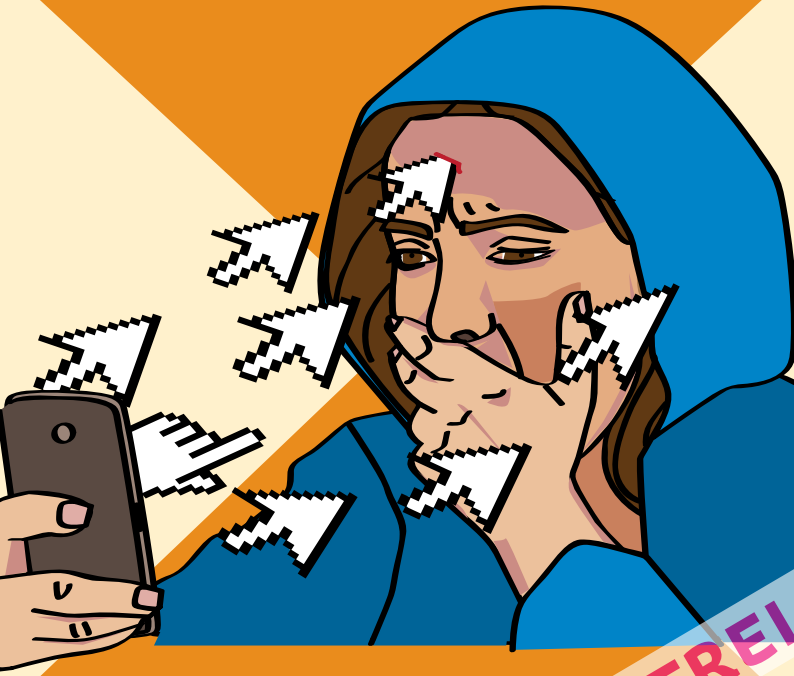
Leena Simon

Stalking, Hass, Kontrolle

Digitale Gewalt erkennen und beenden



digitalcourage

KURZ&MÜNDIG

Art d'Ameublement

Band 6

KOSTENFREI

„Mein Freund hat mir mein Handy eingerichtet, und jetzt liest er alle meine E-Mails mit.“

„Mein Ex läuft mir dauernd „zufällig“ über den Weg. Woher weiß der, wo ich bin?“

„Meine Freunde bekommen Nachrichten von mir, die ich nie geschrieben habe.“

„Jemand hat in meinem Namen ein Social Media-Profil eingerichtet und beschimpft damit Leute und verrät dort meine Geheimnisse.“

„Jemand bestellt auf meinen Namen Sachen oder meldet mich bei Newslettern an.“

Impressum

1. Auflage 02-21, Art d'Ameublement, cc-by 4.0, ISBN 978-3934636-34-7

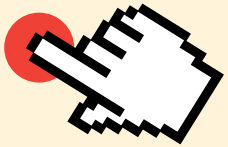
Autorin: Leena Simon, 🔗digitale-muendigkeit.de

Redaktion: Claudia Fischer, 🔗verstandenwerden.de

Layout: Isabel Wienold, 🔗iwi-design.de

Bildlizenzen: S. 16 Düng Art bei flickr; S. 23 DJANDYW.COM cc-by-sa 2.0; S. 27 und 29 geralt auf Pixabay; S. 30 Alexander Altmann cc-by-sa 4.0; S. 31 Fabian Kurz cc-by 4.0
Alle weiteren Bilder: iwi-design.de, Isabel Wienold cc-by-nc-nd 4.0

Digitale Gewalt



Gewalt verlagert sich zunehmend in den digitalen Raum. Das ist auch völlig erwartbar. Je mehr Zeit wir Menschen mit etwas verbringen, desto mehr tragen wir unsere Eigenschaften dort hin. Gewalt gehört leider zu diesen Eigenschaften.

Digitale Gewalt besteht nicht nur in verbalen Anfeindungen. Sie hat viele Gesichter und kann auch in Form von Erpressung, Nötigung oder Ausspähung vorkommen.

Digitale Gewalt ist nicht physisch, doch oft hat sie physische Auswirkungen. Leider wird sie häufig nicht so recht ernst genommen. Drohungen werden beispielsweise häufig von Polizei und Justiz herunter gespielt. Und auch Politik und das persönliche Umfeld haben häufig wenig Verständnis für Betroffene von digitaler Gewalt.

Wenn Sie Opfer digitaler Gewalt geworden sind, hilft Ihnen diese Broschüre, dem Thema auf die Spur zu kommen.

Ich wurde gehackt, was nun?

