Annonce de service public

FEDERAL BUREAU OF INVESTIGATION

Le 5 juin, 2023

Alerte numéro :
I-060523-PSA

Les questions relatives à cette annonce de service publique doivent être adressées à votre **bureau local du FBI.**

Bureaux locaux du FBI :
www.fbi.gov/contact-us/field-offices

Manipulation de photos et de vidéos par des opérateurs malveillants en vue de créer des contenus explicites et des stratagèmes de sextorsion

Le FBI lance un avertissement au public concernant des opérateurs malveillants qui créent des contenus synthétiques (communément appelé « deepfakes »[a]) en manipulant des photos ou des vidéos anodines en vue de cibler des victimes. Les avancées technologiques ne cessent d'améliorer la qualité, la personnalisation, et l'accessibilité de la création de contenu assistée par l'intelligence artificielle. Le FBI continue de recevoir des rapports de victimes, y compris des enfants mineurs et des adultes non-consentants, dont les photos ou les vidéos ont été modifiées pour produire un contenu explicite. Ces photos ou ces vidéos sont ensuite diffusées publiquement sur des réseaux sociaux ou sur des sites web pornographiques, dans le but de harceler les victimes ou de se livrer à des stratagèmes de sextorsion.

Création de contenu explicite

Les opérateurs malveillants utilisent des technologies et des services de manipulation de contenu afin d'exploiter des photos et des vidéos – généralement capturées à partir du compte de réseaux sociaux d'une personne, de l'internet ouvert, ou demandées à la victime - en images à caractère sexuel qui semblent plus vraies que nature, puis les font circuler sur les réseaux sociaux, les plateformes publiques, ou sur les sites web pornographiques. De nombreuses victimes, y compris des mineurs, ne savent pas que leurs images ont été copiées, manipulées, et distribuées jusqu'à ce que quelqu'un d'autre leur en fasse part. Les photos sont alors envoyées directement aux victimes par les opérateurs malveillants à des fins de sextorsion ou de harcèlement, ou jusqu'à ce qu'elles soient découvertes par elles-mêmes sur l'Internet. Une fois que les photos ont été diffusées, les victimes peuvent faire face à des défis importants en termes d'empêcher le partage continu du contenu manipulé ou de le supprimer de l'internet.

Sextorsion et harcèlement

La sextorsion,[b] qui peut constituer une violation de plusieurs lois pénales fédérales, consiste à contraindre les victimes à fournir des photos ou des vidéos sexuellement explicites d'elles-mêmes, puis à les menacer de les partager publiquement ou avec la famille et les amis de la victime. Les principales motivations sont le désir d'obtenir davantage de contenu plus illicite, un gain financier, ou le désir d'intimider et de harceler d'autres personnes. Les opérateurs malveillants ont utilisé des photos ou des vidéos manipulées dans le but d'extorquer une rançon aux victimes ou d'obtenir leur consentement à d'autres demandes (par exemple, l'envoi de photos de nu).

Depuis le mois d'avril 2023, le FBI a constaté une augmentation du nombre de victimes de sextorsion signalant l'utilisation de fausses images ou de vidéos créées à partir de contenus publiés sur leurs sites de réseaux sociaux ou sur le web, fournies aux opérateurs malveillants sur demande, ou capturées lors de chats vidéo. D'après les rapports récents de victimes, les opérateurs malveillants exigent généralement ce qui suit : 1. Un paiement (par exemple, de l'argent, des cartes-cadeaux) avec la menace de partager les photos ou les vidéos avec des membres de la famille ou des amis sur les réseaux sociaux si les fonds ne sont pas reçus ; ou 2. l'envoi par la victime de véritables images ou vidéos à caractère sexuel.

Les recommandations :

Le FBI exhorte le public à faire preuve de prudence lorsqu'il publie ou envoie par messagerie directe des photos, des vidéos ou des informations d'identification personnelles sur les réseaux sociaux, les applications de rencontre et d'autres sites en ligne. Bien qu'apparemment inoffensives lorsqu'elles sont publiées et partagées, les photos et les vidéos peuvent fournir aux opérateurs malveillants une abondance de contenu à exploiter pour des activités criminelles. Les progrès de la technologie de création de contenu et les photos personnelles accessibles en ligne offrent aux opérateurs malveillants de nouvelles possibilités de trouver et de cibler les victimes. Celles-ci sont alors vulnérables à l'embarras, au harcèlement, à l'extorsion, à la perte financière, ou à la revictimisation à long terme.

Le FBI recommande au public de tenir compte des éléments suivants lors d'un partage de contenu (par exemple, des photos et des vidéos) ou d'un échange avec des personnes en ligne :

- Surveillez l'activité en ligne des enfants et discutez des risques associés au partage de contenu personnel.

- Faites preuve de discrétion lors de la publication d'images, de vidéos et de contenu personnel en ligne, en particulier lorsqu'il s'agit d'enfants or d'informations les concernant.

    - Les images, vidéos, ou informations personnelles publiées en ligne peuvent être capturées, manipulées, et distribuées par des auteurs malveillants à votre insu ou sans votre consentement.

  - Une fois qu'un contenu est partagé en ligne, il peut être extrêmement difficile, voire impossible, de le supprimer une fois qu'il a été diffusé ou publié par des tiers.

- Effectuez des recherches fréquentes en ligne sur vos informations et celles de vos enfants (par exemple, nom complet, adresse, numéro de téléphone, etc.) afin d'identifier l'exposition et la circulation d'informations personnelles sur l'internet.

- Appliquez les paramètres de confidentialité sur vos comptes de réseaux sociaux, notamment en définissant les profils et les listes d'amis comme privés, afin de limiter l'exposition publique de vos photos, vidéos, et autres informations personnelles.

