DAS INTERNET.
ES IST SCHNELL, COOL UND GLOBAL.

Aber es ist auch komplex. Manchmal sind die Risiken nur schwer zu erkennen – denn manchmal können andere Menschen unsere privaten Dinge sehen und verwenden. In unserem Paralleluniversum kämpfen die Superhelden der **DIGITALEN DEFENDER** gegen die Schurkengruppe **DATENJÄGER**. So ist zum Glück leicht zu sehen, wer zu den Guten und wer zu den Bösen gehört.

www.edri.org

EDRi

dein ratgeber:

DIGITALE DEFENDER

gegen die

DATEN-JÄGER

BEHALTE DIE KONTROLLE ÜBER DEINEN KRAM IM NETZ!

privatsphäre für kids!

CMS CHAOS MACHT SCHULE

EPICENTER .WORKS for digital rights

digitalcourage

DIGITALE GESELLSCHAFT

Das Internet. Es ist schnell, cool und global.

Aber es ist auch komplex. Manchmal sind die Risiken schwer zu erkennen – und man sieht nicht leicht, wie und wo andere Menschen unsere privaten Sachen sehen und verwenden können.

In unserem Paralleluniversum kämpfen die Superhelden der DIGITALEN DEFENDER gegen die Schurkenbande DATENJÄGER. So ist zum Glück leicht zu sehen, wer die Guten und wer die Bösen sind. Die DIGITALEN DEFENDER zeigen euch Tipps und Tricks, wie ihr euch online schützen könnt. So lernt ihr Selbstverteidigung gegen die Angreifer, die DATENJÄGER.

» Mit dieser Broschüre könnt ihr Teil des Superhelden-Teams der DIGITALEN DEFENDER werden!

Dein Freund,
EDRi-former

» ACH SO, UND HALTE DIE AUGEN OFFEN FÜR DAS EDRi-former-SPIEL

In einigen Kapiteln findest du verschiedene Missionen. Bei jeder Mission gibt es eine richtige Antwort, damit bekommt ihr einen Buchstaben. Zusammen ergeben diese Buchstaben das Lösungswort. Tipp: Das Lösungswort ist ein englisches Wort mit sechs Buchstaben. Die Trophäe: eine MÄCHTIGE DIGITALE RÜSTUNG. Mit dem Lösungswort kannst du dann eine geheime Seite im Internet finden. Und so funktioniert's:

1. Finde den fehlenden Teil des folgenden Links: https://edri.org/xxxxxx .
2. Ersetze das xxxxxx mit dem englischen Lösungswort (sechs Buchstaben), das sich aus den Spielmissionen ergibt und gib den vollständigen Link in deinem Browser ein.

KAPITEL

1 WAS IST DAS INTERNET?
2 WAS IST PRIVATSPHÄRE?
3 UNTERWEGS IN SOZIALEN NETZWERKEN
4 TIPPS UND TRICKS
5 SICHERES MESSAGING
6 WIE SCHÜTZE ICH MEIN HANDY?
7 IM INTERNET SURFEN
8 PASSWÖRTER
9 FOTOS UND VIDEOS TEILEN
10 COOLE APPS UND TOOLS
11 PRAKTISCHE ANLEITUNG FÜR SIGNAL

Redaktion:
Kirsten Fiedler, EDRi
Theresia Reinhold, EDRi

Comics:
Gregor Sedlag

Grafik und Design:
Gregor Sedlag
Heini Järvinen („EDRi-former")

Mit Beiträgen von:
ApTI Romania
Bits of Freedom
CCC / Chaos macht Schule
Cryptoparty.in
Digitale Gesellschaft e. V.
EDRi (Brussels office)
Open Rights Group
Mediamocracy

Besonderen Dank an:
Gloria González Fuster, Vrije Universiteit Brussel (VUB)
Hans Martens, Better Internet for Kids, EUN Partnership AISBL

Deutsche Übersetzung:
Kirsten Fiedler, EDRi
Sebastian Lisken, Digitalcourage
Hanno Wagner, FITUG

European Digital Rights

20 Rue Belliard
B-1000 Brussels

edri.org
@edri
brussels@edri.org
+32 2 274 25 70

EDRi

KAPITEL 1

Was ist das Internet?