Wenn Sie den Eindruck haben, „gehackt“ worden zu sein, sollten Sie zunächst Ruhe bewahren und prüfen, ob Ihr Verdacht begründet ist. Meist gibt es nämlich sehr viel einfachere Erklärungen für ein komisches Verhalten Ihrer Geräte:

? Kann ein Defekt ausgeschlossen werden?

? Kann es Zufall gewesen sein?

? Hat der Angreifer vielleicht einfach gut geraten und weiß in Wirklichkeit viel weniger, als er vorgibt? Verbreitet er nur heiße Luft?

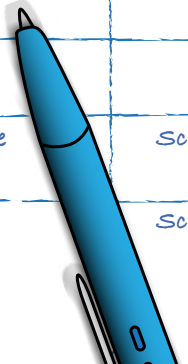
Je kritischer Sie prüfen, desto mehr können Sie hinterher Ihrem Urteil vertrauen.

Erster Schritt: Beweise sichern und bewerten

Am besten machen Sie sich eine Tabelle, ähnlich wie die hier unten. In der rechten Spalte ist Ihre Bewertung gefragt: Wie schätzen Sie den Vorfall ein auf einer Skala von 1 bis 5? Je höher der Wert, desto sicherer sind Sie sich, dass es sich nicht um einen Defekt/Zufall/heiße Luft handelt. Wie oft haben Sie hohe Werte vergeben?

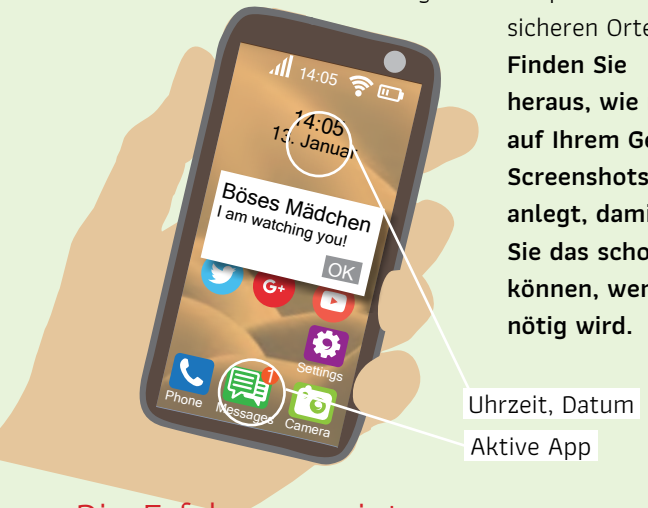
Beobachten Sie sich selbst beim Ausfüllen der Tabelle. Können Sie sich noch auf den Gedanken einlassen, dass Ihre Beobachtungen evtl. auf Zufall oder einen Defekt zurück gehen? Oder wollen Sie die Bestätigung, dass jemand Ihre Geräte manipuliert? Mehr zu diesem Thema finden Sie im Kapitel „Hypervigilanz“ auf Seite 26.

Datum/ Zeit	Was ist passiert?	Psychische/ physische Reaktionen	Beweise / Zeug.innen	Defekt /Zufall / heiße Luft?
22.01. 16:38	Treffen in Ubahn	Innere Unruhe	Marie war dabei	2* (wahrscheinlich Zufall)
28.01. 10:19	Handy stürzt ab	Denkblockade		1* (ziemlich sicher Defekt)
07.02. 18:33	SMS: „Ich weiß alles über dich.“	Einschlafprobleme	Screenshot Nr. 13	3* (unklar: tut er nur so?)
14.02. 16:22	Er schickt mir eine Mail, die ich meiner Mutter geschrieben habe.	Appetitlosigkeit, Angst	Screenshots Nr. 23 Nr. 24	5* (Er hat Zugriff auf meinen Account)



Beweise sichern

Dokumentieren Sie komisches Verhalten oder bedrohliche Nachrichten auf Ihrem Gerät, am besten als Screenshot. Achten Sie dabei darauf, dass der Kontext möglichst mitdokumentiert wird und legen Sie Kopien davon an sicheren Orten an.



Finden Sie heraus, wie man auf Ihrem Gerät Screenshots anlegt, damit Sie das schon können, wenn es nötig wird.

Die Erfahrung zeigt: Auch wenn Sie sich sicher sind, dass etwas nicht mit rechten Dingen zugeht, ist es dennoch eher unwahrscheinlich, dass Sie „gehackt" wurden, wie man sich das weitläufig – inspiriert durch Film und Fernsehen – vorstellt. Nur in den seltensten Fällen ist jemand von außen in Ihr Gerät eingedrungen und hat es manipuliert. Meist nutzen Angreifer.innen ganz andere Wege – deshalb schauen wir erst mal genauer hin, wie zuverlässig bestimmte Anzeichen sind.

