POLIZEI
Nordrhein-Westfalen
Kreis Lippe

bürgerorientiert · professionell · rechtsstaatlich

Smartphone & Co.

Präventionstipps zum Thema Sicherheit für Smartphone, Tablet und anderen Computern

Dein Verhalten…

… mein Smartphone ist mein Smartphone: Das Smartphone ist ein Computer voll mit Apps, persönlichen Daten und Inhalten. Gebt das Smartphone nicht unbeaufsichtigt aus der Hand. Schad- bzw. Spionagesoftware könnte installiert werden.

… Privatsphäre-Einstellungen von Apps überprüfen: **Wer** darf mich **wo** sehen ist hier die Frage. Freunde, Freunde von Freuden oder Jeder. Das Letztere ist wohl die schlechteste Wahl und wird nicht empfohlen. Jeder kann dich anschreiben dir Nachrichten und Bilder senden. Sogenannte „Groomer“ könnten versuchen mit dir in Kontakt zu treten. Ihr Ziel ist es sexuelle Kontakte zu dir aufzubauen. Dabei geben sie sich oft als gleichaltrige aus, sind es aber nicht. Mit Chatfunktion ausgestattete Apps und Spiele sind potentielle Spielfelder für Groomer. Schreiben solltest du nur mit Personen, denen du schon einmal die Hand geschüttelt hast.

… unbekannte Telefonnummern: Solltest du erst einmal kritisch betrachten. Sie tauchen nicht in deinen Kontakten auf und sind erst einmal Fremde die dich kontaktieren. Gerade auch bei WhatsApp solltest Du darauf achten. Informiere deine Erziehungsberechtigten und lösch die Nachricht.

… sei sparsam mit deinen persönlichen Daten und Informationen über dein persönliches Umfeld:

Viele Betrüger sammeln Daten über ihre potentiellen Opfer. Sie gaukeln Freundschaft vor und fragen dich nach vielen Dingen aus. Wo arbeitet dein Vater, wann fahrt ihr in den Urlaub, wo wohnt deine Oma. In der Wirtschaft nennt man das nennt „Social Engineering“. Einfach gesagt Beeinflussung durch einfachste Kommunikation. Gebt nicht zu viele Informationen preis und seid skeptisch.

… den Klick auf Links vermeiden: Gerade in E-Mails und SMS sind Links sehr gefährlich. Beim Klick auf diese wird immer eine Aktion ausgelöst, die

du nicht kontrollieren kannst. Bei E-Mails solltest du den Absender schon kennen. Bei einer SMS oder einer Messanger-nachricht ist dies zu 90% ein Betrugsversuch. Der Mouseover-Effekt[1] funktioniert beim Smartphone nicht.

Deine Technik deine Sicherheit:

… ein Antivirenprogramm ist nicht nur für den PC oder Laptop wichtig. Es schützt auch dein Smartphone vor kriminellen Machenschaften.

…Updates schließen Sicherheitslücken von Apps und Betriebssystem. Stellt wenn möglich eure Computer und Smartphones auf „Updates automatisch installieren“ ein.

…Passwörter: mindestens 10 Stellen, Groß- und Kleinbuchstaben, Sonder-zeichen und Zahlen. Wann immer möglich Zwei- oder Mehrfaktorauthentifizierung benutzen.

… unverschlüsseltes WLAN nicht nutzen: Niemals ohne eine Ver-schlüsselung im Internet surfen. Un-verschlüsselte Kommunikation kann mitgelesen werden. (Zugangsdaten, Passwörter, etc.).

Ein verschlüsseltes WLAN erkennt ihr an folgenden Symbolen.

… VPN benutzen: Ein VPN[2] stellte eine verschlüsselte Verbindung (Tunnel) zwischen deinem Endgerät und einer Website her, auch wenn kein verschlüsseltes WLAN vorhanden ist. Außerdem wird dein Standort nicht freigegeben.

… die Verschlüsselung von Smart-phone, Laptop, USB-Stick und Fest-platten hilft dir bei Diebstahl. Deine Daten können nicht eingelesen werden

… aktuelle Sicherungen helfen dir deine entwendete Hardware, Daten und Dokumente wieder herzustellen.

… IMEI und Kopie der Rechnung von deinem Smartphones solltest du griffbereit haben, falls du bei der Polizei eine Anzeige wegen Diebstahls aufgeben möchtest.