Das Internet ist ein globales Netzwerk von elektronischen Geräten. Das Internet hat die besondere Eigenschaft, dass viele verschiedene Technologien gleichzeitig in dem Netzwerk benutzt werden können.

» Wenn du dein Laptop, Tablet oder Handy benutzt, sind diese Geräte Teil des Netzwerkes.

Das Internet gibt es weltweit, es ist schnell und es bietet uns eine Welt voller Möglichkeiten.

Das Internet ist eine tolle und gewaltige Erfindung. Vor dem Internet war es nicht so einfach, viele Menschen miteinander zu verbinden.

Es war viel schwieriger, Musik zu hören und einen Film zu schauen. Das Internet ist auch ein großartiger Platz, um neue Dinge zu lernen, denn ganz viel Wissen wird über das Netz geteilt.

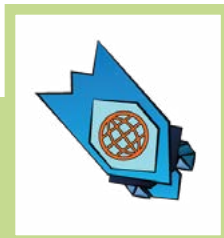
Internettechnik ist ein bisschen so wie ein großer schneebedeckter Hügel – wir können darauf Ski oder Snowboard fahren oder einen Schneemann bauen. Alles was wir brauchen, ist Schnee!

In der Welt des Internets ist dieser Hügel unsere Internetverbindung und der Schnee ist die Sprache, die das Netzwerk spricht – das „Internetprotokoll"!

Soziale Netzwerke und andere Onlinedienste sprechen ebenfalls dieses Protokoll. Sie erscheinen oft so, als wären sie kostenlos – aber in Wirklichkeit zahlen wir mit unseren persönlichen Daten, die wir dort herausgeben. Information über das, was wir online schreiben, lesen oder anschauen, wird von Unternehmen (aus)genutzt..

» Wie können wir also die Kontrolle über die Daten behalten, die wir online posten?

Die Antwort auf diese Frage wirst du auf den nächsten Seiten finden.



» MISSION 1: DAS INTERNET IST...

[A] ...ein Netzwerk von elektronischen Geräten.
[B] ...ein gutes Fischfangnetz für internationale Gewässer.
[C] ...ein soziales Netzwerk.

KAPITEL 2

Was ist Privatsphäre?

Wenn wir Privatsphäre haben, haben wir Kontrolle. Aber was bedeutet das?

» Privatsphäre ist unser Recht, zu entscheiden, was wir mit wem teilen wollen.

Das bedeutet beispielsweise, dass du das Recht hast, Google, Facebook und alle anderen zu fragen, welche Informationen sie über dich gesammelt haben. Du kannst sie auch bitten, diese Daten zu löschen.

Wenn wir unsere Privatsphäre schützen, können wir uns sicherer fühlen – denn manche Informationen könnten uns schaden, wenn die falsche Person sie in die Hände bekommt. Das können Informationen sein, die wir mit einigen Leuten (wie unseren Eltern oder Lehrern) teilen wollen, aber mit niemandem sonst. Aber wir helfen auch anderen, wenn wir unsere Privatsphäre schützen: Zum Beispiel wenn jemand uns etwas erzählen möchte, das er oder sie mit niemandem sonst teilen möchte.

» Wir alle haben etwas, das wir nicht der ganzen Welt erzählen möchten.

Wenn wir uns um unsere eigene Privatsphäre kümmern, dann kümmern wir uns auch um unsere Freunde. Das macht uns frei, sicher und vertrauenswürdig.

Unsere Eltern, Freunde oder jeder, der nach uns unseren Computer benutzt, kann manchmal herausfinden, wonach wir gesucht haben. Das kann passieren, wenn wir vergessen, uns abzumelden oder sie sich den Suchverlauf im Browser anschauen.

» WUSSTEST DU DAS?

Vor nicht einmal 20 Jahren hatten die meisten Haushalte nur eine Telefonleitung, die nur eine Person zur gleichen Zeit nutzen konnte. Fast niemand hatte ein Mobiltelefon und nur wenige Menschen schrieben sich E-Mails.

KAPITEL 3

Unterwegs in sozialen Netzwerken

Soziale Netzwerke können so viel Spaß machen! Dort kannst du mit deinen Freunden und der Familie chatten, Fotos teilen, private Nachrichten senden und Informationen veröffentlichen.

