer, E-Mail-Adresse, Geburtstag).

- ☐ Sei bei Freundschaftsanfragen misstrauisch. Nimm nur Anfragen von Leuten an, die du wirklich kennst. Verschicke umgekehrt keine an Fremde.

- ☐ Überlege, ob du alle Inhalte für alle Freund*innen sichtbar machst oder ob du die „Freund*innen" nicht besser in Gruppen einteilst: Bekannte, Freund*innen, enge Freund*innen, Familie.

- ☐ Nimm es ernst, wenn das soziale Netzwerk die Privatsphäreeinstellungen ändert. Lies dir die Änderungen durch und passe dein Profil entsprechend an.

☐ Gib deinen Namen in Suchmaschinen (yasni, Google, 123people) ein und teste so, ob jemand etwas über dich ins Netz gestellt hat.

☐ Stelle deine Privatsphäreeinstellungen so ein, dass dein Profil nicht über Suchmaschinen auffindbar ist.

Checkliste 3 Nicknames und Benutzernamen

In Chatrooms, Blogs und Foren tauschst du dich mit Menschen aus, die du möglicherweise gar nicht kennst.

Deshalb gilt:

☐ Sei vorsichtig und melde dich mit einem Spitznamen („Nick") an.

☐ Dein „Nick" hat nichts mit deinem echten Namen, Alter oder Geburtstag zu tun. „Alex15" oder „Mariechen2001" sind beispielsweise keine guten Ideen.

☐ Benutze deinen Nickname nicht, um andere im Netz anonym zu beleidigen oder bloßzustellen. Das ist nicht nur feige, sondern kann in manchen Fällen sogar strafbar sein.

Checkliste 4 Fotos, Videos und Posts

Wenn du Bilder, Filme oder deinen Status posten willst, dann frag dich vorher:

- ☐ Würdest du dasselbe auch wildfremden Menschen auf der Straße erzählen?
- ☐ Soll das wirklich jede*r wissen oder sehen?
- ☐ Würdest du dieses Foto auch ans Schwarze Brett in deiner Schule hängen, sodass alle es anschauen können?
- ☐ Darfst du das Bild/Video überhaupt hochladen? Oder hast du nicht das Recht dazu, weil es jemand anderes gemacht hat?
- ☐ Ist eine Person auf dem Foto/Video zu sehen, die vielleicht nicht möchte, dass du das von ihr postest?

Wichtig: Poste keine Fotos und Videos öffentlich, weil sie sonst jede*r herunterladen kann.

Weißt du, wer alles Bilder von dir geteilt hat?
So verschaffst du dir einen Überblick darüber:

- ☐ Überprüfe, ob du auf Fotos verlinkt wurdest.
- ☐ Schau dir die Fotoalben deiner Freund*innen an.
- ☐ Bitte Leute, Bilder von dir zu löschen, wenn du findest, dass diese nicht online sein sollten.

Bewegungsprofile

Natürlich ist es nett, wenn du bei Facebook oder Instagram siehst, dass Freund*innen gerade in der Nähe sind und ihr euch spontan treffen könnt.

Beachte: Möchtest du wirklich, dass alle deine Netzwerk-Freund*innen wissen, wo du gerade bist? Oder dass Internetanbieter nachvollziehen können, wo du gerne shoppen oder Eis essen gehst?

Nein? Dann lautet unser Tipp für dich: Überprüfe, ob du die GPS-Funktion oder Standortbestimmung deines Handys aktiviert hast. Falls ja – stell sie doch einfach mal aus.

Umgang mit Daten anderer

Jede*r entscheidet selbst, was er*sie im Netz über sich preisgibt. Das bedeutet auch: Nur wenn deine Freund*innen und Bekannten damit einverstanden sind, lädst du Bilder, Filme und private Infos von ihnen hoch und verlinkst sie auf Fotos, in Posts und bei Standortbestimmungen.

Und das geht gar nicht: Stell keine falsche Behauptungen oder Beleidigungen über jemanden ins Netz. Das ist unfair und du kannst dafür sogar angezeigt werden.

