www.lapresse.ca /actualites/2024-01-22/hypertrucage-audio/berne-par-la-fausse-voix-de-son-fils.php

Hypertrucage audio et berné par la fausse voix de son fils

Charles-Éric Blais-Poulin ⁝

Fernand Boissonneault, 91 ans, en est persuadé : c'est la voix de son fils qu'il entendait au bout du fil, le 15 décembre à 11 h 30.
« Papa, je suis en prison. »

Le « chauffard », paniqué, expliquait au téléphone avoir renversé une femme alors qu'il tenait son cellulaire au volant.
Il resterait détenu jusqu'à la fin de son procès s'il ne versait pas une caution.
« Un avocat va te téléphoner bientôt. »

La sonnerie retentit.

L'interlocuteur se présente sous le nom de M^{e} Martin-Ménard.
Le juriste explique qu'une caution de 5800 $ doit être versée pour que l'accusé soit libéré. Un nouvel appel est prévu pour convenir de l'endroit où déposer les sommes.

Inquiet, M. Boissonneault obtempère.
Il retire les billets à la banque, puis rappelle son fils :

« Bonne nouvelle, c'est réglé, tu vas pouvoir sortir.

— De quoi tu parles ? »

C'est là que M. Boissonneault comprend qu'il a été berné.
Le Trifluvien, comme de nombreux Québécois, est convaincu que l'intelligence artificielle (IA) a été utilisée pour imiter la voix de son fils.
Le recours à ce procédé, avec l'émergence de nouveaux outils grand public, est un jeu d'enfant, avons-nous pu constater en tentant de reproduire la voix de notre collègue Patrick Lagacé, avec son accord (voir encadré).

Dans la dernière année, des médias américains ont fait état d'un modus operandi semblable à celui décrit par M. Boissonneault.
Un expert et au moins un service de police contactés par *La Presse* ne doutent pas que le stratagème a fait son chemin jusqu'au Québec.

« Le trucage audio est disponible depuis au moins une décennie », mais « ce qui a changé, c'est l'accessibilité, la rapidité et la précision des outils », note Philippe Chevalier, directeur de SarX, agence de détectives privés en ligne et de cyberenquête.

« Se rendre à l'évidence »

La Presse a pu vérifier, en composant des numéros inscrits sur l'afficheur de victimes, que les fraudeurs utilisent le *spoofing*, une technique archi simple visant à faire croire qu'un appel provient de n'importe quelle combinaison de chiffres.

M. Chevalier ne serait pas surpris que les escrocs opèrent à partir d'un autre continent, par exemple l'Asie.
Les outils de traduction vocale font tomber les barrières linguistiques, explique-t-il.
Les capacités de la police à intervenir s'en trouvent largement diminuées.

Pour l'instant, les autorités policières du Québec hésitent à confirmer le recours à des technologies avancées dans des fraudes de type grands-parents.
Puisque les appels frauduleux ne sont pas enregistrés, prouver le recours à l'intelligence artificielle est difficile.

La Presse a pu parler à cinq Québécois qui disent avoir été la cible ou avoir été témoins d'un coup de fil impliquant l'hypertrucage audio.
Dans quatre cas, les victimes avaient fait des démarches pour retirer des milliers de dollars avant d'obtenir de vraies nouvelles de leur proche, ce qui a fait échouer le stratagème.

Devant le nombre et la diversité des témoignages de citoyens, la Régie intermunicipale de police Roussillon, dont le territoire couvre sept villes au sud-ouest de l'île de Montréal, a diffusé un avertissement sur sa page Facebook le 16 janvier.

PHOTO ANDRÉ PICHETTE, ARCHIVES LA PRESSE

La Régie intermunicipale de police Roussillon a diffusé un avertissement sur sa page Facebook.

« Si l'on parlait d'un seul cas, on pourrait croire à des problèmes cognitifs, par exemple, mais il faut se rendre à l'évidence », dit Karine Bergeron, agente aux relations communautaires et médiatiques.
Au fil de rencontres de prévention, « des personnes de tous les âges nous disent avoir reconnu la voix d'un proche.
Une dame a même raconté que le défaut de langage de son fils, très reconnaissable, avait été reproduit ».

Cette vague de fraudes diffère aussi des arnaques usuelles de type grands-parents : il s'agirait davantage de fraudes de type parent, puisque c'est souvent la mère ou le père de l'« appât » qui est contacté.

Maîtres fraudeurs

L'avocat Patrick Martin-Ménard, titre et nom utilisés par au moins un fraudeur, existe bel et bien.
Son bureau est situé dans Hochelaga-Maisonneuve.
L'escroc qui a usurpé son identité aurait d'ailleurs précisé à certaines victimes que son cabinet se trouvait à l'angle des rues Viau et Hochelaga.

Environ une dizaine de personnes ont contacté M^{e} Martin-Ménard – le vrai ! – pour savoir s'il était bel et bien l'auteur d'appels afin de demander une caution pour un client.

« Heureusement, à cette étape-là, les victimes n'avaient pas encore transféré l'argent », explique-t-il en entrevue avec *La Presse*.

L'avocat a fait un signalement au Service de police de la Ville de Montréal (SPVM) et a déposé une plainte pour « supposition de personne ».
Le poste de quartier 23, raconte-t-il, lui a fait savoir que sa requête resterait sans suite, puisque les auteurs de fraudes téléphoniques sont trop difficiles à identifier et à localiser.

Je ne vous cache pas que je suis très déçu de l'inaction de la police.

L'avocat Patrick Martin-Ménard

Fernand Boissonneault raconte lui aussi s'être fait dire par les autorités policières que ses plaintes seraient vaines puisqu'il a flairé l'arnaque avant de vider ses poches : il n'est donc pas considéré comme une victime.