In manchen Ländern ist es Kindern unter 13 Jahren nicht erlaubt, soziale Netzwerke zu nutzen. Wenn du dich anmelden möchtest, frag am besten vorher deine Familie und Lehrer, ob das in Ordnung geht.

» YouTube, Facebook, Instagram, Snapchat, Diaspora und viele andere – all dies sind soziale Netzwerke.

Hast du ein Lieblingsnetzwerk? Warum magst du diese Netzwerke?

Manche sozialen Netzwerke speichern Nachrichten, selbst wenn wir sie (noch) nicht abgeschickt haben. Stell dir vor, du schreibst eine Nachricht an deinen Freund bei Facebook, aber du sendest sie nicht ab. Dein Freund wird niemals von dieser Nachricht erfahren, aber Facebook hat sie gespeichert!

Denk daran: Alles, was du in sozialen Netzwerken tust, wird von den Computern der Firmen, die das soziale Netzwerk betreiben, gespeichert. Das bedeutet nicht unbedingt, dass sie etwas schlechtes damit anfangen – aber du solltest wissen, dass sie das tun.

» WUSSTEST DU DAS?

Was wir eine Suchmaschine fragen oder in eine Chat-Nachricht an einen Freund schreiben, verschwindet nie komplett. Unternehmen (wie Youtube, Facebook, Snapchat und so weiter) können Nachrichten, die wir schreiben, Webseiten, die wir besuchen und die Dinge, nach denen wir online suchen, speichern und später wiederverwenden.

DIGITALE DEFENDER gegen DATENJÄGER (I)

A. NONYM

TEAM: DIGITALE DEFENDER

KRÄFTE:
Staatliche Tests haben ihr Immunsystem verbessert. Sie hat die Fähigkeit, sich in sozialen Netzwerken anonym zu bewegen. Niemand weiß, wer sie wirklich ist.

WAFFEN:
Sie ist eine erfahrene Nahkämpferin.

IRIS INFEKT

TEAM: DATEN-JÄGER

KRÄFTE:
Sie sieht, was du online machst und stiehlt dann deine persönlichen Informationen. Sie versucht, deine Identität zu klauen, um deinen Namen und deine Konten in sozialen Netzwerken für kriminelle Zwecke zu nutzen.

WAFFEN:
Der Alpha-Virus – mit dem sie Computer und Telefone infiltriert.

» MISSION 2: PRIVATSPHÄRE IST WICHTIG, WEIL...

[T] ...wir dann Musikvideos anschauen können.
[R] ...sie uns hilft, frei zu sein und online die Kontrolle zu behalten.
[G] ...wir leichter unsere Fotos mit der gesamten Welt teilen können.

KAPITEL 4

Tipps und Tricks

1. Nicht jeder muss alles über uns wissen

Wie in der Offline-Welt sollten wir auch online sorgfältig darauf achten, was wir teilen wollen und was nicht. Instinktiv erzählen wir manche Dinge bestimmten Leuten und anderen nicht. Das Internet macht uns diese Wahl manchmal schwer.

Einerseits ist das so, weil nicht immer klar zu erkennen ist, was im Internet privat ist und was nicht. Andererseits gelten im Internet andere Regeln als in der Offline-Welt.

Ein Beispiel: Unsere Freunde verzeihen uns, wenn wir einen blöden Spruch machen. Sie verstehen unser Verhalten, weil sie uns kennen. Wenn dagegen andere Leute unseren wütenden Kommentar online lesen, können sie das vielleicht falsch verstehen und glauben, dass wir absichtlich gemein sein wollten.

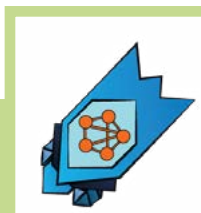
2. Sicherheit und Privatsphäre im Internet sind nicht schwer

Wir müssen keine Nerds sein, um uns sicher durchs Internet zu bewegen. Wir können ein Tablet, ein Smartphone oder einen Laptop benutzen, zu dem unsere Klassenkameraden keinen Zugang haben. Wir können uns ein Passwort ausdenken, das keiner errät. Wir können Videos online anschauen, ohne dabei im Netz verfolgt zu werden. Und das kann alles sehr einfach sein.