- Envisagez d'utiliser des moteurs de recherche d'images inversée pour repérer les photos ou les vidéos qui ont circulé sur le net à votre insu.

- Soyez prudents lorsque vous acceptez des demandes d'amis, communiquez, participez à des conversations vidéo, ou envoyez des images à des personnes que vous ne connaissez pas personnellement. Méfiez-vous en particulier des personnes qui vous demandent immédiatement de leur fournir des images ou qui font pression sur vous pour que vous les fournissiez. Ces éléments peuvent être capturés à l'écran, enregistrés, manipulés, partagés à votre insu ou sans votre consentement, et utilisés pour vous exploiter ou exploiter quelqu'un que vous connaissez.

- Ne donnez pas de l'argent ou d'autres objets de valeur à des personnes inconnues ou non familières. Le fait de se conformer aux opérateurs malveillants ne garantit pas que vos photos ou contenus sensibles ne seront pas partagés.

- Faites preuve de discrétion lors des échanges avec des personnes connues en ligne qui semblent agir en dehors de leurs habitudes. Les comptes de réseaux sociaux piratés peuvent facilement être manipulés par des opérateurs malveillants pour gagner la confiance d'amis ou de contacts afin de faire avancer des projets ou des activités criminels.

- Sécurisez vos comptes de réseaux sociaux et autres comptes en ligne en utilisant des mots de passe ou de phrases de passe complexes et une authentification multifactorielle.

- Renseignez-vous sur les politiques de confidentialité, de partage et de conservation des données des plateformes de réseaux sociaux, des applications, et des sites web avant de télécharger et de partager des images, des vidéos ou d'autres contenus personnels.

Federal Bureau of Investigation

Annonce de service public

Pour obtenir plus d'informations sur la sextorsion, consultez l'annonce de service public du 2 septembre 2021, « *FBI Warns about an increase in Sextortion Complaints*, » [« Le FBI met en garde contre une augmentation des plaintes en matière de sextorsion »] à l'adresse suivante : https://www.ic3.gov/media/Y2021/PSA21092.

En outre, les communiqués de presse du FBI mentionnés ci-après contiennent des informations importantes sur ce type d'escroquerie :

- https://www.fbi.gov/news/press-releases/international-law-enforcement-agencies-issue-joint-warning-about-global-financial-sextortion-crisis.

- https://www.fbi.gov/news/press-releases/fbi-and-partners-issue-national-public-safety-alert-on-financial-sextortion-schemes.

Le Centre national pour les enfants disparus et exploités [*National Center of Missing and Exploited Children, NCMEC*, en anglais] propose un service gratuit appelé ***Take it Down*, [éliminer]** qui peut aider les victimes, qui sont en possession des fichiers image ou vidéo, à supprimer ou à arrêter le partage en ligne de contenus de nudité totale ou partielle ou de contenu sexuellement explicite qui ont été pris alors qu'elles étaient âgées de moins de 18 ans. Pour plus d'informations, consultez le site : https://takeitdown.ncmec.org.

SI vous croyez être victime d'un crime utilisant ce genre de tactique, conservez toutes les informations relatives à l'incident (par exemple, noms d'utilisateurs, adresses électroniques, sites web ou noms de plateformes utilisées pour la communication, photos, vidéos, etc…) et signalez-le immédiatement au :

- FBI's Internet Crime Complaint Center [Le centre de plaintes du FBI contre la criminalité sur Internet] à l'adresse suivante : www.ic3.gov
- Bureau régional du FBI [www.fbi.gov/contact-us/field-offices, ou appelez le 1-800-CALL-FBI (225-5324)
- *National Center for Missing and Exploited Children* [Centre national pour les enfants disparus et exploités] (1-800-THE LOST ou www.cybertipline.org)

Le signalement de ces crimes peut aider les forces de l'ordre à identifier les opérateurs malveillants et à prévenir d'autres victimes.

Federal Bureau of Investigation

Annonce de service public

Le terme « [a] Deepfake » désigne le large éventail de médias numériques générés ou manipulés (par exemple, des images, des vidéos, du son ou du texte ; collectivement appelés « contenu synthétique » ou « médias synthétiques ») créés à l'aide de processus d'intelligence artificielle et d'apprentissage automatique. Les « deepfakes » peuvent représenter la modification ou l'usurpation de l'identité d'une personne pour faire croire qu'elle fait ou dit des choses qu'elle n'a jamais faites ou dites.

En principe, le contenu synthétique peut être considéré comme une liberté d'expression protégée en vertu du premier amendement ; toutefois, le FBI peut enquêter lorsque les faits et les rapports associés indiquent des violations potentielles de lois pénales fédérales. Les applications mobiles, les « *deepfake-as-a-service,* » et d'autres outils disponibles au public rendent la tâche de plus en plus facile aux opérateurs malveillants de manipuler des images ou vidéos existantes ou d'en créer des nouvelles. Ces outils, souvent disponibles gratuitement en ligne, sont utilisés pour créer des contenus deepfake très réalistes et personnalisables des victimes ciblées ou pour cibler des victimes secondaires associées.

La [b]sextorsion est une forme de coercition et d'exploitation sexuelle des enfants qui, selon les circonstances, peut enfreindre plusieurs lois pénales fédérales, (par exemple, la production de matériel pédopornographique [en violation de l'article 2251(a) du titre 18 du Code des États-Unis], la coercition/l'incitation d'un mineur [en violation de l'article 2422(b) du titre 18 du Code des États-Unis], la réception/possession/distribution de matériel pédopornographique (en violation de l'article 2252A du titre 18 du Code États-Unis), et/ou l'extorsion par le biais de communications interétatiques [en violation de l'article 875 (d) du titre 18 Code des États-Unis]).