CREATION DE FAUX PROFIL, PHISHING

Conseils pratiques publié le **14/11/2024**, vu **15 fois**, Auteur : Murielle Cahen

Les infractions servant de base légale à la répression de la cybercriminalité ont toutes pour point commun d'utiliser les systèmes et réseaux numériques

« La cybercriminalité », également appelée criminalité informatique, consiste en la réalisation de délits commis à l'aide d'équipements informatiques et d'Internet. Parmi les exemples classiques de cybercriminalité, il est possible de citer la diffusion de virus informatiques, le téléchargement illégal, les actes de phishing, le vol d'informations personnelles telles que des données bancaires ou données à caractère personnelles, la création de faux profils, l'usurpation d'identité sont devenus des tactiques courantes utilisées par des cybercriminels pour tromper les utilisateurs innocents et obtenir des informations sensibles.

Ces activités criminelles, qui ont pris de l'ampleur avec l'augmentation exponentielle de l'utilisation d'Internet, posent un sérieux défi à la sécurité dans notre société numérique. Cet article vise à démystifier l'univers sombre de la création de faux profils, du phishing et de l'usurpation d'identité, à comprendre leurs implications et à explorer des solutions potentielles pour prévenir de telles attaques à l'avenir."

I. La création de faux profils

1. Les motivations derrière la création de faux profils :

La création de faux profils est devenue une pratique courante sur les médias sociaux et les plateformes en ligne. Les individus malveillants utilisent de fausses informations personnelles et des photos volées pour se dissimuler derrière une identité fictive. Ces faux profils peuvent être utilisés pour l'arnaque en ligne, l'intimidation, le harcèlement, l'espionnage ou même pour voler des informations sensibles. Pour éviter de tomber dans le piège, assurez-vous de vérifier attentivement les profils avant d'établir une relation en ligne et signalez tout comportement suspect aux administrateurs de la plateforme. Quelle que soit la motivation, la création de faux profils porte atteinte à la confiance en ligne et peut avoir des conséquences néfastes pour les victimes.

2. Les dangers de la création de faux profils :

L'un des dangers les plus évidents de la création de faux profils est la propagation de fausses informations. Les faux profils peuvent être utilisés pour diffuser des rumeurs, propager des discours de haine ou même nuire à la réputation d'une personne. De plus, les faux profils peuvent être utilisés pour l'usurpation d'identité, où les informations personnelles d'une personne sont utilisées à des fins malveillantes.

3. Les conséquences de la création de faux profils :

Les conséquences de la création de faux profils peuvent être graves. Les victimes peuvent subir des atteintes à leur vie privée, des dommages à leur réputation et même des préjudices émotionnels. De plus, si les faux profils sont utilisés à des fins d'arnaque, les victimes peuvent subir des pertes financières importantes. Il est essentiel de prendre cette menace au sérieux et de mettre en place des mesures pour se protéger.

4. Comment se protéger de la création de faux profils :

- Soyez attentif aux signes révélateurs de faux profils, tels que des photos douteuses, des informations contradictoires ou des activités suspectes.

- Vérifiez attentivement les profils avant d'établir une relation en ligne ou de partager des informations personnelles.

- Ne partagez pas d'informations sensibles avec des personnes que vous ne connaissez pas en personne.

- Signalez tout faux profil aux administrateurs des plateformes concernées.

- Protégez vos informations personnelles en utilisant des paramètres de confidentialité appropriés sur les médias sociaux et en évitant de les partager publiquement.

La création de faux profils en ligne présente de nombreux dangers et conséquences néfastes. Il est essentiel d'être vigilant et de prendre des mesures pour protéger notre identité en ligne . En sensibilisant les autres à cette pratique et en signalant les faux profils, nous contribuons à maintenir un environnement en ligne plus sûr et plus fiable. N'oubliez pas que la confiance en ligne repose sur l'authenticité et l'intégrité, et en travaillant ensemble, nous pouvons limiter l'impact de la création de faux profils.

II. Le phishing : Comment se protéger des attaques en ligne

1. Qu'est-ce que le phishing ?

Le phishing est une technique sophistiquée utilisée par les cybercriminels pour obtenir des informations confidentielles. Ils se font passer pour des entités légitimes, telles que des banques ou des entreprises bien connues, et envoient des e-mails ou des messages trompeurs demandant aux destinataires de divulguer leurs informations personnelles. Soyez vigilant face à ces tentatives de phishing en vérifiant toujours l'authenticité des expéditeurs, en évitant de cliquer sur des liens

suspects et en utilisant des outils de sécurité tels que des logiciels antivirus et des filtres anti-spam.

2. Comment fonctionne le phishing ?

Les cybercriminels utilisent diverses techniques pour tromper les utilisateurs. Ils peuvent envoyer des e-mails ou des messages texte qui semblent provenir d'une marque ou d'une institution bien connue, demandant aux utilisateurs de mettre à jour leurs informations ou de cliquer sur un lien suspect. Ces liens redirigent souvent les utilisateurs vers des sites web frauduleux qui ressemblent à s'y méprendre aux sites légitimes, mais qui sont conçus pour voler des informations.

3. Comment se protéger contre le phishing ?

- Soyez vigilant : Méfiez-vous des e-mails, des messages texte ou des appels téléphoniques non sollicités vous demandant de fournir des informations personnelles. Vérifiez toujours l'authenticité de l'expéditeur ou de l'appelant.

- Ne cliquez pas sur les liens suspects : Évitez de cliquer sur des liens provenant de sources non fiables ou douteuses. Si vous avez des doutes, rendez-vous directement sur le site officiel de l'organisation concernée.

