OUCH! Septembre 2024

Les voix fantômes : se défendre contre les attaques de clonage de voix

L'appel inattendu : une histoire de tromperie

Fabienne, enseignante à la retraite, profitait de ses matinées paisibles dans sa petite maison de banlieue. Un jour, alors qu'elle prenait son café du matin, elle a reçu un appel frénétique de son petit-fils, Julien, qui était parti à l'université. Il explique d'une voix paniquée qu'il a eu un accident de voiture et qu'il a besoin d'argent de toute urgence pour payer les dégâts et éviter les ennuis judiciaires. S'il n'arrivait pas à avoir l'argent rapidement, il pouvait finir en prison. La voix au bout du fil était sans aucun doute celle de Julien. Fabienne s'est immédiatement inquiétée. Sans se poser de question, elle s'est précipitée à sa banque pour envoyer l'argent à Julien. Ce n'est que plus tard, lorsque Fabienne a téléphoné à la mère de Julien pour avoir de ses nouvelles, qu'elle comprit qu'elle avait été arnaquée. Un cybercriminel avait utilisé une technologie de clonage de voix par intelligence artificielle (IA) pour imiter la voix de Julien, en utilisant l'amour et l'inquiétude de Fabienne pour son petit-fils.

Qu'est-ce que le clonage de voix ?

On parle de clonage vocal lorsqu'une personne utilise l'IA pour recréer la voix d'une personne en y incluant ses tics vocaux, ses intonations et ses rythmes d'élocution, créant ainsi une réplique quasi parfaite.

Une attaque par clonage de voix commence avec un cybercriminel qui collecte des échantillons audio de la voix de la cible. Ces échantillons peuvent être récoltés à partir de diverses sources telles que des vidéos sur YouTube ou des publications personnelles sur TikTok. Après s'être entraînée sur le son enregistré, l'IA génère un nouveau son qui ressemble à celui de la cible. Cette voix générée peut être utilisée de différentes manières, des appels téléphoniques aux messages vocaux, ce qui en fait un puissant outil de tromperie.

Lorsqu'ils créent des attaques par clonage de voix, les cybercriminels commencent souvent par faire des recherches. La plupart des informations dont ils ont besoin sont accessibles au public sur les sites de réseaux sociaux. Ils étudient les victimes auxquelles ils s'adressent, c'est-à-dire à la fois la voix de la personne qu'ils vont reproduire et la victime qu'ils vont appeler. Les cybercriminels apprennent non seulement qui leurs victimes connaissent et en qui elles ont confiance, mais aussi quels sont les déclencheurs émotionnels les plus efficaces. Lors de ces appels téléphoniques, les cyber-attaquants modifient souvent l'identification de l'appelant, de sorte que lorsque les victimes regardent leur téléphone, l'appel semble provenir d'un numéro auquel elles font confiance. L'identification de l'appelant peut être facilement falsifiée et n'est pas un bon moyen de valider ou d'authentifier les personnes qui vous appellent.

Protégez-vous

Pour se protéger, il faut d'abord savoir que le clonage de voix est désormais possible et de plus en plus facile à réaliser pour les cyber-attaquants. Voici quelques mesures que vous pouvez prendre pour vous protéger :

- **Vie privée**: soyez vigilants et limitez les informations que vous partagez avec d'autres personnes, et restreignez l'accès aux enregistrements de vous sur les réseaux sociaux.

- **Indices**: soyez à l'affût d'indicateurs communs indiquant que quelque chose ne va pas. Si quelqu'un vous appelle avec un énorme sentiment d'urgence ou vous presse d'agir immédiatement, il s'agit très probablement d'une escroquerie. Plus le sentiment d'urgence est grand, par exemple en exigeant de l'argent immédiatement, plus il est probable que quelqu'un essaie de vous pousser à commettre une erreur. Parmi les autres indicateurs courants, citons les choses trop belles pour être vraies (non, vous n'avez pas gagné à la loterie) ou un appel inattendu qui vous semble bizarre.

- **Vérification**: si vous n'êtes pas sûr que l'appel est légitime, raccrochez et rappelez la personne sur un numéro de téléphone de confiance. Par exemple, si vous recevez un appel téléphonique d'un cadre supérieur ou d'un collègue de votre entreprise, rappelez-le à un numéro de téléphone de confiance que vous savez être le sien. Si vous recevez un appel téléphonique étrange d'un membre de votre famille, essayez de le rappeler (peut-être même par appel vidéo) ou appelez un autre membre de la famille qui le connaît bien.

- **Mots de passe**: créez une phrase secrète ou un code d'accès que seuls vous et votre famille connaissez. Ainsi, si vous recevez un appel téléphonique étrange qui semble provenir d'un membre de votre famille, vous pouvez vérifier s'il s'agit bien de lui en vérifiant s'il connaît votre code secret.

Rédacteur Invité

Maria Singh est Cyber Content Manager chez EnterpriseKC et membre passionné de WiCyS avec plus de 14 ans d'expérience en technologie et cybersécurité. Elle est titulaire d'une certification SANS GIAC GSEC et candidate à un Master of Science en Cybersécurité à l'Université de Purdue. En tant qu'ancienne présidente de Women in Security Kansas City et lauréate du prix OCA Corporate Achievement, Maria est une source d'inspiration pour les femmes dans les domaines des STIM et de la cybersécurité. Ses conférences et son leadership ouvrent la voie aux générations futures pour qu'elles s'épanouissent dans ces domaines.

Ressources

Les trois principaux moyens utilisés par les cyberattaquants pour vous cibler : https://www.sans.org/newsletters/ouch/top-ways-attackers-target-you/
Stop aux appels téléphoniques frauduleux : https://www.sans.org/newsletters/ouch/stop-phone-call-scams/
Déclencheurs émotionnels, comment les cyber-attaquants vous piègent-ils ? :
https://www.sans.org/newsletters/ouch/emotional-triggers-how-cyber-attackers-trick-you/

Traduit pour la communauté par : Juliette Busson