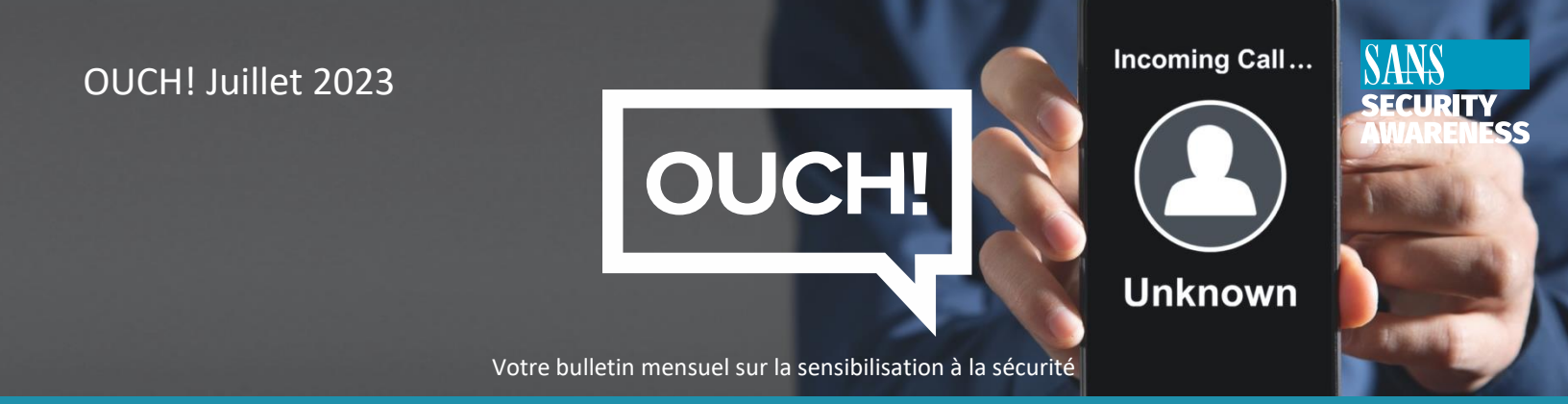
OUCH! Juillet 2023



Votre bulletin mensuel sur la sensibilisation à la sécurité

Stop aux escroqueries par téléphone

L'histoire

David regardait sa série préférée en streaming quand il a reçu un appel d'un numéro qu'il ne connaissait pas. L'indicatif régional était le même que le sien, il a donc supposé que c'était une personne locale et a répondu. Immédiatement, la personne au bout du fil a demandé à David de confirmer son identité complète. L'interlocuteur a ensuite déclaré être de la police et annoncé à David qu'un mandat d'arrêt avait été déposé contre lui. David aurait des impôts impayés et s'il ne les réglait pas dans les 24 heures, la police devrait l'arrêter. David a pris peur et a demandé ce qu'il devait faire.

L'interlocuteur lui a procuré le numéro de téléphone du service des impôts de l'administration locale, où il pourrait s'occuper de ses impôts impayés. David a immédiatement raccroché et a ensuite appelé ce numéro, où une aimable dame a répondu et s'est présentée comme étant du service des impôts local. David lui a donné toutes ses coordonnées. Au bout d'un moment, elle lui a confirmé qu'il avait 1 487,72 dollars d'impôts à payer. S'il payait immédiatement par téléphone avec sa carte de crédit, elle pourrait régler la situation et il n'irait pas en prison. David s'est senti soulagé et lui a immédiatement donné les informations relatives à sa carte de crédit. Le montant total a été débité et l'interlocuteur lui a dit que tout était résolu.

L'attaque

Le problème, c'est que les personnes qui appelaient n'étaient ni de la police, ni d'une agence fiscale gouvernementale. Il s'agissait de deux criminels travaillant ensemble pour escroquer les gens. Ils appelaient des milliers de personnes au hasard et répétaient la même histoire. Ils utilisaient un logiciel spécial pour s'assurer que le numéro à partir duquel ils appelaient utilisait toujours le même indicatif régional que les victimes qu'ils appelaient, donnant l'impression que leur numéro de téléphone était local et plus fiable.