Wichtig:

Jede Situation ist unterschiedlich und bedarf individueller Maßnahmen. Was im einen Moment hilft, kann es in einer anderen Situation noch schlimmer machen. Holen Sie sich daher unbedingt Unterstützung in einer Beratungsstelle.

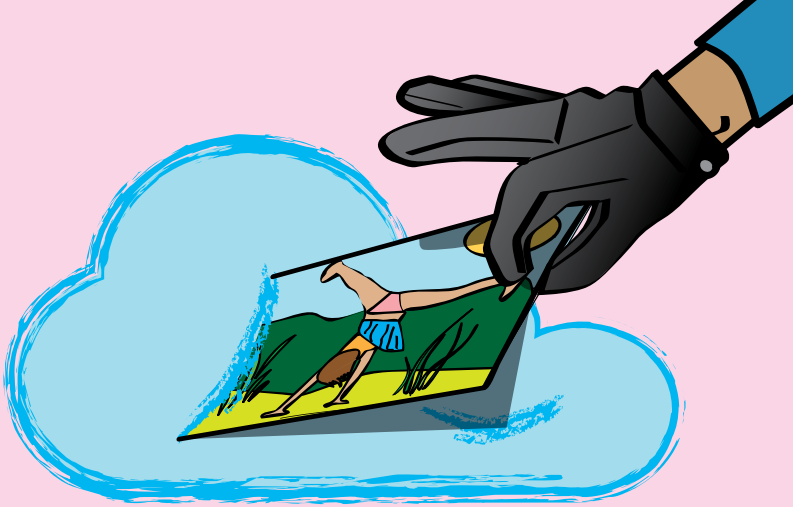
Suchen Sie im Netz nach einer guten Anlaufstelle, die Sie dann womöglich an lokale Beratungsstellen weiter vermitteln kann. Zum Einstieg: 🔗**hilfetelefon.de** oder 🔗hateaid.org

Ein paar Beispiele aus der Praxis:

„Jemand weiß Dinge, die er eigentlich nicht wissen kann. Werde ich abgehört?“ Mit einer Spy-App ist es tatsächlich möglich, ein Smartphone abzuhören. Mehr dazu finden Sie im Abschnitt zu Spy-Apps [ab Seite 18], im Kapitel „Werde ich abgehört?“ auf Seite 11 und „Der Mensch als Sicherheitslücke“ auf Seite 17.

„Ich habe das alte Smartphone meines Freundes übernommen.“ Vorsicht: Fast alle Smartphones sind mit einem Account verknüpft [Google-Account / Apple-ID], über den man umfassenden Zugriff auf das Gerät hat. Ändern Sie mindestens das Passwort, oder legen Sie [noch besser] den Account ganz neu an. [Siehe Seite 14/15]

„Mein Handy macht komische Sachen. Bin ich gehackt worden?“ Es gibt viele Gründe, weshalb sich ein Smartphone seltsam verhält. Abstürze, komische Benachrichtigungen oder Fehlverhalten können von Spy-Apps [siehe S. 18] ausgelöst werden. Es kann aber auch ganz harmlose Erklärungen geben. Mehr dazu finden Sie auf den Seiten 4/5, 10 und 14/15.



„Jemand hat Zugriff auf Handyfotos, die ich nie veröffentlicht habe.“ Werden Ihre Fotos vielleicht in einer Cloud gesichert und jemand hat Zugriff darauf? Ändern Sie umgehend Ihre Passwörter und deaktivieren Sie die Synchronisierung am besten ganz. Auch über eine Spy-App kann man die Fotos eines Gerätes anzeigen. [Siehe Seite 18]

„Mein Ex begegnet mir dauernd ‚zufällig‘.“ Kennt er Sie gut? Hat er Freunde ausgehorcht oder ist er Ihnen gefolgt? Deaktivieren Sie sicherheitshalber so oft wie möglich GPS und W-Lan auf Ihren Geräten.

Technische Probleme einschätzen

Leider sind die meisten Zeichen, an denen man Unregelmäßigkeiten feststellt, nicht eindeutig und könnten auch andere Ursachen haben.

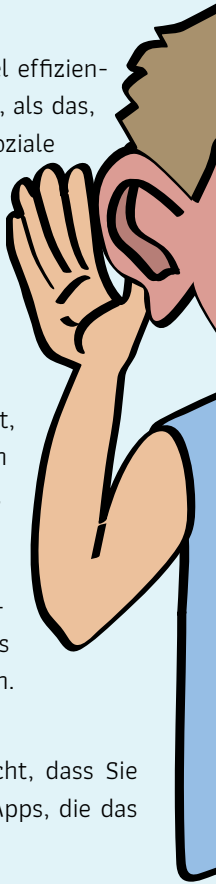
Relativ einfach zu erkennen, aber kein eindeutiges Zeichen:

- Akku geht plötzlich besonders schnell leer.
- Es werden ungewöhnlich viele Daten übertragen.
- Programme stürzen ab.
- Der Platz auf dem Datenträger nimmt ab, obwohl nichts neues installiert/gespeichert wurde.
- Der Bedroher hat Informationen, die er anders nicht haben könnte.