Apps

26–27

Apps sind praktisch oder einfach ein guter Zeitvertreib. Doch selbst wenn sie kostenlos sind, zahlst du häufig mit deinen Daten dafür: Wenn du eine App benutzt, hat sie möglicherweise Zugriff auf deine Kontakte, dein Telefonbuch und andere persönliche Infos (Name, E-Mail-Adresse, Profilbild, Geschlecht). Denk deshalb vor dem Download kurz nach, ob du die App wirklich brauchst.

Auf welche Daten Apps genau zugreifen, erfährst du übrigens in den Allgemeinen Geschäftsbedingungen (AGB).

Wissenswertes zu AGB

Wichtig: Den AGB musst du ausdrücklich zustimmen.

Checkliste 5 Was steht in den AGB?

☐ Wie viel eine App kostet.

☐ Wie alt du sein musst, um bestimmte Dienste (Facebook, WhatsApp etc.) zu nutzen.

☐ Welche Regelungen es gibt, wenn du etwas bestellt hast und es umtauschen oder ein Abo kündigen möchtest.

Das sind alles wichtige Infos. Darum solltest du dir die AGB genau durchlesen. Oft sind sie aber sehr kompliziert geschrieben.

Dein Durchblick bei den AGB:

☐ Lies zumindest die Kurzfassung der AGB, wenn es eine gibt.

☐ Durchforste die AGB nach bestimmten Wörtern wie z. B. Kosten, Euro, Daten, Alter, Kündigung, Rücktritt, Widerruf, Dritte etc.

So filterst du die wichtigsten Infos heraus und kannst sichergehen, dass du nicht aus Versehen z. B. eine teure App herunterlädst.

Abofallen

Im Internet sind jede Menge Apps und Spiele umsonst. Doch Vorsicht – schnell tappt man auf vermeintlich kostenlosen Seiten in die Abofalle.

Ohne es zu merken, schließt du einen Vertrag ab und deine nächste Handyrechnung ist viel zu hoch.

Du hast zwar nichts gekauft, aber vermutlich bei einer App auf einen Werbebanner geklickt. Oder dich auf einer Website mit deinen Daten registriert, um z. B. an einem Gewinnspiel teilzunehmen. Und irgendwo in den AGB oder am Ende der Seite versteckte sich ein kleiner Hinweis, dass du dadurch ein Abo abschließt.

Und jetzt?

Erst einmal gilt: Seit August 2012 muss jedes Abo als solches klar zu erkennen sein. Ein Button weist mit den Worten „zahlungspflichtig bestellen", „kostenpflichtig bestellen" oder „kaufen" darauf hin. Außerdem werden die Kosten erläutert. Klickst du auf „anmelden", „bestellen" und „weiter", hast du noch keinem Vertrag zugestimmt.

Checkliste 6: Was tun bei einer Abofalle?

- ☐ Mach den Aboanbieter in Suchmaschinen ausfindig. Handelt es sich um Abzocke, wirst du im Internet entsprechende Meldungen dazu finden.

- ☐ Deine Eltern bezahlen die Rechnung nicht oder buchen das Geld wieder zurück, wenn es automatisch vom Konto eingezogen wurde.

- ☐ Zeitgleich reichen deine Eltern schriftlich Widerspruch ein – am besten per Einschreiben mit Rückschein. Wird das Geld über deine Handyabrechnung eingezogen, richtet sich der Widerspruch in der Regel an deinen Mobilfunkanbieter.

- ☐ Deine Eltern widerrufen vorsorglich den Vertrag. Dafür haben sie zwei Wochen Zeit, wenn sie über das Widerrufsrecht informiert wurden. Ein Widerruf ist übrigens nicht zu verwechseln mit einer Kündigung.

- ☐ Deine Eltern ignorieren nachfolgende Mahnungen. Für einen gerichtlichen Mahnbescheid gilt das allerdings nicht. Liegt der im Briefkasten, sollten deine Eltern sich juristischen Rat bei einem*einer Anwalt*Anwältin oder einer Beratungsstelle holen.