3. Risiken erkennen

So wie Banken sich gegen Diebe schützen, müssen auch wir uns schützen: gegen Unternehmen, die unsere Daten im Netz sammeln, gegen Mitschüler, die vielleicht unsere Nachrichten lesen wollen oder gegen neugierige Eltern, die … neugierig sind.

Wir sollten uns fragen, welche Gefahren möglich sind und was wir dagegen machen können. Sobald wir darüber ein bisschen nachdenken, finden wir sehr schnell heraus, wie wir unsere Privatsphäre besser schützen können.



» MISSION 3: SOZIALE NETZWERKE SIND TOLL, WEIL…

[Q] …ich sicher sein kann, dass sie niemals meine Daten benutzen oder verkaufen.
[M] …ich mit meinen Freunden und Familie in Kontakt bleiben kann.
[N] … ich sicher sein kann, dass nur meine Freunde meine geposteten Fotos sehen.

KAPITEL 5

Sicheres Messaging

Wir alle benutzen unsere Telefone, um Nachrichten an Freunde und die Familie zu senden.

Allerdings lesen einige Messaging-Apps den Inhalt deiner Nachrichten und speichern, mit wem wir uns unterhalten. Manche Apps machen das, um mit diesen Informationen Profit zu machen.

» Was du sagst und was du online machst, ist sehr wertvolles Wissen für Firmen.

Unternehmen, die Messaging-Apps betreiben, durchleuchten oft das, was wir schreiben oder sagen. Sie speichern, mit wem wir uns unterhalten, um uns passende Werbung einzublenden. Manchmal verkaufen sie die gesammelten Informationen an andere Firmen.

Am Ende dieser Broschüre findest du eine Liste mit coolen Messaging-Apps. Diese Apps sorgen auch dafür, dass wir keine Nachrichten von fremden Leuten erhalten. Und zu guter Letzt haben wir sogar eine Anleitung für dich in dieser Broschüre, wie man Signal installiert – Signal ist eine coole App, um Nachrichten sicherer zu machen.

Wie schütze ich mein Handy?

Unsere Smartphones sind für uns sehr wichtig geworden.

Wir benutzen sie, um mit Familie und Freunden zu kommunizieren, um auf sozialen Netzwerken aktiv zu sein oder einfach nur um im Internet zu surfen.

Aber unsere Smartphones sind auch für viele andere Dinge nützlich. Wir können sie als Taschenlampe benutzen, Spiele spielen oder die Abfahrtszeit des nächsten Busses nachschauen.

Wenn du eine neue App installierst, liest du dir durch, welche Berechtigungen du der App gibst? Und wie die App auf Daten auf deinem Smartphone zugreifen kann? Braucht eine Taschenlampen-App wirklich Zugang zu deinem Adressbuch?

Es ist sehr verlockend, einfach schnell auf „Akzeptieren" zu klicken. Aber es ist besser, kurz die Berechtigungen anzuschauen und nachzudenken. Man sollte einer App nicht vertrauen, wenn sie Informationen will, die sie offensichtlich nicht braucht.

Mit ein paar Klicks können wir die Berechtigungen unseres Smartphones oder einzelner Apps überprüfen und sogar einschränken. Auf den meisten Geräten können wir das über die Option „Einstellungen" tun. Schau dir die verschiedenen Einstellungen auf deinem Smartphone mal genauer an. So lernst du, wie dein Gerät funktioniert.

» Viele Apps haben Zugang zu den persönlichen Infos, die auf deinem Telefon sind.

Wir können den Zugang zu unserem Standort einschränken. Wir können einstellen, dass vor dem Entsperren des Bildschirms ein Passwort eingegeben werden muss. Mit ein paar Klicks können wir auch das Smartphone komplett verschlüsseln (also schützen).

Unser Smartphone sicherer und Privatsphäre-freundlicher zu machen, dauert nicht lange. Am Ende dieser Broschüre findest du eine Liste mit tollen Apps, die dir dabei helfen.

» WUSSTEST DU DAS?

