

Leena Simon

DIGITALE SICHERHEIT FÜR FRAUENHÄUSER

So schützen Sie Ihre Einrichtung
vor digitalen Angriffen.

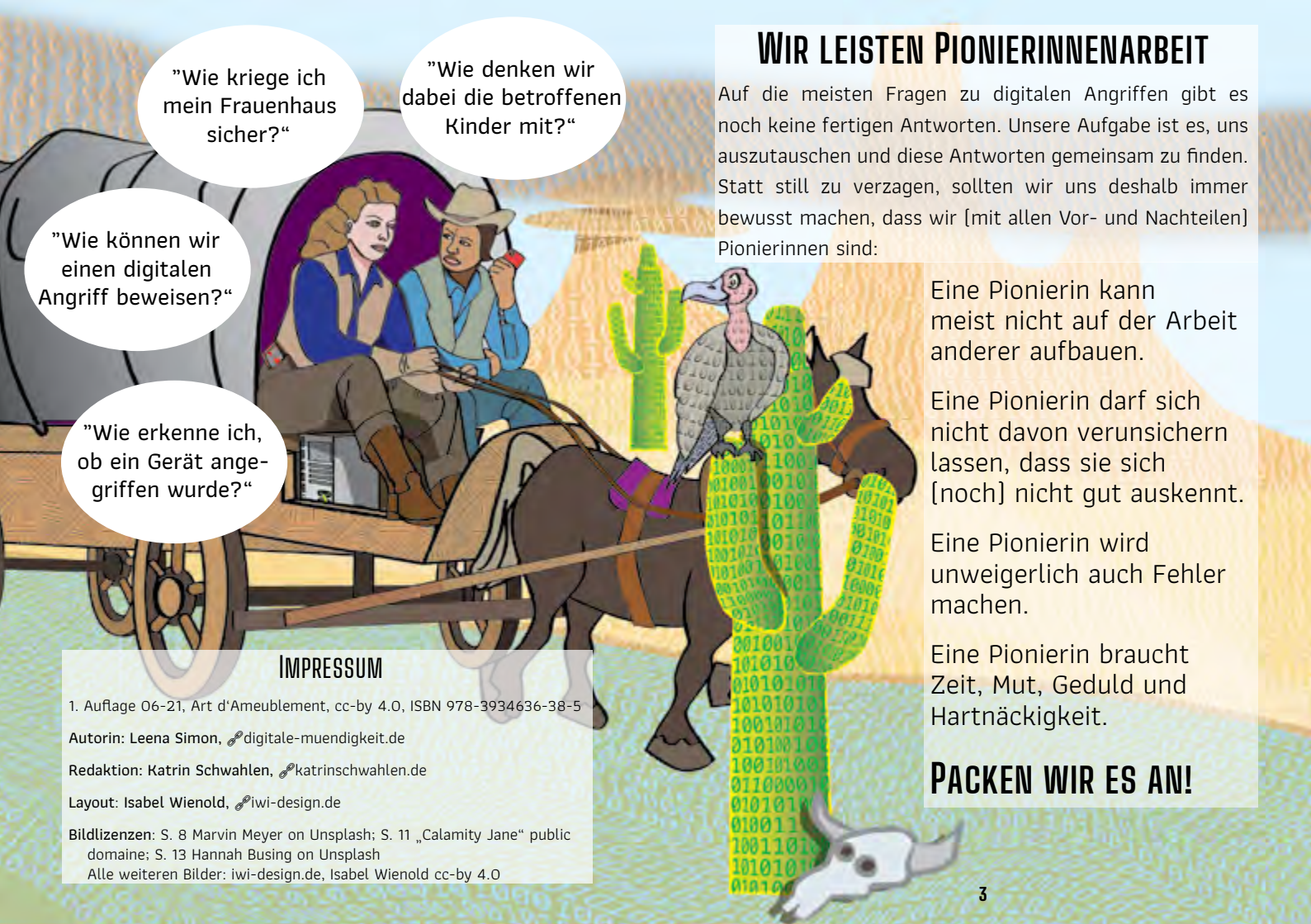


▶ digitalcourage

KURZ&MÜNDIG
ART D'AMEUBLEMENT

KOSTENFREI

BAND 10



„Wie kriege ich
mein Frauenhaus
sicher?“

„Wie denken wir
dabei die betroffenen
Kinder mit?“

„Wie können wir
einen digitalen
Angriff beweisen?“

„Wie erkenne ich,
ob ein Gerät ange-
griffen wurde?“

IMPRESSUM

1. Auflage 06-21, Art d'Ameublement, cc-by 4.0, ISBN 978-3934636-38-5

Autorin: Leena Simon, digitale-muendigkeit.de

Redaktion: Katrin Schwahlen, katrinschwahlen.de

Layout: Isabel Wienold, iwi-design.de

Bildlizenzen: S. 8 Marvin Meyer on Unsplash; S. 11 „Calamity Jane“ public
domaine; S. 13 Hannah Busing on Unsplash

Alle weiteren Bilder: iwi-design.de, Isabel Wienold cc-by 4.0

WIR LEISTEN PIONIERINNENARBEIT

Auf die meisten Fragen zu digitalen Angriffen gibt es noch keine fertigen Antworten. Unsere Aufgabe ist es, uns auszutauschen und diese Antworten gemeinsam zu finden. Statt still zu verzagen, sollten wir uns deshalb immer bewusst machen, dass wir [mit allen Vor- und Nachteilen] Pionierinnen sind:

Eine Pionierin kann meist nicht auf der Arbeit anderer aufbauen.