- ☐ Lass für dein Handy durch den Mobilfunkanbieter eine Drittanbietersperre einrichten. So verhinderst du, dass du in Zukunft noch einmal in eine Abofalle tappst.

Wichtig: Ohne Zustimmung deiner Eltern darfst du als Minderjährige*r keine Verträge im Internet oder am Telefon abschließen.

Denn diese „Fernabsatzverträge" sind laut Taschengeldparagraf ungültig: Du kannst nämlich nur Dinge kaufen, die du sofort von deinem Geld bezahlst.

Was das Internet über dich weiß

6–7, 10–11, 22–23

Du glaubst, mit deinen Daten kann niemand etwas anfangen? Dann beobachte mal die Werbeleiste auf Websites und in sozialen Netzwerken. Dort werden dir Produkte, Gruppen und Seiten vorgeschlagen, die dein Verhalten im Netz widerspiegeln – wie z. B. was du bei Suchmaschinen eingegeben hast, auf welchen Seiten du gesurft hast und was du über dich in sozialen Netzwerken preisgibst. Du verrätst also mehr über dich als du denkst. Doch was kannst du dagegen tun?

Checkliste 7 Privatsphäre

- ☐ Wie schon erwähnt: Geh sparsam mit deinen persönlichen Daten um und schalte die Standortbestimmung aus.
- ☐ Achte beim Surfen darauf, dass dein Browser keine Cookies zulässt. Denn diese kleinen Dateien verfolgen, was du im Internet treibst.
- ☐ Sollte eine Website ohne Cookies nicht funktionieren, kannst du in diesem Fall eine Ausnahmeerlaubnis erteilen.
- ☐ Lösche im Nachhinein Cookies. Dann weißt du allerdings nicht, welche Daten sie schon gesammelt haben oder ob ein Super-Cookie nicht weiterhin deine Aktivitäten beobachtet.
- ☐ Verwende Suchmaschinen, die auf Cookies verzichten und sich nicht merken, was du bei ihnen eingibst. Eine Liste solcher alternativen Suchmaschinen findest du auf Seite 19.

Cybermobbing

18–21

Mobbing ist nichts Neues. Auch früher wurden Leute bedroht, beleidigt oder lächerlich gemacht. Mittlerweile passiert dies jedoch häufig im Internet oder per Handy. Man kann nun andere beleidigen, ohne ihnen dabei ins Gesicht schauen zu müssen.
Das Problem ist, dass sich solche Attacken in sozialen Netzwerken, Foren oder Gruppen schnell verbreiten. Das Publikum ist viel

größer als auf dem Schulhof. Und stehen Posts, Fotos und Videos erst einmal im Netz, lassen sie sich nicht immer vollständig löschen. Die Täter*innen können zu jeder Tages- und Nachtzeit aktiv werden und müssen sich im Internet nicht zu erkennen geben. Betroffene fühlen sich oft wehrlos und vertrauen sich niemandem an. Dabei ist es wichtig, gegen die Täter*innen vorzugehen und sich Hilfe zu suchen.

Checkliste 8 Was tun bei Mobbing?

- ☐ Sprich mit deinen Eltern oder Lehrer*innen. Du musst dich für nichts schämen, denn der Fehler liegt nicht bei dir.
- ☐ Antworte auf keinen Fall auf Mobbing-Posts, -SMS oder sonstige Nachrichten. Das macht es meistens nur noch schlimmer.
- ☐ Lösche die Nachrichten nicht, denn sie sind Beweismaterial.
- ☐ Mach von den Posts Screenshots, wenn du mit Fotos oder in Gruppen, Foren usw. gemobbt wirst.

- ☐ Melde in sozialen Netzwerken den Beitrag bzw. den*die Täter*in und/oder sperre ihn*sie.
- ☐ Lass deine Eltern den Betreiber der entsprechenden Seite auffordern, die betreffenden Inhalte zu löschen.
- ☐ Suche im Internet auf Seiten für Mobbing-Opfer nach Rat.
- ☐ Gehe in ganz schlimmen Fällen zur Polizei.