Wenn es einen guten Grund gibt, einer App die Erlaubnis für etwas zu erteilen, dann gibt es wenig Grund zur Sorge. Zum Beispiel, wenn eine Foto-App Zugang zur Kamera möchte. Aber wenn du glaubst, dass eine App zu viele Berechtigungen verlangt, kannst du im App-Store nachschauen, ob es eine ähnliche App gibt, die weniger verlangt.

DIGITALE DEFENDER gegen DATENJÄGER (II)

PROFESSOR FREI

TEAM: DIGITALE DEFENDER

KRÄFTE:

Er kämpft für dein Recht zu entscheiden, mit wem du was teilen willst. Er hat die Fähigkeit, ein privates und sicheres Umfeld zu schaffen, in dem du sagen kannst, was du denkst.

WAFFEN:

Sein Verstand.

DER MANN IN DER MITTE

TEAM: DATEN-JÄGER

KRÄFTE:

Er hat die mysteriöse Fähigkeit, abzufangen, was du online machst. Er kann dir vorgaukeln, ein vertrauenswürdiger Partner im Internet zu sein. Das nutzt er dann aus, um sich in deine Kommunikation einzuhacken, deine E-Mails zu lesen und deine Fotos und Videos anzuschauen.

WAFFEN:

Sein Anzug und seine Antennen.

DATEN-JÄGER

DIGITALE DEFENDER

EDRi

Im Internet surfen

Häufig nutzen wir das Internet über einen Browser.

» Man vergisst leicht, dass der Browser eine Software ist.

Manchmal ist er die erste Sache die du öffnest, wenn du dein Telefon, Tablet oder den Computer einschaltest und die letzte Sache, die du schließt. Aber es passiert viel innerhalb des Browsers, das unsichtbar ist und das schlecht (oder gut) für den Schutz deiner Daten sein kann.

Wenn wir online gehen, um etwas zu kaufen, Videos zu schauen oder um zu sehen, was unsere Freunde gerade gepostet haben, dann hinterlassen wir digitale Fußabdrücke. Manche Websites und sozialen Netzwerke nutzen diese Fußabdrücke, um uns zu verfolgen.

» Websites sammeln viele Informationen über uns!

Wer unsere Freunde sind, was wir mögen, wonach wir suchen und was wir uns anhören: das alles kann nachverfolgt werden. Diese Websites können das tun, weil sie „Cookies" in unseren Browsern verwenden. Diese Cookies sind kleine Computerprogramme.

Sie sind unsichtbar für uns, aber wenn genug Daten gesammelt und mit anderen Informationen über uns kombiniert werden, werden persönliche Details (von denen wir vielleicht dachten, dass sie geheim sind) für viele Leute und Unternehmen bekannt.

Die meisten Geräte verfügen von Anfang an über einen Browser. In Windows können wir den Internet Explorer verwenden, Apple-Geräte verfügen über Safari und der Standardbrowser der Android-Geräte ist Google Chrome. Aber dies sind nicht zwingend die Browser, die am besten für dich geeignet sind.

» WUSSTEST DU DAS?

Schau in den „Einstellungen für Privatsphäre" deines Browsers nach und übernimm die Kontrolle – genau wie unser Superheld die Perfekte Welle! Viele Leute denken, dass Firefox der beste und sicherste Browser ist. Warum? Weil du ihn anpassen, ihn kontrollieren und sehen kannst, wie er funktioniert. Du kannst mit Firefox auch im „privaten Modus" surfen. Vielleicht ist er nicht auf deinem Computer installiert, aber du kannst ihn sehr leicht runterladen.

» MISSION 4: MANCHE APPS ...

[F] ...sind so sicher, dass ich niemals über meinen Datenschutz nachdenken muss.
[L] ...sind besser als Schokolade.
[O] ...können auf meine Kontakte, Bilder und Nachrichten zugreifen.

DIGITALE DEFENDER gegen DATENJÄGER (III)

PERFEKTE WELLE

TEAM: DIGITALE DEFENDER

KRÄFTE:
Er kann auf seinem Brett im Raum, Hyperraum und Cyberspace navigieren. Perfekte Welle benötigt kein Essen oder Getränke. Er überlebt, indem er Daten in Energie umwandelt. Er ist so gut wie unzerstörbar.

WAFFEN:
Sein Surfbrett.