Anzeige bei jeder Wache der Polizei oder unter: https://internetwache.polizei.nrw/

---

[1] Sobald der Nutzer zum Beispiel mit dem Maus-Zeiger oder einem digitalen Stift über ein mit dem Mouse Over Effekt versehenes Element fährt (Trigger Bereich), verändert sich dieses. Der Mouseover-Effekt bei einem Link zeigt die wirkliche Adresse an.

[2] VPN = „Virtual Privat Network“ stellt in diesem Fall eine sichere Verbindung zwischen einer Website und deinem Endgerät her.

Wichtige WhatsApp Regeln für dich und deine Klasse:

- Wer ist Admin? Doch wohl nicht alle? Am besten - abwechselnd immer nur einer.
- Keiner wird ausgegrenzt. Wer kein WhatsApp nutzt, bekommt trotzdem alle wichtigen Infos. Dafür sorgt ihr in eurer Klasse.
- Keine Fotos weiterleiten, die Dir nicht persönlich gehören. Oder vorher um Erlaubnis bei dem Besitzer fragen und bei allen, die auf dem Foto abgebildet sind.
- Veröffentliche keine peinlichen Fotos und Videos, auch nicht von anderen. Sei immer vorsichtig, z.B. bei deinen TikTok-Videos. Auch sie könnten peinlich sein oder verbotene Inhalte besitzen und dir und anderen schaden.
- Droh/Kettenbriefe sind nicht harmlos und lustig. Nimm sie nicht ernst. Du wirst durch sie gemein belogen und es gibt auch nichts umsonst. Diese Nachrichten sollen Dich nerven, vielleicht dein Smartphone zerstören oder dich in Angst und Schrecken versetzen. Klicke keine Links in diesen Kettenbriefen an, denn sie können brutal sein und/oder Schadprogramme enthalten. Frage eine Person deines Vertrauens, wenn du Sorgen wegen eines Kettenbriefes oder einer Nachricht hast. Ab sofort löschst du solche Kettenbriefe und schickst sie nie wieder weiter.
- Beachte: die Weiterleitung von Drohkettenbriefen, brutalen Videos/Fotos/Stickern, sexistischen Videos/Fotos/Stickern/Memes oder Hakenkreuzen kann eine Straftat sein.
- Achte auf deinen Umgangston. Sei freundlich mit allen. Rede und benehme dich so, wie du auch behandelt werden willst. Beleidigungen können eine Straftat sein.
- Nur mit der persönlichen Erlaubnis darfst du Freunde einer neuen Gruppe zufügen.
- Schreibe nicht mit fremden Personen oder mit Menschen, die du nicht persönlich kennst und bei denen du ein ungutes Gefühl hast.
- Manchmal werden dich unbekannte Leute kontaktieren. Blockiere sie am besten gleich, denn meistens nerven sie und ein Telefongespräch mit ihnen könnte sehr unangenehm und auch sehr teuer werden.
- Mach den Chat nicht zu deinem Leben. Nicht alle müssen alles über dich wissen. Sei auch kein Angeber, das bringt nur schlechte Stimmung unter Freunden.
- Schalte deine Gruppen stumm. Sonst nervt WhatsApp schnell.
- Angst etwas zu verpassen? Lass dich nicht stressen! Schalte dein Smartphone zum Beispiel bei Hausaufgaben, Besuch von Freunden, bei Gesprächen mit der Familie, beim Essen oder abends im Bett aus.
- Schlaf gut. Schließ daher jeden Abend deine Gruppenchats bis zum Morgen. Keine Panik! Wirklich wichtige Nachrichten werden immer zu dir finden ☺.

Wenn es in WhatsApp nicht so gut läuft:

Wenn WhatsApp dir Ärger macht oder jemand geärgert oder gemobbt wird, dann kannst du:

- dich beschweren und Regeln fordern oder aus der betroffenen Gruppe austreten
- jeden einzelnen negativen Kontakt aus dem Adressbuch löschen
- die betreffende Person blockieren, die einen mobbt. Für den Täter ist dann nicht zu erkennen, dass er blockiert wird. Seine Nachrichten werden aber nicht mehr ankommen.

