PRÄVENTIV DIGITAL ABSICHERN

Verschlüsselung der Kommunikation

Mails und Nachrichten werden häufig wie Postkarten verschickt und können leicht von Dritten gelesen werden. Das können nicht nur Betreiber*innen von E-Mail-Diensten sein, sondern auch Menschen, die bei uns zuhause den Internetzugang verwalten. Im Prinzip können alle, die sich im selben W-Lan befinden, auf unsere Kommunikation zugreifen.
Es ist sehr einfach, über die Nutzer*innenoberfläche eines Internet-Routers die gesamte Kommunikation in dem Netzwerk mitzuschneiden und jede unverschlüsselte Nachricht mitzulesen.

Eine Ende-zu-Ende-Verschlüsselung aller im Internet versendeten Nachrichten sorgt dafür, dass nur an der Kommunikation beteiligte Geräte die Nachricht lesen können.

E-Mails verschlüsseln mit PGP

Ein relativ unkompliziertes System zur Verschlüsselung von E-Mails nennt sich Pretty Good Privacy (PGP) und lässt sich mit E-Mail-Programmen wie Mozilla Thunderbird leicht einrichten.

Diese verschlüsselte E-Mail-Kommunikation ist jedoch nur dann hilfreich, wenn alle Beteiligten die PGP-Verschlüsselung eingerichtet haben und miteinander austauschen.
Eine einfache Schritt-für-Schritt-Anleitung stellt der Verein digitalcourage unter *www.digitalcourage.de/digitale-selbstverteidigung/email-verschluesselung* zur Verfügung.

Verschlüsselt chatten

Auch Direktnachrichten können verschlüsselt werden. Die Verschlüsselung übernehmen hier sogar die Kurznachrichtendienste selber.

Es reicht also aus, wenn von beiden Gesprächsparteien zum Schreiben ein Dienst gewählt wird, der eine Ende-zu-Ende-Verschlüsselung (am besten standardmäßig) anbietet.

Sichere Passwörter

Für die Sicherung unserer Daten vor unerlaubten Zugriffen brauchen wir sichere Passwörter.

Kurze Passwörter oder solche, die leicht zu erraten sind, stellen genauso wie die mehrmalige Verwendung eines Passworts ein Problem dar.

Gefährlich wird es beispielsweise, wenn das gleiche Passwort, das für einen E-Mail-Account verwendet wird, auch für Social-Media-Accounts genutzt wird. Dann kann eine Person, die das Passwort erraten hat, gleich auf mehrere Kommunikationswege zugreifen, Nachrichten versenden oder sogar diese Konten löschen.

Vorsicht auf Social-Media

Wenn wir uns auf Social-Media-Plattformen bewegen, sollte uns immer bewusst sein, dass wir uns dort in einer Art öffentlichem Raum aufhalten.

Ein schönes Foto vom Balkon kann leicht unseren Wohnort verraten, wenn jemand die Gegend kennt. Gerade wenn wir gerne private Fotos oder Neuigkeiten von uns teilen möchten, ist es empfehlenswert, die Sichtbarkeit unseres Profils möglichst stark zu beschränken. Auf den meisten Plattformen können mit der Einstellung "Privat" nur noch Abonnent*innen des Accounts die geteilten Inhalte sehen.

Alle Formen von sexualisierter Gewalt im Netz haben gemeinsam, dass sie ein Ausdruck patriarchaler Machtausübung sind. Wie auch im analogen Leben sind FLINTA* im Netz besonders gefährdet, Opfer von sexualisierter Gewalt zu werden. Um effektiven Schutz zu erreichen, müssen patriarchale Strukturen bekämpft werden.

Solidarität mit allen Betroffenen! Ihr seid nicht allein!

kritische jurist*innen leipzig

AG-Link.xyz
AG für kritische Informatik

Sigma-Stern

WAS TUN BEI: SEXUALISIERTER GEWALT IM NETZ (TW)

RECHTLICHE HINTERGRÜNDE UND ERLÄUTERUNGEN

Upskirting & Downblousing

Upskirting ist das heimliche Filmen bzw. Fotografieren unter den Rock. Downblousing bezeichnet das heimliche Aufnehmen in den Ausschnitt.

Seit 1.1.2021 ist beides nach § 184 k StGB mit einer Geldstrafe oder Freiheitsstrafe von bis zu zwei Jahren strafbar. Entsprechende Taten können bei der Polizei zur Anzeige gebracht werden.

Doxxing

Bei Doxxing handelt es sich um das Zusammentragen und anschließende Veröffentlichen von personenbezogenen Daten. Ein Problem bei Doxxing ist häufig, dass Täter*innen anonym bleiben.

