Sextortion

"Als je me niet betaalt, stuur ik je naaktfoto's naar je familie!"

Sextortion

Sextortion is een samenvoeging van de Engelse woorden 'sex' en 'extortion'. We spreken van sextortion wanneer iemand wordt gechanteerd met seksueel getint (beeld)materiaal. Dit kan bijvoorbeeld een naaktfoto of video zijn, maar het kan ook gaan om gefingeerd seksueel getint materiaal of seksueel getinte chatgesprekken waarvan je niet wilt dat ze uitlekken. Meestal eist de crimineel geld of nog meer beeldmateriaal.

Wat kun je doen?

Ga niet in op chantage

In de eerste plaats; ga niet in op de chantage. Het is namelijk geen garantie dat het chanteren daarna stopt. Zolang het loont, blijven criminelen dit doen.

Laat afbeeldingen verwijderen

Neem meteen contact op met de beheerders van de site waar je belastend materiaal van jezelf hebt gevonden. Op de website is meestal een mogelijkheid voor 'help', 'meld misbruik', 'abuse' of 'contact'. Geef in de mail aan dat je nadrukkelijk geen toestemming hebt gegeven voor het plaatsen van betreffend (beeld)materiaal en vraag of ze het verwijderen.

Voor voorbeeldteksten, handleidingen en/of meer informatie zie: ***www.helpwanted.nl/content_verwijderen***

Vraag om juridisch advies

Indien een website bijvoorbeeld weigert om jouw beeldmateriaal te verwijderen kun je juridisch advies inwinnen. Dit kan gratis bij een lokale Rechtswinkel.

Monitor de afbeeldingen

Controleer of er afbeeldingen van jouw online zijn geplaatst. Dit kan onder meer via: ***www.tineye.com***

Regie over je accounts

Is je account gehackt? Verander dan indien mogelijk direct het wachtwoord en stel tweestapsverificatie in. Doe dit voor alle accounts waarvoor je hetzelfde wachtwoord gebruikt als het gehackte account.

Doe aangifte

Doe aangifte bij de politie. We begrijpen dat dit confronterend kan zijn en dat de drempel daartoe hoog is. Echter zonder aangifte kunnen we geen onderzoek starten. Bel 0900 8844 voor het maken van een afspraak. Vraag naar de zedenpolitie bij jou in de buurt. Indien ook je account is gehackt, vraag of een digitaal specialist kan aansluiten bij de aangifte.

Wat kun je doen?

Vraag hulp

Zoek hulp en steun bij mensen die je vertrouwt of slachtofferorganisaties zoals Helpwanted.nl, Qpido of Slachtofferhulp NL. Onthoud: jij bent het slachtoffer, niet de dader.

Voorkom herhaling

Beveilig je accounts

Zorg dat je beeldmateriaal goed beveiligd is. Zet je sociale media-accounts op privé, zorg dat je vriendenlijsten niet zichtbaar zijn, gebruik een sterk wachtwoord, stel tweestapsverificatie in, gebruik nooit hetzelfde wachtwoord voor meerdere accounts en maak eventueel gebruik van een wachtwoordmanager. Kijk voor meer informatie op ***www.veiliginternetten.nl***

Wees bewust

Laat je niet verleiden om materiaal te sturen naar mensen die je niet kent en/of niet vertrouwt. Wil je dit toch doen, zorg er dan voor dat je niet herkenbaar in beeld bent. Wees je ervan bewust dat het materiaal in verkeerde handen kan vallen.

Tips voor bij aangifte

Verzamelen van bewijs

Hierbij enkele adviezen om bewijs te verzamelen voor bij de aangifte. Deze gegevens kunnen het eventuele

opsporingsonderzoek helpen.

1) Vraag aan de beheerders van de site(s) waar je jouw beeldmateriaal hebt gevonden om de uploadgegevens veilig te stellen en aan je te verstrekken. Deze informatie kan mogelijk leiden naar de dader(s).