S.Schattenfroh, Medienpädagogin 2024

Sabine Schattenfroh
Medienpädagogin, Erziehungsberaterin
Spiegelberg 105
32657 Lemgo
Fon 05261/14629
Schattenfroh@unitybox.de

Internetseiten für Eltern - Thema: Internetsicherheit für die ganze Familie

www.bsi.bund.de
Tipps zum **digitalen Verbraucherschutz und alltägliche Internetsicherheit** für Internetnutzer.
Unter dem Bereich „Themen“ finden Sie den Bereich „**Verbraucherschutz**“.

www.klicksafe.de
Klicksafe unterstützt Eltern dabei, ihre Kinder bei der Nutzung von digitalen Medien zu begleiten. Das Ziel ist ein sicherer, fairer und selbstbestimmter Umgang mit Internet, digitalen Spielen, Smartphones und Apps.
Mit **Smartphone-Checkliste für Eltern**.

www.schau-hin.info
Medienratgeber für Eltern. Rund um Hörspiele, TV, PC, Internet, Handy, Tablet, Smartphone, Smartwatch, Bildschirmspiele und Co.

www.mediennutzungsvertrag.de
Ein **Mediennutzungsvertrag** für die ganze Familie.

www.jugendschutzprogramm.de
JusProg ist eine **kostenlose Filtersoftware**, die junge Internetnutzer vor nicht altersgerechten Inhalten im Internet schützt.

www.mobilsicher.de
Das **Infoportal für mehr Sicherheit am Smartphone u. Tablet**. Mit vielen Tipps zur sicheren Einrichtung eines Smartphones.

www.handysektor.de
Eine **Infoseite für Jugendliche**: mit Tipps, Informationen und auch kreativen Ideen zu Smartphones, Tablets, Apps.

www.saferinternet.at
Medienratgeber für Eltern und Jugendliche. **Mit Anleitungen und Leitfäden für WhatsApp, YouTube, Instagram, Snapchat, TikTok, Discord, Facebook, etc**.

www.nummergegenkummer.de
Kostenlose Lebens-Beratungsseite für Kinder und Eltern.

www.polizeifürdich.de
Internetplattform der Polizei - für Kinder und Jugendliche.

https://play.google.com/store/apps/details?id=de.apisservices.cybermob&gl=DE
https://apps.apple.com/de/app/cyber-mobbing-erste-hilfe-app/id1090734113
Kostenlose “Erste Hilfe App” - zum Schutz gegen und zur Hilfe bei Cybermobbing.

www.mimikama.at
Verein zur Aufklärung gegen Internetmissbrauch, u.a. mit Informationen zu aktuellen Fake News.

www.spieleratgeber-nrw.de
Bildschirmspiele werden vorgestellt und bewertet, mit einer **Suchmaschine für aktuelle Spiele**.

www.digitalcourage.de
Bielefelder Datenschutzverein - mit wertvollen Tipps zur Internetsicherheit und zum Datenschutz: schaffe deine persönliche **„digitale Selbstverteidigung“** und richte dein Smartphone neu ein.

www.jugendschutz.net
Jugendschutz.net sichtet Angebote im Netz auf Verstöße gegen den Jugendschutz. **Jugendschutz.net nimmt Beschwerden entgegen** (auch anonym), recherchiert und klärt auf, welche Risiken für Kinder und Jugendliche im Internet bestehen. Hier können u.a. Cybermobbing oder Fake News gemeldet werden.

Technische Einstellungen Smartphone & Tablet

Hilfestellung für Eltern

	Android	iOS
Jugendschutz-einstellungen am Gerät und im Store nutzen	• Play Store-App öffnen • Menü öffnen • Einstellungen • Jugendschutzeinstellungen • Schiebeschalter „ein“ und PIN erstellen • PIN bestätigen und Altersfreigabe für Inhalte wählen	• Einstellungen • Bildschirmzeit • Beschränkungen aktivieren • 4-stelligen Code wählen • Beschränkungen • Altersfreigaben wie gewünscht festlegen
Internet (Daten, WLAN) ausschalten	• Einstellungen • Offline Modus • Schiebeschalter ein	• Einstellungen • Schiebeschalter bei „Flugmodus“ an
In-App-Käufe verhindern; Zugang zu App-Stores mit Passwort sichern	• Google Play Store-App öffnen • Menü öffnen • Einstellungen • Authentifizierung für Käufe erforderlich • Häkchen bei „Für alle Käufe bei Google Play auf diesem Gerät“	• Einstellungen • Bildschirmzeit • Beschränkungen • Käufe in iTunes & App Store • In-App-Käufe „Nicht erlauben“ und • „Passwort erforderlich“ auf „Immer erforderlich“
Push-Mitteilungen bei Spielen deak-tivieren	• Einstellungen • Apps • App wählen • App-Benachrichtigung • Schiebeschalter aus	• Einstellungen • Mitteilungen • App wählen • Mitteilungen erlauben • Schiebeschalter aus
Ortungsdienste deaktivieren	• Einstellungen • Standort • Schiebeschalter aus	• Einstellungen • Allgemein • Einschränkungen aktivieren • 4-stelligen Code wählen • Ortungsdienste • Schiebeschalter aus

