ERPRESSUNG MIT NACKTBILDERN: CHECKLISTE FÜR DEN ERNSTFALL

Was als Onlineflirt beginnt, endet als Erpressung. Cyberkriminelle nutzen mitunter heimlich aufgezeichnete, intime Aufnahmen ihrer Opfer, um diese zu erpressen. Sie drohen dabei mit der Veröffentlichung von Bildern oder Videos und fordern hohe Geldsummen.

Täterinnen und Täter sprechen zwar vor allem Männer an, wenden sich aber auch an Frauen. Sie agieren oft aus dem Ausland und sind in vielen Fällen in Banden organisiert. Um ihre Spuren einfacher verwischen zu können, fordern einige auch Zahlungen in Kryptowährungen.

SO GEHEN TÄTERINNEN UND TÄTER VOR

Ihre Opfer finden Täterinnen und Täter in unterschiedlichsten Onlinechats: Das können soziale Netzwerke, aber auch zum Beispiel Dating-Plattformen sein. Dort bauen sie einen mitunter engen und zunächst harmlosen Kontakt zu ihren Opfern auf und gewinnen so deren Vertrauen. Schließlich schlagen sie beispielsweise vor, Nacktbilder auszutauschen oder per Video-Telefonie statt im Chat miteinander zu sprechen. Sexuelle Handlungen vor der Kamera zeichnen sie dann ohne das Wissen der Betroffenen auf und nutzen sie später, um diese zu erpressen. In einigen Fällen verschicken Kriminelle auch Erpresserschreiben, ohne tatsächlich kompromittierendes Material zu besitzen. Sie geben zum Beispiel vor, ein Smartphone gehackt zu haben. Dabei vertrauen sie darauf, dass Opfer befürchten, die Täterinnen und Täter hätten sich Zugang zu ihren gespeicherten Bildern oder Videos verschafft.

DAS SOLLTEN SIE TUN, WENN…

… Sie mit Nacktbildern und intimen Inhalten erpresst werden

- ✓ **Überweisen Sie kein Geld!** Nach der Zahlung hören Täterinnen und Täter meist nicht auf. Stattdessen erpressen sie ihre Opfer weiter.
- ✓ **Erstatten Sie Anzeige bei der Polizei!**
- ✓ **Brechen Sie den Kontakt zu Täterinnen und Tätern ab!** Reagieren Sie nicht auf weitere Kontaktaufnahmen.
- ✓ **Informieren Sie Chatbetreiber!** Melden Sie die Erpressung, sodass der Betreiber der Onlineplattform zum Beispiel die Profile von Täterinnen und Tätern sperren kann.
- ✓ **Veranlassen Sie die Löschung Ihrer Inhalte!** Melden Sie kompromittierende Inhalte beim Plattformbetreiber und fordern Sie eine Löschung.
- ✓ **Sammeln Sie Beweise!** Sichern Sie etwa Chatverläufe und Nachrichten mithilfe von Screenshots.

Bundesamt
für Sicherheit in der
Informationstechnik

Wir wollen, dass Sie sicher leben.
Ihre Polizei

DAS SOLLTEN SIE TUN, WENN…

… fremde Personen online Kontakt zu Ihnen aufnehmen

- ✓ **Nehmen Sie keinen Videochat von Fremden an.**
- ✓ **Stimmen Sie keinen Entblößungen oder intimen Handlungen zu.** Auch wenn Sie mit einer Person chatten, die Sie gut kennen, bleiben Risiken: Beispielsweise verschlüsselt die verwendete Plattform Ihre Daten womöglich nicht ausreichend, um sie vor Kriminellen zu schützen.
- ✓ **Nutzen Sie eine Webcamabdeckung.**

HINWEIS

Geben Sie niemals Anmeldedaten weiter. Wenn Sie anderen Personen, auch Familienmitgliedern oder engen Freundinnen und Freunden, Ihre Anmeldedaten geben, erhöhen Sie die Chance, dass Unbefugte an diese gelangen. Behalten Sie Daten wie Ihre Passwörter daher unbedingt für sich.

SO SCHÜTZEN SIE SICH IN ZUKUNFT VOR DIGITALER ERPRESSUNG

- › **Freundschaftsanfragen prüfen:** Nehmen Sie solche Anfragen ausschließlich von Menschen an, die Sie persönlich kennen.
- › **Kontakt mit Fremden einschränken:** Seien Sie misstrauisch gegenüber Fremden, die Sie im Internet kennenlernen. Meist können Sie nicht mit Sicherheit feststellen, wer die Person wirklich ist und warum sie Kontakt zu Ihnen aufnimmt.
- › **Auf persönliche Daten achten:** Sensible Informationen, etwa Ihre Anschrift, Ihr Geburtsdatum oder Ihren Arbeitgeber, sollten Sie für sich behalten.
- › **Account- und Privatsphäreeinstellungen kontrollieren:** Sie können beispielsweise einstellen, dass nur Freundinnen und Freunde Ihnen Nachrichten schicken können. Auch können Sie festlegen, wer Ihre veröffentlichten Fotos und weiteren Inhalte sehen kann.
- › **Updates installieren:** Auf diesem Weg schließen Hersteller Sicherheitslücken, bevor technisch versierte Betrügerinnen und Betrüger sie ausnutzen können.
- › **Virenschutzprogramme und Spamfilter nutzen:** So erschweren Sie es Täterinnen und Tätern, zum Beispiel unbemerkt Schadsoftware in Ihr System einzuschleusen.

Mehr Informationen zu Cybersicherheit für Verbraucherinnen und Verbraucher:
www.bsi.bund.de/VerbraucherInnen

Mehr Informationen für Opfer von Cybercrime:
www.polizei-beratung.de/infos-fuer-betroffene/cybercrime/

Bundesamt
für Sicherheit in der
Informationstechnik

Wir wollen, dass Sie sicher leben.
Ihre Polizei