Eindeutiges Zeichen, aber schwer zu entdecken (z.B. von IT-Fachleuten):

- ausführbare Programme sind länger geworden
- unbekannte Programme im Arbeitsspeicher
- Der Hashwert [Prüfsumme] einer Datenmenge stimmt nicht mehr mit der Baseline [als sicher angesehener Zustand] überein.

Werde ich abgehört?



Sehr wahrscheinlich nicht. Denn es gibt viel effizientere Wege, um viel mehr über Sie zu erfahren, als das, was Sie in Gesprächen über sich preisgeben. Soziale Medien, Einkäufe, Suchmaschinen oder wie lange Sie auf einer Seite verweilen – das alles wird automatisch von Algorithmen erfasst. Durch normales Online-Verhalten geben Sie viel über sich preis.

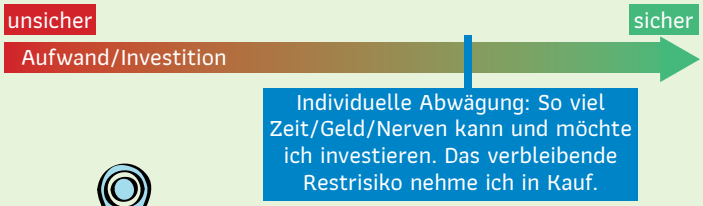
Diese Algorithmen sind mittlerweile so gut, dass wir den Eindruck kriegen, wir würden abgehört. Wir sind geneigt, das zu glauben, denn „Abhören“ ist eine Form der Überwachung, die wir greifen können. Deshalb ziehen wir sie eher in Betracht, als die völlig ungreifbaren mathematischen Verfahren, die uns täglich analysieren und in Schubladen stecken.

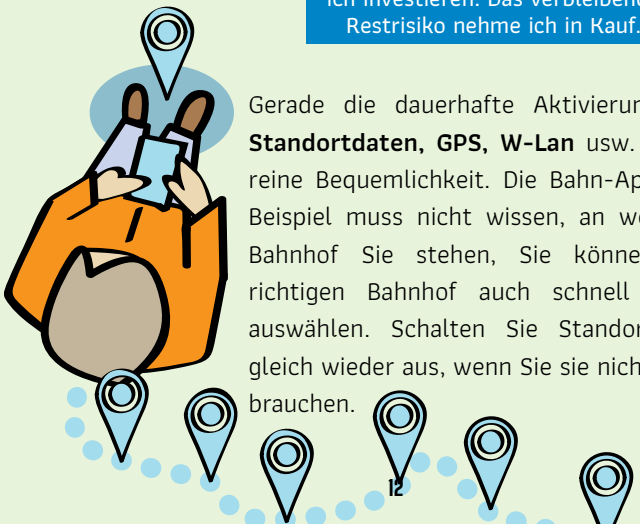
Völlig auszuschließen ist es allerdings nicht, dass Sie belauscht werden. Es gibt mittlerweile Spy-Apps, die das können. [Mehr zu Spy-Apps ab Seite 18]

Was Sie konkret für Ihre digitale Sicherheit tun können

Wenn Sie Ihre Geräte sicherer machen wollen, ist das immer eine gute Idee! Aber: IT-Sicherheit kann keine 100%ige Sicherheit gewährleisten.

Es geht also darum, abzuwägen, wie viel Restrisiko Sie bereit sind zu akzeptieren. Je geringer das Restrisiko sein darf, desto aufwändiger und unbequemer werden die dafür erforderlichen Maßnahmen.





Gerade die dauerhafte Aktivierung von **Standortdaten, GPS, W-Lan** usw. ist oft reine Bequemlichkeit. Die Bahn-App zum Beispiel muss nicht wissen, an welchem Bahnhof Sie stehen, Sie können den richtigen Bahnhof auch schnell selbst auswählen. Schalten Sie Standortdaten gleich wieder aus, wenn Sie sie nicht mehr brauchen.

Mehr Sicherheit für Ihre Geräte und Accounts

Digitale Angriffe können auf drei Wegen geschehen.

1. Gerät selbst wird angegriffen.

Für einen Geräteangriff muss man dieses Gerät in der Regel in der Hand haben [Fachleute nennen das physischen Zugriff"].