Eine Pionierin darf sich nicht davon verunsichern lassen, dass sie sich [noch] nicht gut auskennt.

Eine Pionierin wird unweigerlich auch Fehler machen.

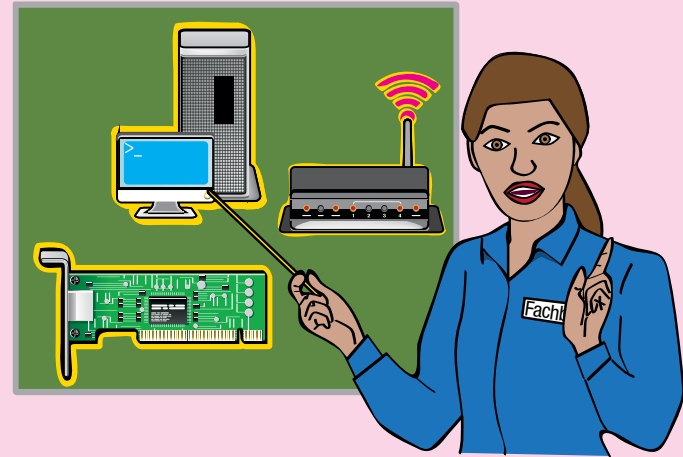
Eine Pionierin braucht Zeit, Mut, Geduld und Hartnäckigkeit.

PACKEN WIR ES AN!

SCHLUSS MIT DER VERWALTUNG DES MANGELS!

Frauenhäuser haben immer häufiger mit digitaler Gewalt zu tun und müssen Wege finden, den Betroffenen zu helfen. Dazu brauchen sie sowohl eine gute technische Ausstattung als auch das nötige Wissen über IT- und Sicherheitsmaßnahmen.

Leider fehlen häufig finanzielle und personelle Mittel. Hard- und Software sind veraltet, Administration und Sicherheit laufen „nebenbei“ mit, weil es keine fachlich ausgebildete Kollegin gibt. Für gute Teamfortbildungen fehlt das Geld.



Auf der anderen Seite kommen viele von digitaler Gewalt betroffene Klientinnen ins Frauenhaus, die zwar ihre Smartphones nutzen, aber nicht unbedingt verstehen. Damit sie nicht ungewollt sich selbst oder andere Bewohnerinnen gefährden, brauchen sie eine kompetente Anleitung.

**Um ein Frauenhaus digital zu sichern,
braucht es IT-Fachexpertise
und Finanzierung.**

Billige Lösungen gibt es nicht.

