Comprendre le chiffrement: les liens avec la sécurité des victimes

Pour de nombreuses victimes de violence domestique, d'agression sexuelle, de harcèlement criminel et de trafic, disposer de moyens privés et sécurisés pour communiquer et stocker des fichiers par voie électronique est essentiel à leur sécurité. Pour les fournisseurs de services aux victimes et les autres professionnels travaillant avec les victimes d'abus, l'utilisation d'outils de communication et de stockage privilégiant la confidentialité et la sécurité contribue à garantir la protection de la vie privée et de la sécurité des victimes. Un chiffrement fort est un élément essentiel de la solution.

Voici quelques exemples de la manière dont le chiffrement de bout en bout et le chiffrement à connaissance nulle peuvent contribuer à atténuer les impacts des abus liés à la technologie.

1. Planifier et déménager en toute sécurité :

Le chiffrement de bout en bout peut fournir un canal sécurisé permettant à une victime de faire des plans et de communiquer avec des personnes de confiance, comme lors d'une tentative de déménagement ou d'obtention d'un logement et d'un soutien. (Cela est particulièrement vrai lorsque l'agresseur n'a pas accès aux appareils ou aux comptes de la victime.)

2. Protéger l'intégrité des preuves:

L'utilisation du chiffrement de bout en bout et du chiffrement à connaissance nulle lors du stockage et du transfert de preuves numériques aux forces de l'ordre, aux procureurs ou à d'autres professionnels du système juridique permet de maintenir l'intégrité de ces preuves. Lorsque les preuves numériques sont transmises par des sources non sécurisées ou qu'il existe une possibilité d'interception, l'intégrité des preuves peut être diminuée, ce qui augmente la probabilité que leur authenticité soit remise en question devant un tribunal.

3. Protection contre les accès non autorisés :

Un accès non autorisé aux données peut se produire lorsqu'une communication en cours d'envoi (données en transit) est interceptée ou lorsque des informations stockées dans une base de données en ligne ou un coffre-fort en ligne (données au repos) sont violées. C'est pourquoi il est essentiel que toutes les données—celles en transit et

Qu'est-ce que le chiffrement et comment fonctionne-t-il ?

Généralement, le chiffrement est un processus qui consiste à brouiller les informations afin qu'elles ne puissent être lues que par ceux ayant accès aux clés pour les déchiffrer. Ce processus de désembrouillage est appelé déchiffrement. Tous les chiffrements ne sont pas identiques et certaines plateformes de communication et de stockage en ligne utilisent des méthodes de chiffrement faibles. Pour garantir que les victimes gardent le contrôle de leurs informations, il est important qu'aucun tiers ne dispose d'une clé pour accéder à leurs communications ou aux informations stockées dans le cloud.

Le chiffrement de bout en bout offre le niveau de sécurité et de confiance le plus élevé pour les technologies de communication, car, de par sa conception, seuls l'appareil de l'expéditeur et l'appareil du destinataire prévu détiennent les clés pour déchiffrer le message. Pour les cas où des données sensibles doivent être stockées en ligne en toute sécurité, ce que l'on appelle le chiffrement à « connaissance nulle » ou « connaissance zéro » devrait être la norme. Ce niveau de chiffrement signifie que personne, à l'exception du titulaire du compte, ne peut consulter les données.

celles au repos—soient protégées avec le plus haut niveau de chiffrement. Les informations communiquées sans chiffrement de bout en bout courent un risque accru d'être violées par des tiers. En outre, les informations stockées sans chiffrement à connaissance nulle risquent davantage d'être violées. Les deux types de violations peuvent avoir un impact négatif sur la vie privée, la sécurité et le bien-être des victimes en révélant des informations sensibles. Cela pourrait amener leur agresseur à les retrouver après leur déménagement, ou à la perte de preuves liées à leur procès en cours, ou à la divulgation d'informations personnelles pouvant avoir un impact négatif sur leur capacité à obtenir ou à conserver un logement ou un emploi.

4. Chercher de l'aide :

Le chiffrement de bout en bout permet aux victimes de communiquer en toute sécurité lorsqu'elles décident de demander de l'aide. Il contribue à protéger contre l'interception, la suppression et l'altération. Il permet de garantir que les communications privées restent privées, de sorte que seuls les appareils de l'expéditeur et du destinataire prévu puissent accéder aux messages.

Protéger le chiffrement de bout en bout pour protéger les victimes

Un chiffrement fort est un outil essentiel contribuant à protéger la confidentialité et la sécurité des victimes. Malheureusement, les efforts pour saper le chiffrement de bout en bout et le chiffrement à connaissance nulle porteront également atteinte à la confidentialité et à la sécurité des victimes. L'utilisation de formes de chiffrement plus faibles ou la création de portes dérobées aux méthodes de chiffrement les plus sécurisées menace la sécurité de tous ceux qui en dépendent pour leurs communications privées.

La meilleure façon de garantir la sécurité des utilisateurs en ligne est de continuer à préserver des pratiques de chiffrement de bout en bout et de chiffrement à connaissance nulle sans compromis, et d'adopter des politiques de chiffrement fort et de les renforcer. Les victimes de violence domestique, d'agression sexuelle, de harcèlement criminel et de trafic méritent de savoir que leurs communications privées restent confidentielles lorsqu'elles recherchent de l'aide et que les preuves qu'elles collectent peuvent être préservées sans risque de falsification ou de suppression malveillante. Lorsque la technologie basée sur le chiffrement de bout en bout et le chiffrement à connaissance nulle est disponible pour les victimes, celles-ci disposent de plus d'options pour trouver de l'aide, la sécurité et la guérison.

Pour en savoir plus sur les éléments techniques et humains du chiffrement, consultez www.internetsociety.org, et pour en savoir plus sur la manière d'aider les victimes, consultez www.techsafety.org. Suivez-nous sur Twitter @internetsociety et @nnedv.