2. Ein Account, z.B. Ihr Mail-Konto, wird angegriffen.

Erfahrungsgemäß kommen Accountangriffe wesentlich häufiger vor als Angriffe auf ein Gerät. Deshalb ist es wichtig, immer beide Angriffsformen abzuwehren [siehe nächste Seite].

3. Der Angriff erfolgt auf sozialer Ebene

Für Angriffe auf sozialer Ebene braucht man keinen direkten Zugriff auf Geräte oder Accounts. Dazu gehören Verleumdung, Drohungen, unerwünschte Kontaktaufnahmen, Erpressung, Beschimpfungen, aber auch Fake Accounts, Identitätsmissbrauch oder Doxxing [Veröffentlichen von privaten Informationen]. Mehr dazu auf den Seiten 17 und 24.

Die Frage „Ist es theoretisch möglich, dass…?"
muss in digitalen Zusammenhängen
praktisch immer mit „ja" beantwortet werden.
Stellen Sie besser die Frage: „Ist es realistisch, dass…?"

Geräte und Accounts sicher machen

Bevor es zu einem Angriff kommt

Gerät

- Öffnen Sie keine Links oder Anhänge aus unbekannter Quelle.
- Bei Android-Handys gibt es eine Funktion „Software aus unbekannten Quellen installieren“. Lassen Sie das nur für Ausnahmen zu, z.B. für den F-Droid-Store.
- Schützen Sie Geräte mit einem Sperrcode, sagen Sie den Sperrcode nicht weiter und ändern Sie ihn regelmäßig.
- Vorsicht beim Installieren von Programmen!
- Halten Sie Ihre Geräte aktuell. Prüfen Sie regelmäßig, ob es Updates gibt.

Account

- Wählen Sie sichere Passwörter und teilen Sie sie mit niemandem [siehe Seite 22].
- Verzichten Sie wenn möglich auf Accounts [man kann z.B. Android-Handys mit Hilfe von F-Droid ohne Google-Konto betreiben].
- Übernehmen Sie keine Accounts von anderen, sondern richten Sie ausschließlich selbst ein.
- Besonders sensible Accounts benötigen am meisten Schutz. Dazu gehören: E-Mail-Accounts, alles was Ihre Bankdaten enthält [Online-Banking, Shopping-Accounts,] und Geräte-Accounts [Google-Account, Apple-ID].

Nachdem ich angegriffen wurde

Gerät

- Setzen Sie das Gerät auf Werkseinstellung [siehe Seite 22] zurück. [Vorher Daten sichern!]
- Ggf. Gerät austauschen
- Virenscanner-Apps und Google-Play-Protect können helfen, Schadsoftware zu entfernen.

„Beim Ändern meines Passworts habe ich gerade noch entdeckt, dass er seine Mailadresse bei „Zweitadresse“ eingetragen hatte. Er hätte sich also ein neues Passwort schicken lassen können. Und ich wäre ausgesperrt gewesen.“

Account

- Passwortwechsel [Prüfen Sie vorher, ob eine fremde E-Mail-Adresse zur Passwortwiederherstellung berechtigt ist, siehe Seite 22.]
- Löschen Sie Ihren Account und legen Sie ihn neu an.
- Behalten Sie die Zugriffe im Auge [Viele Anbieter nennen beim Login Datum und Uhrzeit des letzten Logins. Notieren Sie sich Datum und Uhrzeit ihrer Zugriffe und prüfen Sie beim nächsten Login, ob es zwischenzeitlich einen Login gab, der nicht von Ihnen stammte.]

Der Mensch als Sicherheitslücke

Haben Sie schon mal den Begriff „Social Engineering“ gehört? So nennen IT-Sicherheitsleute eine Form des Angriffs, die nicht auf die Technik als Schwachstelle zielt, sondern auf den Menschen. Deshalb erklären Ihnen Banken immer wieder, dass kein Mitarbeiter jemals nach Ihrem Passwort fragen wird: Weil Spitzbuben genau das tun.

Die Tricks sind vielfältig:

- Überzeugungskraft (Rhetorik, Täuschung, Druck)
- Manipulation und Fälschung (falsche E-Mails, Vertrauensaufbau)
- Dumpster Diving (Müll durchsuchen)
- Techniker-Trick (Defekt vortäuschen, vorgeben Techniker zu sein)
- Telefon-Trick (anrufen und Infos z.B. Logindaten erfragen)

Spy-Apps
(Spionage-Programme)

Die schlechte Nachricht ist: Es gibt sie wirklich. Programme fürs Smartphone (und den PC), mit denen sich quasi alles darauf kontrollieren lässt. Man kann alles sehen, was damit passiert, und es sogar fernsteuern. Solche Apps lassen sich auf dem Smartphone verstecken und kosten auch nicht viel.