DIGITALE GEWALT

Der Begriff der digitalen Gewalt ist weit gefasst. Dazu gehören u.a. Drohungen, Nachstellung, Rufschädigung, Nötigung, Herabsetzung und Kontrolle mittels digitaler Medien und Geräte. Wenn dann noch Genderstereotype zusammenkommen, wird es besonders schwierig: Viele Frauen halten Technik und IT für „Männerthemen“. Männer wiederum nutzen ihre daraus entstehende technische Überlegenheit oft aus, um einen vermeintlichen Anspruch auf die Frau zu erheben.

Je mehr Kontrolle wir anderen über unsere Smartphones, Laptops, Tablets usw. überlassen, desto größer ist die Gefahr, dass diese Menschen Macht über uns bekommen und diese ausnutzen, um uns zu kontrollieren.

ATTACKEN UND ÜBERWACHUNG

Frauenhäuser bzw. ihre Klientinnen sind digital vor allem von sogenannten Advanced Persistent Threats (APT) betroffen. Bei dieser „fortgeschrittenen andauernden Bedrohung“ attackiert der Angreifer ein Ziel (in diesem Fall eine Person) immer wieder, mit großer Anstrengung und auf verschiedenen Wegen. Oft kommt der Bedroher aus dem nahen Umfeld der betroffenen Person und nutzt sein Insiderwissen und interne Zugriffsrechte (wie z.B. Familienfunktionen oder gemeinsame Accounts).

Um eine solche APT-Attacke zu verhindern, braucht es ein detailliertes Sicherheitskonzept. Das haben Privatpersonen und geförderte Organisationen wie Frauenhäuser aufgrund fehlender Ressourcen aber selten.



TECHNIK VERSTEHEN UND GESTALTEN

In den Computerkursen der 1980er- und -90er-Jahre ging es vor allem darum, Computer bedienen zu können. Wir haben gelernt, IT zu konsumieren, sind aber ungeübt darin, damit verantwortungsvoll umzugehen.

Privatpersonen und oft auch Organisationen investieren meist zu wenig Arbeit in sichere IT-Systeme.

IT wird selten als etwas betrachtet, dass aktiv gestaltet und betreut werden muss. Das kann nur eine fachlich kompetente Administratorin leisten.

Das Team eines Frauenhauses sollte sich fragen:

- ? Wie viel Sicherheit können und wollen wir gewährleisten? (Sicherheitsmodelle)
- ? Wie viel Restrisiko ist akzeptabel?
- ? Wie viel Arbeitszeit und Geld können wir dafür investieren?
- ? Wie stark wollen oder müssen wir die Möglichkeiten der Bewohnerinnen einschränken?
Wie binden wir sie ein?
Wie informieren wir sie über Sicherheitsmaßnahmen?
- ? Wer berät uns im Arbeitsalltag?
Wer administriert unsere Geräte?

Wichtigste Frage für die Frauenhausleitung:

- ? Wie bringen Sie Ihre Geldgeber:innen dazu, das Budget ausreichend zu erhöhen?