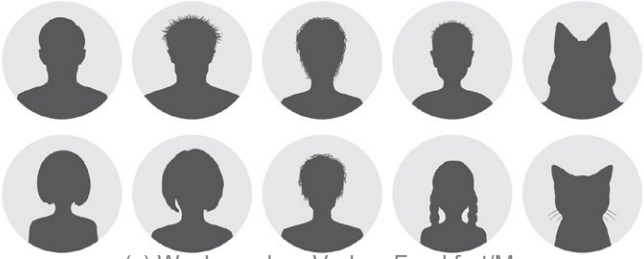
Cybergrooming

20

Im Netz kommst du auch mit Menschen in Kontakt, die du noch nie gesehen hast. Du weißt also nicht, wer sich hinter den Profilen verbirgt. Vielleicht heißt der nette Typ nicht Lucas – und ist auch nicht 15, sondern 50 Jahre alt. Tatsächlich gibt es Erwachsene, die sich im Internet als Jugendliche ausgeben. Sie wollen dein Vertrauen gewinnen, um sich an dich heranzumachen. Kommt es so zu sexueller Belästigung, nennt man das Cybergrooming.

Checkliste 9 Schutz vor Cybergrooming

- ☐ Glaub nicht alles, was andere über sich erzählen und verrate nicht zu viel von dir selbst – wie z. B. deine Adresse und wo du zur Schule gehst.
- ☐ Schicke Fremden keine Bilder von dir.
- ☐ Lass am Anfang die Webcam aus und schalte sie auch nicht ein, wenn dein Chatpartner keine hat.
- ☐ Brich Kontakte ab, die dir nicht geheuer sind – z. B., wenn jemand wissen will, ob du allein zu Hause bist.
- ☐ Informiere deine Eltern oder Lehrer*innen, wenn Leute dich ausfragen, zweideutige Anmerkungen machen, dir Nacktfotos schicken oder wollen, dass du dich vor der Kamera ausziehst.
- ☐ Schalte gemeinsam mit deinen Eltern die Polizei ein, wenn dich jemand sexuell belästigt hat.



Sexting

Mit Sexting-Bildern und -Videos sind Fotos und Filme gemeint, auf denen du in aufreizenden Posen und leicht bekleidet oder nackt zu sehen bist. Darunter fallen also keine Bilder aus dem Freibad oder vom Strand. Solche Dateien können schnell in die falschen Hände geraten und sich dann im Netz verbreiten.

Checkliste 10 Schutz vor Sexting

- ☐ Verschicke solche Bilder und Videos von dir auf keinen Fall.
- ☐ Poste sie niemals in Gruppen.
- ☐ Sei sogar bei privaten Nachrichten an deine*n Freund*in vorsichtig. Du kannst nie wissen, ob er*sie die Datei für sich behält oder weiterverschickt.
- ☐ Und versende nie Sexting-Fotos und -Filme von anderen, denn umgekehrt wäre dir das sicherlich auch peinlich.

Foto: © Pro Juventute

Weiterführende Links

Alternative Suchmaschinen
www.duckduckgo.com
www.bing.com
www.ixquick.com
www.metager.de
www.semager.de
www.startpage.com/deu
www.yacy.net/de

Weitere Internetseiten für Jugendliche zu dem Thema
www.chatten-ohne-risiko.net
www.datenparty.de
www.digitale-helden.de
www.handysektor.de
www.internauten.de
www.juuuport.de
www.youngdata.de

Anlaufstellen für Opfer von Cybermobbing
www.bündnis-gegen-cybermobbing.de
www.cybermobbing-hilfe.de
www.mobbingberatung-bb.de/tag/cybermobbing
www.mobbing-schluss-damit.de

Überblick zur Vertrauenswürdigkeit von Apps
www.privacygrade.org/

Impressum

Wochenschau Verlag

Eschborner Landstr. 42-50
60489 Frankfurt am Main
Tel.: +49 (0)69/788 0 772-0
Fax: +49 (0)69/788 0 772-25

Bestellung

Wochenschau Verlag

www.wochenschau-online.de
info@wochenschau-verlag.de
www.wochenschau-verlag.de