Die gute Nachricht ist: Um so eine App zu installieren, muss man das Zielgerät in den Händen halten. Aus der Ferne kann man so etwas (bisher) noch nicht installieren. Deshalb kommen Spy-Apps erheblich seltener vor als die völlig berechtigte Angst vor ihnen.

Eine Spy-App auf einem Gerät zu finden ist sehr schwer. Ein Zeichen könnte sein, wenn plötzlich der Datenverbrauch enorm steigt oder der Akku sich schnell entleert. Aber das ist nicht eindeutig: Es könnte auch damit zu tun haben, dass der Akku alt wird und kaputt geht. Oder man hat eine andere App installiert, die viel Strom oder Daten verbraucht.

Manche Spy-Apps werden von Virenscanner-Apps oder von Google Play Protect entdeckt. Doch auch das hat seine Nachteile. Denn nicht jede App, die sich „Virenscanner“ nennt, ist auch tatsächlich ein Virenscanner. Und Google Play Protect setzt voraus, dass man Google nutzen möchte.

Auf einem iPhone kann man keine Apps verstecken. Eine Spy-App kann sich aber auch hier tarnen, indem sie sich einen harmlosen Namen gibt, wie „Wi-Fi“.

Hausputz gegen Spy-Apps

Bei aller Unsicherheit gibt es wenigstens eine gute Nachricht: **Bisher ist keine Spy-App bekannt, die das Zurücksetzen auf Werkseinstellungen überlebt hat.** Im Zweifelsfall ist das also immer Ihre letzte Option. Siehe Seite 22

Vorsorglich:

- Deinstallieren Sie alle Apps, die Sie nicht brauchen.
- Sichern Sie Ihr Gerät mit einem Sperrcode.
- Aktivieren Sie Google Play Protect (wenn Sie Google nutzen).
- Installieren Sie eine Virenscanner-App von einer renommierten Firma.

IT-Sicherheit leicht gemacht

Passwortsicherheit:

Sichere Passwörter sollten lang/komplex sein, nirgendwo doppelt verwendet und mit niemandem geteilt werden. Namen oder Geburtstage von Haustieren oder den Liebsten sind verboten. Die können viel zu leicht erraten werden.

Am besten wählen Sie vier Wörter und trennen diese mit einem Sonderzeichen. Links sehen Sie z.B. Hund.Teekanne.rot.Kopfstand – das ist sicherer und leichter als Xz7Qm9?HnqrY*

Updates:

Halten Sie ihre Systeme auf Stand. Viele Geräte sind nur deshalb angreifbar, weil sie nicht aktualisiert wurden. Deshalb ist es wichtig, immer zeitnah alle Updates zu machen.

Werkseinstellungen:

Wenn Sie das Gerät auf Werkseinstellungen zurücksetzen, werden alle nachträglich hinzugekommenen Programme und Daten gelöscht. Also auch Schadsoftware. Leider müssen Sie danach alles neu konfigurieren und installieren. Lassen Sie dies nicht über Backups oder Cloud-Dienste erledigen, da Sie sonst womöglich das wieder herstellen, was sie loswerden wollten.

Sicherheit am Computer

Tails:

Ein vollwertiges Betriebssystem auf einem USB-Stick mit jeder Menge Sicherheitsvorkehrungen. Stecken Sie den USB-Stick an Ihren Computer an und starten Sie in eine sichere Umgebung. Selbst dann, wenn Ihr Computer von Schadsoftware befallen ist.

Edward Snowden empfiehlt Tails.

Achtung: Tails löscht alle Ihre Änderungen beim Neustart. Wie Sie Ihre Dateien schützen, erfahren Sie unter 🔗tails.boum.org

Veracrypt:

Verschlüsseln Sie Daten und Kommunikation. Statt vieler verschiedener Verschlüsselungsmethoden reicht es, wenn sie nur die eine lernen: Veracrypt funktioniert für fast alle Situationen und ist recht einfach zu bedienen. Es erzeugt verschlüsselte Container, die Sie auf Festplatten, USB-Sticks, Cloudspeichern und sogar in E-Mail-Anhängen ablegen können.

Was tun bei Hass im Netz?

Wer sich öffentlich äußert, gerät leider häufig auch ins Blickfeld von Hatern [Hassern] und Trollen. Diese verfügen meist über mehrere Accounts, mit denen sie den Eindruck vermitteln, sehr viele zu sein, obwohl immer die gleiche Person dahinter steckt. Trolle und Hater verabreden sich oft, um einzelne Menschen mit einer ganzen Welle an Hasskommentaren zu überrollen. Sollten Sie Ziel eines solchen „Shitstorms“ werden, ist es ganz wichtig, Ruhe zu bewahren und den Hass so wenig wie möglich an sich ran zu lassen.