Modell 1: HOHE SICHERHEIT

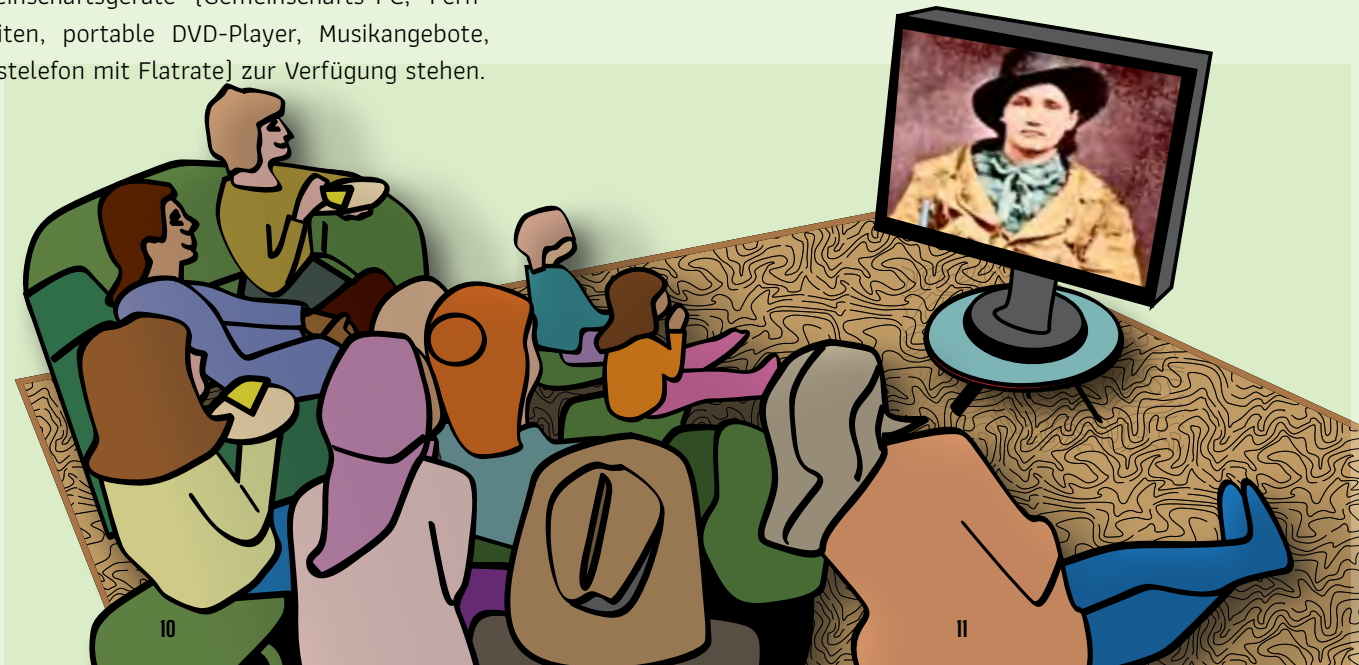
ist nur durch größtmögliche Abschottung zu erreichen. Das bedeutet, dass Kontakte zur Außenwelt weitgehend unterbunden werden. Dieses Konzept ist zwar vergleichsweise einfach umzusetzen, aber die Bewohnerinnen zahlen dafür einen hohen Preis: Sie müssen alle Geräte abgeben, bevor sie das Frauenhaus betreten.

Deshalb muss das Frauenhaus dafür sorgen, dass entsprechende Gemeinschaftsgeräte [Gemeinschafts-PC, Fernsehmöglichkeiten, portable DVD-Player, Musikangebote, Gemeinschaftstelefon mit Flatrate] zur Verfügung stehen.

Modell 2: MITTLERE SICHERHEIT

ist ein Kompromiss zwischen eingeschränkter digitaler Freiheit für die Bewohnerinnen und notwendiger Sicherheit für die Einrichtung.

Die Bewohnerinnen können sich freier im Netz bewegen, dürfen dafür aber z.B. nicht die eigenen Geräte nutzen. Stattdessen stellt das Frauenhaus für die Dauer des Aufenthalts speziell konfigurierte Geräte zur Verfügung.



Weitere Sicherheitsmaßnahmen könnten sein:



Eingeschränkter und geregelter Umgang mit Social Media.



W-Lan-Zugang nur über ein gesichertes Gastnetzwerk.



Die Bewohnerinnen dürfen ihre Smartphones behalten, konfigurieren diese aber in einem externen Training noch vor der Anreise.



Es darf nicht fotografiert werden. Die Kameras von Smartphones und Laptops werden abgeklebt.

Bei der Umsetzung dieses Konzepts ist der Administrations- und Betreuungsaufwand sehr hoch. Eingeplant werden sollten mindestens zehn Stunden pro Woche für eine erfahrene Administratorin. Die Kolleginnen sollten sich zusätzlich regelmäßig fortbilden. Für die Bewohnerinnen sind digitale Bildungsangebote notwendig. Ideal ist es, wenn eine IT-Expertin regelmäßig vor Ort ist.