klicksafe

Quelle: Broschüre „Gutes Aufwachsen mit Medien“
Stand: Juni 2019, iOS 12.3, Android 8.1

Kofinanziert durch die Europäische Union

Checkliste

klicksafe

Ist mein Kind fit für ein eigenes Smartphone?

Sollte es schon alleine Apps installieren? Weiß es, welche Daten und Fotos nicht geteilt werden sollten? Ist WhatsApp oder TikTok für mein Kind okay? Die Beantwortung dieser und ähnlicher Fragen fällt vielen Eltern schwer. Mit der folgenden Checkliste wollen wir Ihnen bei der Entscheidung „Smartphone – ja oder nein?“ helfen. Kreuzen Sie an, was Ihr Kind bei der Handynutzung schon kann. Je mehr Punkte mit einem Haken versehen wurden, desto eher ist Ihr Kind schon „fit“ für ein eigenes Smartphone. Wir empfehlen, dass Sie mit Ihrem Kind die noch ausstehenden Punkte besprechen.

Das kann Ihr Kind:

- [x] **Sicherheitseinstellungen aufrufen** und dort Einstellungen ändern (PIN oder Passwort erstellen und ändern, Bildschirmsperre einrichten)
- [ ] **Kosten** der (monatlichen) **Smartphone-Nutzung** (Prepaid oder Tarif) überschauen
- [ ] Erkennen, wo **Kosten** anfallen (z. B. **In-App-Käufe**) und entsprechende Einstellungen am Gerät vornehmen
- [ ] **GPS-Signal, W-LAN** und **Bluetooth** selbständig aktivieren und deaktivieren
- [ ] **Datenroaming** für Urlaube außerhalb der EU ein- oder ausschalten
- [ ] Apps auswählen und **vor einer Installation kritisch prüfen**, ob die Anwendungen sicher und dem eigenen Alter angemessen sind
- [ ] **Datenschutzrisiken** und die Angemessenheit von **App-Berechtigungen** einschätzen; wissen, wo man sich hierzu informieren kann (z. B. in den AGB, in Foren etc.) und welche Einstellungsmöglichkeiten es gibt
- [ ] Vorsichtig mit eigenen **Informationen/Fotos im Internet** umgehen und wissen, was man lieber **nicht teilen** sollte
- [ ] **Rechte anderer** auch im Digitalen beachten (z. B. niemanden über Messenger beleidigen, Daten, Bilder und andere Informationen anderer nicht ungefragt weitergeben, Hass im Netz melden, usw.)
- [ ] Wissen, bei welchen **Problemen** man Eltern oder anderen Vertrauenspersonen **Bescheid sagen** sollte (ängstigende Nachrichten, Anfragen nach Adresse oder freizügigen Bildern, Abzock-Versuche etc.)
- [ ] **Vereinbarte Regeln** für die Handynutzung verstehen und akzeptieren (z. B. nicht am Esstisch, nach 21 Uhr Handy aus etc.)
- [ ] **Handynutzung** und **Stellenwert des Handys im Alltag** kritisch hinterfragen (vor allem hinsichtlich der Nutzungszeiten)
- [ ] **Werbung** erkennen und den Umgang mit verschiedenen Werbeformen verstehen

Weitere Ideen und Tipps rund um Handys und Apps finden Sie unter:
www.klicksafe.de/smartphones ▪ **www.klicksafe.de/apps** ▪ **www.handysektor.de**

klicksafe wird kofinanziert von der Europäischen Union.