2) Verzamel zoveel mogelijk bewijs door screenshots of exports te maken van:
   a) Internetpagina's met jouw beeldmateriaal. Zorg daarbij dat het webadres (de url) te zien is op de screenshot.
   b) Alle communicatie met de dader inclusief datum, exact tijdstip, telefoonnummer email en of internetadres met gebruikersnaam en of nickname. Zie: ***www.helpwanted.nl/handleidingen***
   c) Bij een hack: maak een back up van het betreffende account.
   Lever bij een hack ook de logbestanden en IP-adressen van gekoppelde apparaten aan. Meer informatie: ***www.internetsporen.nl***
   d) Mocht je toch hebben betaald; vermeld dan de tenaamstellingen het bankrekeningnummer of bitcoinadres(sen) waarnaar je het geld hebt overgemaakt. Voeg afschriften of screenshots van de betaling bij.
   e) E-mailberichten kunnen gegevens bevatten die mogelijk kunnen leiden tot de afzenders. Dit worden "e-mailheaders" genoemd. Stel deze veilig en lever deze op de juiste manier aan. Zie voor het veiligstellen van e-mailheaders: ***www.haltabuse.org/help/headers/index.shtml***

Verwachte vragen bij de aangifte

Vertel bij het doen van de aangifte je verhaal zo kort en bondig mogelijk in chronologische volgorde. Het kan helpen dit van te voren alvast puntsgewijs op papier te zetten en mee te nemen.

Vragen over het beeldmateriaal

- Wie hebben allemaal beschikking over het (beeld)materiaal?
- Hoe is het materiaal uitgelekt? Of hoe weet je dat je bent gehackt?
- Ben je herkenbaar op de beelden te zien?

Chantage (afdreiging)

- Op welke manier heeft de dader contact gezocht? Vermeld eventuele gebruikersnamen, nicknames, telefoonnummers, account ID's, e-mailadressen, signalementen.
- Heb je afdreigingen ontvangen over het verspreiden van het beeldmateriaal?
- Vraagt de dader geld of andere tegenprestaties? Zo ja, wat precies?
- Wat is het totale schadebedrag?
- Heb je aan andere tegenprestaties dan geld gedaan? Zo ja, wat precies?
- Heb je na betaling of tegenprestaties weer dreigingen ontvangen? Zo ja, wat precies?

Verspreiden beeldmateriaal

- Op welke manier dreigt de dader het (beeld)materiaal te verspreiden? Via sociale media, jouw werk, (online)contacten, pornosites, videoplatformen etc.
- Hoe ben je erachter gekomen dat jouw (beeld)materiaal is verspreid?
- Welke stappen heb je ondernomen om het (beeld)materiaal offline te halen?

Contact

- Is er een relatie met de mogelijke dader?

Strafbare feiten

De volgende strafbare kunnen van toepassing zijn:

Afdreiging (artikel 318 Wetboek van Strafrecht).

Afpersing zonder dat er sprake is van het dreigen met geweld (Chantage).

Dwang (artikel 284 Wetboek van Strafrecht)

Afdreiging zonder dat er een duidelijk financieel oogmerk is.

Vervaardigen afbeelding van seksuele aard (artikel 139h Wetboek van Strafrecht)

Indien er zonder jouw toestemming afbeeldingen van seksuele aard zijn geopenbaard (wraakporno).

Computervredebreuk (Artikel 138ab Wetboek van Strafrecht)

Indien er sprake is van hacken.

Identiteitsfraude (artikel 231b Wetboek van Strafrecht)

Indien er zonder jouw toestemming met jouw personalia bijvoorbeeld een account is aangemaakt.

Heimelijk filmen (artikel 139f Wetboek van Strafrecht)

Indien er zonder jouw toestemming en zonder jouw medeweten op een besloten plaats beeldmateriaal is opgenomen.

Heling gegevens (artikel 139g Wetboek van Strafrecht)

Indien er niet-openbare gegevens van jou zoals wachtwoorden, of afbeeldingen zijn verhandeld.

Handige links

Meer tips zijn te vinden op

www.vraaghetdepolitie.nl/dwang-en-seks/chantage/wat-kan-ik-doen-tegen-sextortion.html
www.internetsporen.nl
ww.helpwanted.nl
www.meldpunt-kinderporno.nl
www.slachtofferhulp.nl/gebeurtenissen/seksueel-misbruik-geweld/sextortion/
www.qpido.nl