Doxxing ist nicht immer strafbar. Das unbefugte Ausspähen von Informationen, die der Allgemeinheit nicht zugänglich sind, ist laut § 202a StGB mit einer Geld- oder Freiheitsstrafe bis drei Jahren strafbar. Nicht strafbar ist hingegen die Sammlung von Informationen aus frei zugänglichen Quellen.

Deep-Fake-Pornografie

Bei Deep-Fake-Pornografie werden Fotoaufnahmen von Betroffenen ohne ihre Zustimmung in bereits existierende pornografische Filme eingearbeitet, beispielsweise auf die Gesichter von Darsteller*innen.

Die Verbreitung solcher Deep Fakes ist gemäß § 201a II StGB strafbar. Bei einer Ehrverletzung ergibt sich weiterhin eine Strafbarkeit aus den §§ 185 ff StGB. Es können Geld- und Freiheitsstrafen folgen.

Die betroffene Person hat daneben Ansprüche auf Schadensersatz und Schmerzensgeld.

Revenge Porn

Bei Revenge Porn handelt es sich um die ungenehmigte Verbreitung von Nacktaufnahmen. Hierbei veröffentlicht der*die Täter*in ohne Zustimmung Foto- oder Videomaterial, dass der*die Betroffene ursprünglich freiwillig geteilt hat.

Der*die Täter*in macht sich dabei strafbar nach § 201a StGB. Der*die Betroffene hat zudem mögliche Schadensersatzansprüche aufgrund nachteiliger Folgen für die körperliche und seelische Verfassung. Auch hier bestehen Löschpflichten.

Stalking

Stalking bezeichnet ein Verhalten des willentlichen und wiederholten Verfolgens und Belästigens einer Person, das ihre physische oder psychische Unversehrtheit schädigt oder zu beschädigen droht.

Dies kann in unterschiedlichen Formen geschehen. Der § 238 StGB stellt die Nachstellung unter eine Geld- oder Freiheitsstrafe bis zu drei Jahren. Erfasst sind unter anderem das Ausspähen und Abfangen von Daten nach §§ 202a, 202b StGB sowie die Verbeitung von Abbildungen der betroffenen Person. In besonders schweren Fällen kann eine Freiheitsstrafe von drei Monaten bis zu fünf Jahren drohen, wenn beispielsweise ausgespähte/abgefangene Daten veröffentlicht werden.

Dick Pics

Ein Dickpic steht umgangssprachlich für ein Penisbild, das meist über das Internet verschickt wird. Oft werden diese ohne das Einverständnis der empfangenden Person verschickt.

Das Versenden ohne Einverständnis eines solchen Fotos ist laut § 184 Nr. 6 StGB strafbar und kann mit einer Geld- oder Freiheitsstrafe geahndet werden.

Auf *www.dickstinction.com* können solche Bilder schnell und einfach zur Anzeige gebracht werden.

Hasskommentare & anstößige Nachrichten

Hierunter werden im Allgemeinen menschenverachtende und diskriminierende Äußerungen verstanden, die meist Menschen oder bestimmte Verhaltensweisen herabwürdigen und vor allem in den sozialen Medien auftreten.

Anstößige Nachrichten sind Nachrichten mit beleidigenden oder übergriffigen Inhalten, die Personen auf allen möglichen Internet-Plattformen (auch z.B. Ebay-Kleinanzeigen, Vinted) bekommen können.

Beide Verhalten können den Tatbestand einer Beleidigung gemäß § 185 StGB erfüllen und zu einer Geld- oder Freiheitsstrafe führen.

Was tun?

- Bleib nicht alleine mit dem Erlebten!
  Hilfetelefon "Gewalt gegen Frauen": 08000 116 016
- Sichere Beweise, zum Beispiel durch Screenshots.
- Kontaktiere den*die Webseitenbetreiber*in, melde den betroffenen Inhalt oder die übergriffige Person (Eine Anleitung, wie man Inhalte auf verschiedenen Seiten melden kann, findest du hier: *www.aktiv-gegen-digitale-gewalt.de/de/technik-sicherheit/inhalte-melden-auf-facebook-und-co.html*).
- Überlege, ob du auf einem Nacktbild/Video identifizierbar sein willst. Wenn nicht, dann achte auf Wiedererkennungsmerkmale, die man nicht sehen soll (z.B. Tattoos, Muttermale oder den Hintergrund).
- Merke dir, wem du welches Foto oder Video geschickt hast. Damit kannst du es zurückverfolgen, wenn es im Internet landet.

Weitergehende Informationen:

- *www.frauen-gegen-gewalt.de/de/hilfe-beratung.html*
- *www.images.google.com*: Mit einer umgekehrten Bildersuche bei Google kannst du schauen, ob ein bestimmtes Bild im Internet zu finden ist.
- *www.hateaid.org/category/tipps-betroffene/*