DER KEKS

TEAM: DATEN-JÄGER

KRÄFTE:
Das Keksmonster ist immer auf der Suche nach Streit. Es hasst alle Defenders, aber betrachtet die Perfekte Welle als seinen schlimmsten Feind. Es hat einen monströsen Appetit auf deine Geheimnisse.

WAFFEN:
Sein wirbelnder Roboterarm.

Passwörter

Passwörter: Sie sind sehr wichtig im digitalen Zeitalter.

Unglaublich wichtig. Sie bilden die Grundlage für unsere Sicherheit und Privatsphäre. Die Passwörter der meisten Menschen sind viel zu einfach – das am häufigsten verwendete Passwort ist „Passwort“ oder „12345“.

Dabei ist es gar nicht schwer, sich ein sicheres Passwort auszudenken. So geht's:

1. Benutze für jedes Konto ein anderes Passwort

Das ist wirklich eine der wichtigsten Regeln! Versuche zumindest verschiedene Versionen eines Passwortes zu machen.

Warum? Wenn Kriminelle (wie der Datenschmuggler) dein Passwort auf einer Website herausfinden, dann versuchen sie dasselbe Passwort auch auf anderen Plattformen zu benutzen. Sie wissen, dass viele Menschen dasselbe Passwort auf mehreren Seiten verwenden!

2. Benutze niemals ein Wort aus dem Wörterbuch

... auch dann nicht, wenn es lang oder kompliziert aussieht.

Warum? Weil es Computerprogramme gibt, die jedes einzelne Wort eines Wörterbuchs automatisch ausprobieren, um dein Passwort zu „erraten“. Jeder Superheld der Digitalen Defender hat ein starkes und kreatives Passwort. Du kannst dich ihnen anschließen – dein Passwort ist deine Waffe gegen die Datenjäger.

3. Dein Passwort sollte mindestens 12 Stellen lang sein

Das ist das Minimum. Je länger ein Passwort ist, umso schwieriger ist es zu hacken.

Warum? Weil je länger ein Passwort ist, umso schwieriger ist es zu erraten. Manche Experten sagen, dass es in Ordnung ist, ein Passwort aufzuschreiben. Aber verstecke den Zettel gut!

DIGITALE DEFENDER gegen DATENJÄGER (IV)

SARAH SCHLÜSSEL

TEAM: DIGITALE DEFENDER

KRÄFTE:

Sie kämpft für Privatsphäre und Sicherheit. Sie verteilt mächtige, private Schlüssel an diejenigen, die in Gefahr sind und hilft ihnen, ihre persönlichen Informationen online zu sichern.

WAFFEN:

Ihr Helm – sie benutzt ihn, um Laserstrahlen aus ihren Augen abzufeuern. Sie kann sich direkt durch Finn Fischers gefährliches Netz schneiden.

FINN FISCHER

TEAM: DATEN-JÄGER

KRÄFTE:

Er besitzt übermenschliche Kraft, Geschwindigkeit und Reflexe. Er benutzt seine Kräfte, um sich in dein Telefon hineinzuschleichen und deine Geheimnisse herauszufischen.

WAFFEN:

Seine elektrostatischen Netze betäuben alle Gegner.

» MISSION 5: WENN ICH IM INTERNET SURFE...

[X] ...kann ich machen, was ich will und bin sicher – es ist nicht die Wirklichkeit!
[U] ...kann ich mich schützen, indem ich Cookies verbiete und meinen Browserverlauf nicht speichere.
[Y] ...habe ich nichts zu verbergen, das ist doch nur Paranoia.

Fotos und Videos teilen

Wir erzählen unseren Freunden über unsere Erlebnisse, indem wir Bilder und Videos online mit ihnen teilen.

» Teilen ist cool – aber Fotos und Videos können leicht kopiert werden.

Denk daran, dass es wichtig ist sicher zu gehen, dass wir nichts mit Leuten teilen, mit denen wir nichts teilen wollen. Fremde Leute könnten sonst unsere privaten Bilder sehen und benutzen.

Wo ist das Problem? Hier: Wenn wir jemandem ein Foto oder ein Video schicken, senden wir eine Kopie davon von unserem Gerät auf das Gerät eines Freundes. Stell dir vor, unser Freund teilt das Bild nochmals mit anderen. Jede Kopie kann wieder kopiert werden!