Holen Sie sich Unterstützung: Die Menschen, die ihnen wohlgesonnen sind, sind in der schweigenden Mehrheit. Teilen Sie ihnen mit, dass Sie gerade Zuspruch und Unterstützung brauchen. Dann werden sie sich melden und ihnen deutlich machen, dass nicht alle gegen Sie sind.

Springen Sie anderen bei: Wird eine Person angegriffen, will man sich oft lieber raushalten. Dabei tut es so gut, wenn man auf einen fiesen Kommentar nicht selbst antworten muss, sondern jemand anderes zu Hilfe kommt. Entlasten Sie andere, wenn Sie gerade die Kraft dazu haben.

Abschalten: Am liebsten würde man jede Nachricht über sich lesen, die im Internet gepostet wird – besonders die schlechten. Das ist sehr verständlich. Aber gönnen Sie sich Pausen davon. Legen Sie die Geräte bewusst beiseite, treffen Sie liebe Menschen und gehen Sie in den Wald oder in die Sauna.

Anzeigen, melden, blocken etc.: Handelt es sich um eine Beleidigung oder Drohung? Dann bringen Sie sie konsequent zur Anzeige und melden Sie über die Meldefunktion der sozialen Medien. Es ist auch völlig legitim, Accounts zu blocken oder zu muten [stummzuschalten]. Sie müssen sich das nicht antun. Falls in Ihrem Namen Waren bestellt werden, nehmen Sie die Ware möglichst nicht an und erstatten Sie Anzeige – das ist eine Straftat!

Hass öffentlich thematisieren: Wenn Sie öffentlich darüber sprechen, dass Sie angegriffen werden, können Sie Solidarität erfahren. Aber Vorsicht! Das kann auch den Hass weiter anregen.

Tipps für Diskussionen:

Auf so manche Nachricht möchte man nicht antworten, da sie eine leidige Diskussion auslöst. Man möchte sie aber auch nicht unbeantwortet stehen lassen. Die Lösung: Antworten Sie mit einem Link auf einen Text, der auf diese Frage antwortet. Ist das Gegenüber bereit, die Zeit zum Lesen zu investieren, lohnt sich die Diskussion. Wenn nicht, ist es Ihre Lebenszeit nicht wert.

„Nichts zu verbergen? Lies doch mal hier: https://digitalcourage.de/nichts-zu-verbergen“

Jede Antwort kostet Sie etwas Lebenszeit. Sie allein entscheiden, wem sie ein Stück davon schenken. Lassen Sie sich nicht unter Druck setzen.

„Ich habe kein Interesse, diese Diskussion fortzuführen. Tschüss.“

Manchmal ist klar, dass man das Gegenüber nicht erreichen kann. Dennoch kann sich eine Antwort lohnen. Denn auch andere lesen mit und die sind vielleicht erreichbar. Sie schreiben dann nur „für die Galerie“.

„Ich bin anderer Meinung, weil…“

Setzen Sie Grenzen. Lassen Sie sich nur auf eine Diskussion ein, wenn das Gegenüber respektvoll bleibt. Und bleiben Sie selbst freundlich. Wer wütend wird, macht sich – in den Augen der Hater – noch angreifbarer. Wer freundlich bleibt, erntet Respekt und Anerkennung.

„Lassen Sie uns doch bitte sachlich bleiben. Ich denke…“

Verwenden Sie möglichst nur Ich-Aussagen und vermeiden Sie (auch indirekte) Vorwürfe. Erfahren Sie mehr über „Gewaltfreie Kommunikation“ (GfK).

„Das kommt bei mir gerade sehr unhöflich an.“

Hypervigilanz

Kennen Sie das? Jemand behauptet, dass es keine lila Autos gibt, und erst dann fällt Ihnen auf, wie viele lila Autos es doch gibt. Etwas ähnliches passiert, wenn wir digital angegriffen werden. Dann achten wir ganz besonders auf jede Merkwürdigkeit, die unser Gerät macht, und vermuten hinter jeder davon einen Angriff.

Machen Sie sich keine Sorgen. Es handelt sich nicht um Paranoia, sondern um eine sehr gewöhnliche Reaktion: Hypervigilanz, zu Deutsch Überaufmerksamkeit.

Problematisch wird es erst, wenn Sie nicht mehr bereit sind, in Betracht zu ziehen, dass es auch eine harmlose Erklärung geben könnte. Oder wenn Sie fest von Zusammenhängen ausgehen, die Sie gar nicht überprüfen konnten. Außerdem werden hypervigilante Personen z.B. von der Polizei oft nicht ernst genommen. Das ist das Perfide an digitalen Angriffen: Man bringt die Leute dazu, sich selbst zu schädigen.