- Utilisez des outils de sécurité : Installez un logiciel antivirus et un pare-feu pour protéger votre ordinateur ou votre appareil mobile contre les attaques de phishing. - Mettez à jour vos logiciels : Assurez-vous que tous vos logiciels sont à jour, car les mises à jour contiennent souvent des correctifs de sécurité importants.

Il peut être réprimé en vertu de l'article 323-1 du Code pénal, qui punit le fait d'accéder ou de se maintenir, frauduleusement, dans tout ou partie d'un système de traitement automatisé de données est puni de trois ans d'emprisonnement et de 100 000 € d'amende.

Lorsqu'il en est résulté soit la suppression ou la modification de données contenues dans le système, soit une altération du fonctionnement de ce système, la peine est de cinq ans d'emprisonnement et de 150 000 € d'amende.

Lorsque les infractions prévues aux deux premiers alinéas ont été commises à l'encontre d'un système de traitement automatisé de données à caractère personnel mis en œuvre par l'Etat, la peine est portée à sept ans d'emprisonnement et à 300 000 € d'amende.

Le phishing est une menace sérieuse qui peut causer des pertes financières et compromettre la sécurité des utilisateurs en ligne. En étant attentif et en prenant des mesures de sécurité appropriées, nous pouvons réduire les risques d'être victime d'une attaque de phishing. Souvenez-vous toujours de rester méfiant face aux demandes de renseignements personnels et de signaler tout cas suspect aux autorités compétentes. J'espère que cet article te sera utile pour comprendre le phishing et prendre les mesures nécessaires pour te protéger en ligne.

III. L'usurpation d'identité

1. Qu'est-ce que l'usurpation d'identité ?

En France, cela peut être répréhensible en vertu de l'article 226-4-1 du Code pénal, qui punit le fait d'usurper l'identité d'un tiers de l'identité d'un tiers ou de faire usage d'une ou plusieurs données de toute nature permettant de l'identifier en vue de troubler sa tranquillité ou celle d'autrui, ou de porter atteinte à son honneur ou à sa considération. Les sanctions pour cette infraction peuvent inclure des amendes et des peines de prison.

2. Les dangers de l'usurpation d'identité :

L'usurpation d'identité peut avoir des conséquences graves. Les victimes peuvent subir des pertes financières importantes, des dommages à leur réputation, et une détresse émotionnelle considérable. De plus, il peut être difficile de récupérer son identité une fois qu'elle a été usurpée. Les victimes doivent souvent faire face à des tracas administratifs, des litiges avec les institutions financières et une violation de leur vie privée.

3. Comment se protéger contre l'usurpation d'identité :

- Protégez vos informations personnelles : Ne partagez pas d'informations sensibles en ligne, à moins que cela ne soit absolument nécessaire. Utilisez des mots de passe forts et uniques pour vos comptes en ligne, et évitez de les réutiliser sur plusieurs plateformes.

- Soyez vigilant : Surveillez régulièrement vos relevés bancaires et vérifiez vos comptes en ligne pour détecter toute activité suspecte. Si vous constatez quelque chose d'anormal, signalez-le immédiatement à votre banque ou à l'institution concernée.

- Utilisez la vérification en deux étapes : Activez la vérification en deux étapes pour renforcer la sécurité de vos comptes en ligne. Cela ajoute une couche supplémentaire de protection en exigeant un code ou une confirmation supplémentaire lors de la connexion.

- Méfiez-vous des tentatives de phishing : Soyez prudent avec les e-mails et les messages suspects. Ne cliquez pas sur les liens ou les pièces jointes provenant de sources non fiables, et ne fournissez jamais d'informations personnelles par e-mail ou par message.

4. Que faire si vous êtes victime d'usurpation d'identité :

- Signalez immédiatement le problème à la police et aux autorités compétentes.

- Contactez votre banque pour bloquer vos comptes et émettre de nouvelles cartes si nécessaire.
- Informez les bureaux de crédit pour surveiller votre historique de crédit et vous protéger contre les activités frauduleuses.

- Modifiez tous vos mots de passe et mettez en place des mesures de sécurité supplémentaires pour vos comptes en ligne.

L'usurpation d'identité en ligne est une menace sérieuse qui peut causer de nombreux problèmes et préjudices. En prenant des mesures pour protéger vos informations personnelles et en étant vigilant face aux tentatives de fraudes, vous pouvez réduire les risques d'être victime d'usurpation d'identité. N'oubliez pas de signaler toute activité suspecte et de prendre les mesures appropriées pour protéger votre identité en ligne.

Sources :

1. Cour de cassation, criminelle, Chambre criminelle, 24 janvier 2018, 16-83.045, Publié au bulletin - Légifrance (legifrance.gouv.fr)

2. Cour de cassation, criminelle, Chambre criminelle, 23 janvier 2019, 18-82.833, Publié au bulletin - Légifrance (legifrance.gouv.fr)

3. Cour de cassation, civile, Chambre commerciale, 28 mars 2018, 16-20.018, Publié au bulletin - Légifrance (legifrance.gouv.fr)

4. Cour de cassation, civile, Chambre commerciale, 22 janvier 2020, 18-18.640, Inédit - Légifrance (legifrance.gouv.fr)

5. Cour de cassation, civile, Chambre commerciale, 13 février 2019, 17-23.139, Inédit - Légifrance (legifrance.gouv.fr)

6. Cour de cassation, criminelle, Chambre criminelle, 6 septembre 2023, 23-80.684, Inédit - Légifrance (legifrance.gouv.fr)

7. Cour de cassation, criminelle, Chambre criminelle, 2 septembre 2020, 19-87.356, Inédit - Légifrance (legifrance.gouv.fr)

8. Cour de cassation, criminelle, Chambre criminelle, 16 novembre 2016, 16-80.207, Inédit - Légifrance (legifrance.gouv.fr)