Die Regeln müssen klar kommuniziert werden und es muss regelmäßig an sie erinnert werden. Das Team achtet darauf, dass die Regeln eingehalten werden. Die Nichteinhaltung sollte nicht folgenlos bleiben. Überlegen Sie sich Konsequenzen, die Sie auch einhalten können.

Modell 3: NIEDRIGE SICHERHEIT

Die **Bewohnerinnen** können ihre Geräte behalten, müssen sich aber an Anreise- und Grundregeln halten.

- ✂ GPS, Bluetooth, W-Lan sind auf allen Geräten immer ausgeschaltet.
- ✂ Alle Gerätekameras werden überklebt.
- ✂ Social-Media-Regeln müssen eingehalten werden.
[► Seite 22].
- ✂ Teilnahme an Bildungsangeboten, um die digitale Mündigkeit zu erhöhen.

Das Team

- ✂ schafft eine passende technische Infrastruktur.
- ✂ bietet Trainings u.a. zu Social Media und Passwortsicherheit an.
- ✂ stellt ein W-Lan-Gastnetz bereit.

Konkrete Schritte für die Sicherheit Ihrer Einrichtung

- ✂ Sichern Sie Ihre Passwörter!
- ✂ Sorgen Sie für regelmäßige Updates und Back-ups!
- ✂ Setzen Sie auf sichere Betriebssysteme wie Tails und Lineage OS!
- ✂ Verschlüsseln Sie Ihre Daten und Kommunikation z.B. mit Veracrypt!
- ➡ Weitere Erklärungen finden Sie in der KURZ&MÜNDIG-Broschüre „Stalking, Hass, Kontrolle – digitale Gewalt erkennen und beenden“ [Band 6].

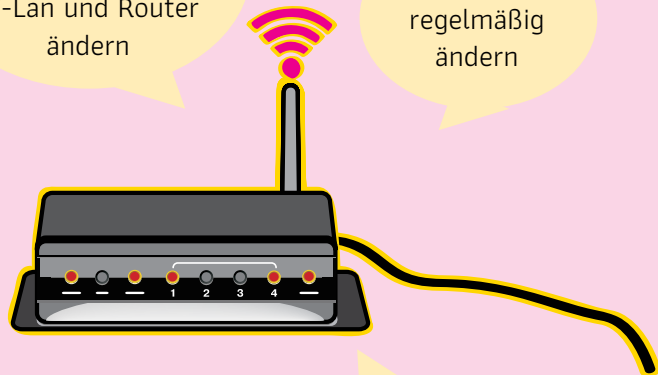


NETZWERK UND ROUTER SCHÜTZEN

Frauenhäuser sollten ein besonders gesichertes W-Lan zur Verfügung stellen:

Direkt nach Inbetriebnahme die Standardpasswörter von W-Lan und Router ändern

Passwörter regelmäßig ändern



Geschütztes Gastnetzwerk einrichten und alle anderen Netze deaktivieren. Zugriff auf den Router ist dann nur noch über Kabel möglich.

VERTRAUEN LERNEN

Bei der großen Auswahl von Serviceanbietern fällt es schwer, den richtigen zu finden. Fragen sie sich:

- ☐ Fühlen Sie sich als Kund.in ernstgenommen?
.....
- ☐ Sind die Allgemeinen Geschäftsbedingungen [AGB] des Unternehmens kurz, transparent und verständlich?
.....
- ☐ Setzt das Unternehmen freie Software ein?
Ein offener Quellcode bedeutet Transparenz.
.....
- ☐ Wie geht das Unternehmen mit Kritik um?
Firmen, die Fehler nicht eingestehen – wie z.B. Facebook – verdienen kein Vertrauen.
.....
- ☐ Wie geht das Unternehmen mit Ihren Daten um?
Wie viel müssen Sie sich von sich preisgeben, um relevante Informationen zu bekommen?
.....
- ☐ Nutzen Sie die telefonische Hotline und/oder den Tag der offenen Tür, um Mitarbeitende kennenzulernen und Vertrauen aufzubauen.