Am besten hilft ein offener Umgang damit. Gestehen Sie sich ein, wenn ein Verdacht nur ein Verdacht ist. Machen Sie sich bewusst, wenn Sie Zusammenhänge nur vermuten und kennzeichnen Sie das in ihrer Sprache anderen gegenüber. Nehmen Sie den Verdacht trotzdem Ernst. In der Ruhe liegt die Kraft.

Psychohygiene

Wenn Sie digitaler Gewalt ausgesetzt sind, sollten Sie damit nicht alleine bleiben. Machen Sie sich bewusst: Da möchte Sie jemand verletzen. Psychosoziale Beratung hilft Ihnen, diesen Versuch abzuschmettern.

Auch beim Beheben der Probleme sollten Sie gut auf Ihre Psychohygiene aufpassen. Wenn jeden Tag 5 Fake-Accounts auftauchen oder Drohungen eingehen, neigen wir dazu, dauernd danach zu suchen. Dann hat der Tag nur noch ein einziges Thema. Unser Tipp: Gibt es vielleicht eine Freundin, die das für Sie übernehmen kann?

Denken Sie immer daran: Es geht hier um Sie und nicht um die Person, die Sie bedroht. Ihr Bedroher will Sie kontrollieren – und das schafft er, wenn Sie Ihr Leben nach dem Angriff ausrichten. Lassen Sie sich das nicht gefallen! Nur Sie bestimmen, wofür Sie Ihre Lebenszeit einsetzen. Gönnen Sie sich Auszeiten.

Die Autorin

Leena Simon ist graduierte Netzphilosophin (M.A.) und IT-Beraterin und beschäftigt sich mit digitaler Mündigkeit und Technikpaternalismus. Sie arbeitet u.a. für das Anti-Stalking-Projekt in Berlin und für Digitalcourage e.V.

Ihr Ziel: Menschen befähigen, Verantwortung über ihre digitale Kommunikation zu übernehmen.

Ihr Angebot: Vorträge, Seminare, Fortbildungen (u.a. für Frauenhäuser, Bildungseinrichtungen und Beratungsstellen) und redaktionelle Beiträge

Kontakt: info@muendigkeit.digital
🔗muendigkeit.digital • 🔗anti-stalking-projekt.de

Weitere kurz&mündig-Broschüren von und mit Leena Simon:

Digitale Bildung
10 Leitlinien, um Schule frei und ganzheitlich zu gestalten
k&m Band 4

Digitale Mündigkeit
Eigenverantwortlich im 21. Jahrhundert
k&m Band 1

Die KURZ&MÜNDIG-Reihe wird herausgegeben von:

e.V. engagiert sich seit 1987 für Grundrechte, Datenschutz und eine lebenswerte Welt im digitalen Zeitalter. Wir sind technikaffin, doch wir wehren uns dagegen, dass unsere Demokratie „verdatet und verkauft" wird. Seit 2000 verleihen wir die BigBrother-Awards. Digitalcourage ist gemeinnützig, finanziert sich durch Spenden und lebt von viel freiwilliger Arbeit.

▶ Mehr zu unserer Arbeit finden Sie auf
🔗digitalcourage.de und 🔗bigbrotherawards.de

In der KURZ&MÜNDIG-Reihe sind bisher erschienen:

01 Digitale Mündigkeit
02 Datenschutzrechte in Schulen durchsetzen
03 Faire Websites
04 Leitlinien für digitale Bildung in Schulen
05 Uploadfilter
06 Stalking, Hass, Kontrolle

Dieses KURZ&MÜNDIG-Minibuch ist auch als komfortables interaktives PDF erhältlich. Es kostet nur 5,00 Euro und ist wie alle KURZ&MÜNDIG-Ausgaben (auch als Printversion) erhältlich unter: 🔗digitalcourage.de/kum

Digitale Gewalt

Woran erkenne ich, ob meine Geräte gehackt wurden? Was kann ich tun, um Angreifer vor der Tür zu lassen? Wie gehe ich mit Hatespeech um? Wie hole ich mir meine Geräte, meine digitale Freiheit und mein Leben zurück? Diese Broschüre gibt kurz und knapp die Antworten, die alle brauchen, die es mit Stalking und digitaler Gewalt zu tun haben.

Lassen Sie sich nicht in Ihr Leben reinfunken!

Digitalcourage e.V.
Marktstraße 18 | 33602 Bielefeld
mail@digitalcourage.de | digitalcourage.de
T: +49 521 1639 1639

9 783934 636347
5,00 Euro
4,00 SFR
ISBN 978-3934636-34-7

digitalcourage
k&m006 Stalking, Hass, Kontrolle