Ces criminels utilisent également d'autres arguments, qu'il s'agisse de prétendre que votre garantie a expiré, de vous proposer des prêts commerciaux que vous pouvez obtenir gratuitement ou de réparer votre ordinateur infecté. Très souvent, ils essaient d'obtenir les informations relatives à votre carte de crédit ou vos mots de passe, de vous inciter à leur transférer de l'argent, voire de leur donner un accès à distance à votre ordinateur.

Ces escrocs créent souvent un énorme sentiment d'urgence ou vous promettent quelque chose de trop beau pour être vrai afin de vous piéger. Le criminel veut vous pousser à faire une erreur. Ils peuvent également avoir recueilli des informations antérieures sur vous, qu'ils utiliseront pour établir leur crédibilité.Plus récemment, grâce aux services d'intelligence artificielle, les escrocs peuvent même changer de voix lors des appels téléphoniques.

La contre-attaque : Ce que vous pouvez faire

Il existe plusieurs mesures que vous pouvez prendre immédiatement pour vous protéger :

- Configurez votre téléphone pour qu'il n'autorise que les appels provenant de numéros de confiance figurant dans le répertoire ou le carnet d'adresses de votre téléphone. Ainsi, tout appel provenant d'une personne que vous ne connaissez pas sera directement dirigé vers la messagerie vocale. La grande majorité des escrocs ne prendront même pas la peine de laisser un message vocal, et pour ceux qui le font, il est plus facile de déterminer s'il s'agit d'une escroquerie et de l'effacer. En outre, certains fournisseurs de services proposent également un service de filtrage des appels que vous pouvez activer.

- Si vous vous retrouvez au téléphone avec une personne que vous ne connaissez pas, soyez prudent. S'ils vous poussent à agir, il s'agit très probablement d'une escroquerie. Si on vous dit que c'est votre banque qui vous appelle, raccrochez et utilisez un numéro de téléphone de confiance pour rappeler votre banque, par exemple le numéro figurant sur votre compte bancaire. Si l'on vous dit que c'est le gouvernement qui vous appelle, rendez-vous sur le site web de l'administration concernée et trouvez un numéro de téléphone fiable à rappeler. Plus ils vous gardent au téléphone longtemps, plus ils ont de chances de vous piéger.

- Ne fournissez jamais à l'appelant des informations personnelles ou sensibles qu'il devrait déjà posséder. Si votre banque vous appelle, elle doit déjà connaître votre nom, votre adresse et votre numéro de compte.

Les escrocs modernes sont extrêmement agressifs. Ils n'ont rien à perdre et tout à gagner. Configurez votre téléphone pour ne recevoir que les appels des contacts que vous connaissez et en qui vous avez confiance, et en cas de doute, raccrochez !

Rédacteur Invité

Prajakta Jagdale est Senior. Directeur de la sécurité offensive et du commandement des incidents chez Palo Alto Networks. Elle est membre du conseil d'administration de Women in CyberSecurity. Elle est passionnée par tout ce qui touche à la sécurité, y compris la diversité de la main-d'œuvre. LinkedIn : https://www.linkedin.com/in/prajaktajagdale/.

Ressources

Les déclencheurs émotionnels - Comment les cybercriminels vous piègent :
https://www.sans.org/newsletters/ouch/emotional-triggers-how-cyber-attackers-trick-you/

N'autoriser que les appels provenant de vos contacts
Android : https://support.google.com/fi/answer/12982560?hl=en&co=GENIE.Platform%3DAndroid#
Apple : https://support.apple.com/guide/iphone/avoid-unwanted-calls-iphe4b3f7823/ios

Traduit pour la communauté par : Juliette Busson