EMPFOHLENE SOFTWARE

Messenger

Den perfekten Messenger gibt es leider nicht. Während WhatsApp und Telegram als unsicher gelten, sind **Signal**, **Wire** und **Threema** etwas empfehlenswerter. Noch besser wäre ein Messenger, der über „freie Schnittstellen“ verfügt und die User.in nicht zwingt, einen bestimmten Anbieter zu wählen. Fragen Sie nach **XMPP** oder **Matrix**, wenn Sie einen wirklich sicheren Messenger suchen.

Hier finden Sie genauere Erklärungen und eine Liste empfehlenswerter Apps:

 digitalcourage.de/f-droid

Fotos

Digitale Fotos werden automatisch mit **„Metadaten“** versehen, also Informationen, wann und wo das Foto aufgenommen wurde, mit welchem Gerät u.v.m. Diese Daten werden weitergegeben, wenn man das Foto teilt. Mit dem Android-Programm **Scrambled Exif** können Sie das sehr einfach verhindern.

Apps

Android-Geräte

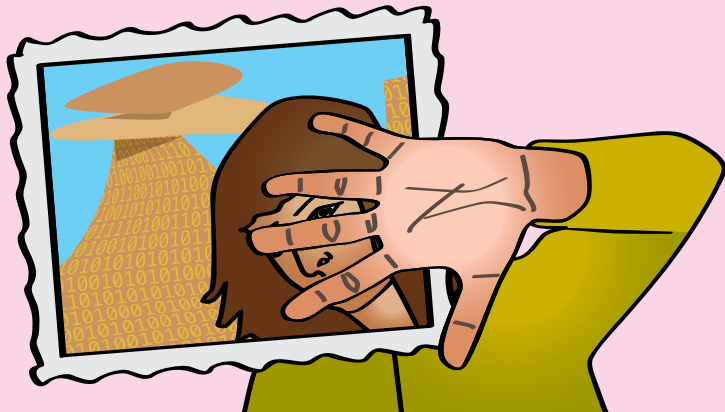
können Sie auch ohne Google-Account nutzen. Statt über den Play-Store beziehen Sie die Apps dann einfach aus dem freien App-Store **F-Droid**.

SOCIAL-MEDIA, CLOUD UND BROWSER

Facebook, Instagram, Tiktok, YouTube u.a. sind immense Datensammler. Geben Sie keine persönlichen Informationen preis und schalten Sie die **Standortübermittlung (GPS)** aus.

Ihre Klientinnen sollten Fotos in den **sozialen Medien** weder teilen noch in der Cloud speichern. Ist das Posten von Fotos erlaubt, dürfen diese keine Rückschlüsse über Ort und Bewohnerinnen geben. Metadaten sollten vorher aus den Bildern gelöscht werden. Dasselbe gilt für Texte. Accounts müssen mit sicheren Passwörtern geschützt werden.

Nutzen Sie besser freie Alternativen wie z.B. **Mastodon**, **Friendi.ca** oder **Hubzilla**.



Cloud-Dienste bieten zu wenig Schutz, Kontrolle und Transparenz darüber, welche Daten wo gespeichert werden. Müssen Sie eine Cloud nutzen, legen Sie Ihre Daten dort ausschließlich in einem **Veracrypt-Container** ab oder nutzen Sie eine **Nextcloud**, die Sie selbst kontrollieren können.

Ob Gemeinschafts-PC oder Mitarbeiterinnenrechner, jedes Gerät sollte einen **gut konfigurierten Browser** haben. Wir empfehlen:

🔧 Standard-Suchmaschine: **metager.de** oder **startpage.com**

🔧 **openstreetmap.org** statt Google Maps

🔧 **Werbung blockieren**

🔧 Besonders sicher ist der **Tor-Browser**.

Weitere Infos finden Sie hier:

🔗 digitalcourage.de/selbstverteidigung



DIGITALE MÜNDIGKEIT

Die meisten Menschen begnügen sich damit, Technik bedienen zu können, nur wenige wollen die Technik beherrschen. Diese Haltung macht es Bedroher:innen so einfach, andere digital zu drangsalieren.