Wenn wir ein Foto oder ein Video online teilen, wird es immer mehrere Kopien davon auf verschiedenen Geräten geben. Auch wenn wir das Originalbild auf unserem Gerät löschen, werden die Kopien immer noch da sein.

Wenn wir etwas teilen, kann unser Kram in die Hände von Leuten geraten, mit denen wir nichts teilen wollten.

Manche Leute könnten sogar versuchen unsere Identität zu stehlen, indem sie unsere Fotos benutzen – genau wie Iris Infekt.

Snapchat ist eine App, um Bilder zu teilen, die schnell verschwinden. Leider ist es trotzdem möglich, mit ein paar Tricks ein Foto zu speichern und es an andere zu schicken. So wurden bereits Tausende von Snaps irgendwo anders im Internet veröffentlicht.

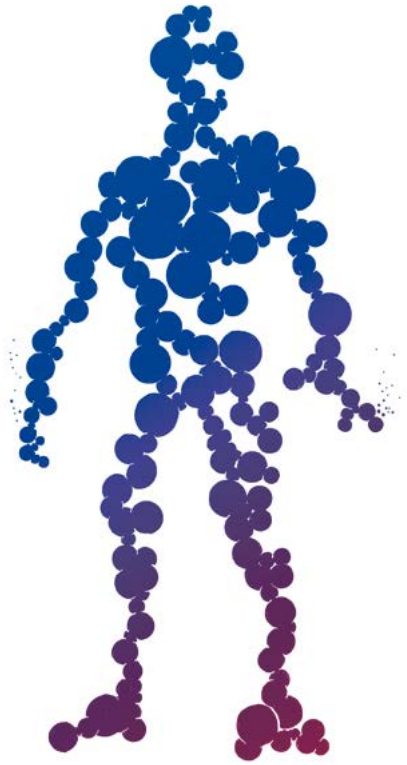
Das bedeutet, dass wir alle mit der Möglichkeit leben müssen, dass soziale Netzwerke auf gute und auf schlechte Weise verwendet werden können. Also müssen wir nachdenken, bevor wir Fotos und Videos im Internet posten und verschicken! Wir sollten uns fragen, ob wir dieses Foto an die öffentliche Pinnwand in unserer Schule hängen würden. Wenn nicht, dann ist es vielleicht auch keine gute Idee, es online zu teilen.

Wenn unser Foto andere Leute zeigt, müssen wir diese um Erlaubnis fragen, bevor wir es teilen. Sie haben das Recht, das zu entscheiden.

Bevor wir Bilder teilen, die wir nicht selber gemacht haben, müssen wir den Urheber um Erlaubnis fragen.

DIGITALE DEFENDER gegen DATENJÄGER (V)

JOHNNY ZUFALL



TEAM: DIGITALE DEFENDER

KRÄFTE:

Er wurde auf dem Planeten Entropia geboren, in einer weit entfernten Galaxis. Wie alle Mitglieder seiner Spezies hat er die Fähigkeit, seine Form nach Belieben zu ändern. Er kann deine Geheimnisse durch sich zufällig ändernde Passwörter schützen.

WAFFEN:

Seine Hauptwaffenarsenal besteht aus energiegeladenen Teilen seines Körpers, die er jederzeit werfen und zurückgewinnen kann.

DATA SMUGGLER

TEAM: DATEN-JÄGER

KRÄFTE:

Er ist sehr reich und hat Fähigkeiten, die weit über dem Menschlichen liegen. Er ist unglaublich flexibel und hat übermenschliche Stärke. Er sammelt wertvolle persönliche Daten (wie deine Fotos und Nachrichten) und verkauft sie auf dem Schwarzmarkt.

WAFFEN:

In seinem Koffer trägt er verschiedene Arten von Waffen mit sich.