Pas d'IA, selon la SQ

C'est la Sûreté du Québec (SQ) qui assure la veille des dossiers de fraude téléphonique à l'échelle de la province.

« L'émergence de l'intelligence artificielle dans les différentes sphères de la société est un phénomène inévitable et la Sûreté du Québec surveille la situation de près », écrit par courriel la sergente Éloïse Cossette, porte-parole de l'organisation provinciale.
Or, selon la SQ, « l'IA n'est en cause dans aucun dossier de fraudes grands-parents ».

Le SPVM et le Service de police de Laval indiquent eux aussi ne pas avoir ouvert de dossiers de fraude « avec imitation de la voix ».

La Régie intermunicipale de police Roussillon, de nombreuses cibles ainsi que leurs proches ont un écho différent.

La créatrice numérique Patricia Paquette, par exemple, raconte que sa voix a été reproduite par un fraudeur qui souhaitait piéger son père.
Ce dernier a découvert le pot aux roses notamment parce que son interlocuteur s'est présenté à lui comme étant son « petit-fils ».

Bien qu'impressionné par la qualité de la voix, « mon père m'a mentionné que [le fraudeur] avait des hésitations et revenait toujours avec les mêmes questions », explique M^{me} Paquette.

L'auteur de l'appel, croit-elle, a utilisé un logiciel *text-to-speech* (du texte à la parole), qui permet de générer facilement et rapidement une voix de synthèse à partir d'un texte écrit.

La voix d'une personne est reconstruite à partir de différents enregistrements sonores accessibles, par exemple, dans les réseaux sociaux ou dans les médias.
« Ma voix étant largement disponible, ils ont pu avoir des échantillons », explique la streameuse chez GeekZoneQC.

Collecte d’échantillons

L’hypertrucage audio ouvre des portes insoupçonnées pour tout type de fraudes – amoureuses, de type grands-parents, du président ou du faux représentant.

Le premier ministre Justin Trudeau, l’animatrice Anne-Marie Dussault, le chef d’entreprise Elon Musk ou encore la chanteuse Nathalie Simard ont tous vu leur voix être dupliquée – avec plus ou moins de succès – dans les derniers mois dans le cadre d’arnaques commerciales ou financières dans les réseaux sociaux.

Les interventions vocales de ces personnalités sont facilement accessibles, mais quid du commun des mortels ?

« On reçoit parfois des appels de numéros inconnus et il n’y a rien qui se passe », fait remarquer Philippe Chevalier, directeur de SarX.

Ce sont souvent des réseaux qui cherchent à collecter des échantillons de voix pour les stocker.
Ces informations sont ensuite reliées à des renseignements personnels dans des banques de données faites maison.

Philippe Chevalier, directeur de SarX

Selon l’expert de la fraude à l’ère numérique, l’IA atteint son plein potentiel pour les fraudeurs lorsqu’elle est jumelée à de l’ingénierie sociale, c’est-à-dire la manipulation par la psychologie.
L’appropriation d’informations personnelles ou encore la simulation d’une situation d’urgence ou de détresse font partie des stratégies déployées.

« En repérant des infos sur un réseau social comme Instagram ou Facebook, il est possible d’en savoir assez sur une personne pour se faire passer pour elle », note M. Chevalier.
« Alors, même si le son n’est pas parfait [parce qu’il est] préenregistré ou [produit] en direct avec des moyens artisanaux, tout est question de facteur humain. »

S’il n’avait pas réussi à joindre son fils à temps, M. Boissonneault aurait aujourd’hui été dépouillé de près de 6000 $.
Les fraudeurs, eux, ne semblent pas avoir à craindre pour leur liberté, avec ou sans caution.

Imiter une voix en quelques minutes

PHOTO PATRICK SANFAÇON, ARCHIVES LA PRESSE
Patrick Lagacé

Avec l'autorisation de notre collègue Patrick Lagacé, nous nous sommes donné comme défi de reproduire son timbre de voix et ses intonations avec un logiciel en ligne grand public.
Nous avons choisi un outil en fonction de son accessibilité, mais il est à noter que les fraudeurs peuvent compter sur des technologies beaucoup plus performantes.
Avec un forfait de base à moins de 15 $ par mois, il nous a fallu moins de 15 minutes pour générer des clips audio qui auraient très bien pu être enregistrés par le chroniqueur de *La Presse* et animateur radio du 98,5 à la voix familière.
Jugez-en par vous-mêmes.

Comment se prémunir contre les fraudes avec l'IA ?

L'éducation demeure la meilleure arme pour déjouer les fraudes téléphoniques.
Mais encore plus avec l'émergence des nouvelles technologies, les internautes doivent faire preuve de discernement quant aux informations personnelles qu'ils diffusent publiquement et qui pourraient être récupérées par des escrocs, souligne Philippe Chevalier, directeur de SarX, agence de détectives privés en ligne et de cyberenquête.
« L'intelligence artificielle nous oblige à faire preuve de discernement et de bon jugement », dit-il.
« C'est ce qui distingue l'être humain de la machine.
Elle donne à la fois des outils et une obligation de vigilance. »
Des technologies pour détecter l'usage de l'IA existent, mais elles sont faillibles et ne sont pas à la portée du commun des mortels.

Dans le doute, il vaut mieux prendre un pas de recul et contacter ses proches.

Les victimes sont quant à elles invitées à signaler les évènements à leur institution bancaire, aux autorités policières et au Centre antifraude du Canada.

Recherche et mise en page par:
Michel Cloutier
CIVBDL
20240122
"C'est ensemble qu'on avance"