Doch nicht nur Anfänger:innen fühlen sich von IT überfordert. Auch Fortgeschrittene müssen sich erst in ein Thema hineindenken, bevor sie es verstehen. Wenn Sie etwas nicht gleich verstehen, lassen Sie sich nicht entmutigen und überlisten Sie ihre Abwehrreflexe.

Probieren Sie die 30-Minuten-Regel aus, wenn Sie ein Computerproblem haben: Versuchen Sie selbst die Lösung zu finden, z.B. durch Internetrecherche. Oft werden Sie schon nach wenigen Minuten fündig. Erst, wenn Sie nach 30 Minuten nicht weiterkommen, bitten Sie um Hilfe – in Form einer Anleitung, ohne sich die Maus oder das Smartphone aus der Hand nehmen zu lassen.

Trainieren Sie Ihre [digitale] Mündigkeit ebenso regelmäßig wie Ihre körperliche Ausdauer und Kraft.



Noch mehr Informationen finden Sie in der KURZ&MÜNDIG-Broschüre "Digitale Mündigkeit".



Schauen wir uns das
mal ganz genau an!

BERATUNGSALLTAG

Wenn Sie mit betroffenen Frauen arbeiten, korrigieren Sie die Vorstellung des allmächtigen Angreifers.

Viele Menschen fühlen sich von der Digitalisierung überfordert. Bei akuter Angst vor einem digitalen Angriff werden sie oft überaufmerksam und fürchten auch dort Angriffe, wo keine sind [Hypervigilanz].

In solchen Situationen ist es wichtig, dass Sie der betroffenen Frau weder Paranoia unterstellen noch sie in ihrer Überaufmerksamkeit bestärken. Suchen Sie stattdessen gemeinsam nach dem, was sich zweifelsfrei belegen lässt. Problematisch wird es erst dann, wenn die Betroffene nicht in Betracht ziehen will, dass es auch eine andere Erklärung geben könnte.

Beispielsweise kann eine Werbung bei Facebook so treffend sein, dass man meint, abgehört worden zu sein. Tatsächlich sind es die Algorithmen der Internetgiganten, die uns erforschen und manipulieren.



Weitere Informationen zu diesem Thema finden Sie in den KURZ&MÜNDIG-Broschüren "Stalking, Hass, Kontrolle – Digitale Gewalt erkennen und beenden" [Nr. 6] und "Digitale Angriffe im Büro – Tipps für alle, die beruflich Geheimnisse wahren müssen" [Nr. 9]



DIE AUTORIN



Leena Simon ist graduierte Netzphilosophin (M.A.) und IT-Beraterin, die sich mit digitaler Mündigkeit und Technikpaternalismus beschäftigt. 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 Informationen zu diesem Thema finden Sie in den KURZ&MÜNDIG-Broschüren:



Digitale Mündigkeit

Eigenverantwortlich im
21. Jahrhundert,
k&m Band 0

Stalking, Hass, Kontrolle

Digitale Gewalt erkennen
und beenden, k&m Band 6



Die KURZ&MÜNDIG-Reihe wird herausgegeben von:

► **digitalcourage** 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 | 06 Stalking, Hass, Kontrolle |
| 02 Datenschutzrechte in Schulen durchsetzen | 07 Homeoffice |
| 03 Faire Websites | 08 Digitale Bildungsangebote selbst erstellen |
| 04 Leitlinien für digitale Bildung in Schulen | 09 Digitale Angiffe im Büro |
| 05 Uploadfilter | 10 Digitale Sicherheit für Frauenhäuser |

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

Wir Pionierinnen schaffen Lösungen.



**Für Fachexpertise und
IT-Sicherheit im Frauen-
haus- und Beratungsalltag**

Für digitale Mündigkeit

Gegen digitale Gewalt

Digitalcourage e.V.

Marktstraße 18 | 33602 Bielefeld

mail@digitalcourage.de | digitalcourage.de

T: +49 521 1639 1639



ISBN 978-3934636-38-5

5,00 Euro
4,00 SFR



digitalcourage

k&m 10 Sicherheit für Frauenhäuser