Coole Apps und Tools

SMARTPHONE-APPS

App	Funktion	Schwierigkeitsgrad
Signal	Messaging, SMS, Telefonate (WhatsApp-Alternative)	Einfach
OrBot & OrFox	Privater im Internet surfen	Einfach
KeePassDroid	Passwort-Manager	Einfach
F-Droid	Archiv mit freier Software und Apps (Alternative zum Google Play Store)	Einfach
K9 Mail	Managt deine E-Mail-Konten (Gmail, GMX etc.)	Einfach
ChatSecure	Messaging-App für mehrere Konten wie Facebook und Google	Mittel
Transportr	Zeiten für die öffentlichen Verkehrsmittel checken	Einfach
Csip Secure	Verschlüsselte Anrufe (Skype-Alternative)	Mittel
APG	Zum Verschlüsseln von E-Mails mit K9-Mail	Schwer

SOFTWARE FÜR WINDOWS, MAC UND LINUX

Software	Funktion	Schwierigkeitsgrad
Jitsi	Verschlüsselte Video-Telefonate	Mittel
Tor Browser	Privater im Internet surfen	Einfach
Pidgin and OTR Plugin	Messaging (Facebook, Google usw.)	Mittel
Thunderbird &Enigmail	E-Mails, das Add-on Enigmail verschlüsselt deine Mails	Mittel

BROWSER PLUG-INS, ADD-ONS UND ERWEITERUNGEN

Plug-in	Funktion	Schwierigkeitsgrad
Privacy Badger	Blockiert Schnüffelprogramme	Einfach
HTTPS Everywhere	Zwingt Webseiten, die Daten bei der Übertragung zu verschlüsseln	Einfach
Disconnect.me	Blockiert Cookies und Schnüffelprogramme	Einfach
Self Destructing Cookies	Entfernt Cookies vom Computer	Mittel
NoScript	Blockiert JavaScript	Schwer

» MISSION 6: MEIN PASSWORT SOLLTE...

[R] ...eine zufällige Kombination aus Zahlen und Buchstaben sein.
[V] ... 123456789 sein – das kann man sich leicht merken!
[D] ...das erste Wort sein, das ich sehe, wenn ich ein Buch auf einer zufälligen Seite aufschlage.

Praktische Anleitung für Signal

Signal Messenger ist eine freie Android- und iPhone-App. Sie speichert nicht, was wir sagen oder mit wem wir reden. Wir können sie benutzen, um zu chatten, zu telefonieren und Bilder, Videos und Kontakte zu teilen.

Sie ist nicht einzige App, die wir zur sicheren Kommunikation verwenden können, aber sie ist von allen am einfachsten zu bedienen. Hier ist eine praktische Anleitung in fünf Schritten:

1. Geh in den Play Store (Android) oder den App Store (iPhone). Suche nach „Signal". Wähle die App „Signal Private Messenger" und tippe auf „Installieren". Öffne die App, sobald sie installiert ist.

2. Melde deine Handy-Nummer bei Signal an, indem du sie eingibst und „Registrieren" oder „Überprüfen" auswählst. Du wirst eine Textnachricht mit einem sechsstelligen Code erhalten. Gib diesen Code bei Signal ein.

3. Tippe auf den „Stift" rechts unten (Android) oder das „+"-Symbol oben rechts (iPhone), um eine Unterhaltung zu starten.

4. Wähle die Person aus, die du kontaktieren möchtest.

5. Wenn du zwischen sicheren (also verschlüsselten) Nachrichten über deine Internetverbindung und normalen SMS auswählen willst, halte „Senden" ein bisschen länger gedrückt.

Es ist viel sicherer, wenn die andere Person auch Signal benutzt. Der Messenger verwendet unsere Internetverbindung, wenn wir andere Signal-Nutzer kontaktieren. Signal kann aber auch normale SMS verwenden, wenn wir Menschen kontaktieren, die kein Signal verwenden.

Denk dran! Du musst nicht direkt jeden dazu überreden, den Signal Messenger zu benutzen. Sag es einfach deinen engsten Freunden und den Leuten, die du am häufigsten kontaktierst. Dann werden immer mehr deiner Freunde anfangen, Signal zu benutzen.

Dieses Booklet wurde ermöglicht dank:

- Einzelnen Spendern auf GlobalGiving.com – Vielen Dank an euch alle für den Beitrag!
- der Adessium-Stiftung und Open Society Foundations

Dieses Dokument wird unter einer Creative-Commons-Lizenz 2.0 verbreitet (CC BY 2.0)
http://creativecommons.org/licenses/by/2.0/