www.darkreading.com /cyberattacks-data-breaches/dont-answer-phone-inside-real-life-vishing-attack

Ne répondez pas au téléphone car vous êtes au cœur d'une attaque d'hameçonnage vocal réelle

Les attaquants qui réussissent se concentrent sur la manipulation psychologique des émotions humaines, c'est pourquoi n'importe qui, même une personne férue de technologie, peut devenir une victime.

Elizabeth Montalbano, Contributing Writer :

Tout a commencé par un appel téléphonique vers 10h30 un mardi à partir d'un numéro de téléphone portable inconnu.
Je travaillais sur mon ordinateur à la maison et je ne réponds généralement pas aux appels téléphoniques de personnes que je ne connais pas.
Pour une raison quelconque, j'ai décidé d'arrêter ce que je faisais et de prendre cet appel.

C'était ma première erreur d'une série de plusieurs que j'allais commettre au cours des quatre heures suivantes, au cours desquelles j'ai été victime d'une campagne d'hameçonnage vocal.
À la fin de l'épreuve, j'avais transféré près de 5 000 € (EUR) de fonds de mon compte bancaire et en Bitcoin aux escrocs.

Ma banque a été en mesure d'annuler la plupart des virements ; cependant, j'ai perdu 1 000 € (EUR) que j'avais envoyés dans le portefeuille Bitcoin des attaquants.

Les experts dis-le peu importe l'expertise que vous avez dans la connaissance des tactiques utilisées par les attaquants ou dans l'expérience pour repérer les escroqueries. La clé du succès des attaquants est quelque chose de plus ancien que la technologie, car elle réside dans la manipulation de ce qui fait de nous des êtres humains : nos émotions.

« Parce que nous sommes tellement centrés sur la technologie, nous oublions qu'en fait, ces tactiques d'escroquerie sont anciennes, antérieures même aux escroqueries sur Internet, et qu'elles ont fait leurs preuves », explique Richard Werner, conseiller en cybersécurité chez Trend Micro.
« Ils travaillent avec les émotions.
Lorsqu'ils nous mettent de bonne humeur et déclenchent la colère ou la peur, nous oublions tous les conseils.
Dans ces cas-là, nous perdons le bon sens, et c'est là que [les attaquants] nous attrapent.

Par conséquent, même un expert en cybersécurité peut tomber dans le piège d'une escroquerie, comme l'a fait Werner lui-même, un vétéran de la cybersécurité informatique depuis 20 ans.
Un courriel d'hameçonnage contenant un message sur le thème de l'assistance Windows est arrivé dans son e-mail alors qu'il était aux prises avec le fait que le système d'exploitation ne fonctionnait pas correctement sur sa machine.
Heureusement, il s'agissait d'un exercice de formation à l'hameçonnage qui provenait d'une source interne de son entreprise, et non d'une source aux enjeux élevés.

Mais en tant que personne qui a écrit des exercices d'hameçonnage pour la formation des employés, Werner sait que tout le monde, du service informatique aux ressources humaines, a un déclencheur qui le rend vulnérable à une escroquerie dans les bonnes circonstances.

Signaux d'alarme

L'escroquerie qui m'a fait trébucher était l'une des configurations d'hameçonnage vocal courantes qui balayent actuellement le monde.
Même si les signaux d'alarme se déclenchaient partout, je suis quand même resté au téléphone avec les attaquants pendant plus de trois heures et je les ai laissés me manipuler.

« Lorsqu'il s'agit d'examiner les signes révélateurs que les gens sont arnaqués par un appel vocal, la principale question à se poser est de savoir s'il s'agit d'une méthode habituelle par laquelle ils seraient contactés, si la personne à l'autre bout du fil leur demande de faire quelque chose qui sort de l'ordinaire, y a-t-il un sentiment d'urgence et cela déclenche-t-il une forte réaction émotionnelle ? », explique Javvad Malik, principal défenseur de la sensibilisation à la sécurité au sein de la société de sécurité KnowBe4. « Si c'est le cas, il s'agit très probablement d'une arnaque. »

Mon escroquerie avait toutes ces caractéristiques dès le début.
Lorsque j'ai répondu à l'appel, un message automatisé m'a dit que ma carte d'identité nationale (je suis basée au Portugal) avait été utilisée dans le cadre d'activités criminelles et qu'il y avait un mandat d'arrêt contre moi.

Si je voulais plus d'informations, je devrais appuyer sur 1.
D'après Werner, cela aurait dû être mon premier signe de raccrocher.

« On ne peut pas faire confiance à tout ce qui a trait à la technologie », dit Malik. Dans ce cas, un message automatisé aurait dû m'avertir.
À la fois alarmé et curieux par la déclaration que je pourrais être arrêté de façon imminente, j'ai mordu à l'hameçon.

J'ai été transféré à un homme qui s'est présenté comme Marco José, un officier de la GNR (Garde républicaine nationale) portugaise à Lisbonne.
Il m'a donné ce qu'il prétendait être son numéro de badge et m'a ensuite dit que mon identité avait été utilisée dans le cadre du blanchiment d'argent et du trafic de drogue.
J'ai répondu consciencieusement à ses questions, donnant des informations sur moi-même parce que je pensais que je parlais à un officier de justice.

La mise en place

Marco a poursuivi en disant que la police a perquisitionné une maison à Lisbonne et a trouvé des documents liés à de nombreux comptes bancaires ouverts à mon nom.
Il a également déclaré que la police avait trouvé une voiture abandonnée qui avait été louée à mon nom et qui était liée à l'affaire, pour laquelle il a fourni un numéro de dossier.

Alors que j'écrivais ce qu'il disait, des questions fusaient dans mon esprit et des sonnettes d'alarme mentales se déclenchaient.
Même si je reconnaissais logiquement que son histoire était pleine de trous, mes émotions pilotaient l'avion à ce moment-là.

Le fait même que les forces de l'ordre m'aient approché par téléphone aurait dû me faire raccrocher. S'ils s'intéressaient vraiment à moi en tant que suspect, ils seraient venus me parler en personne, comme me l'a dit plus tard un ami et ancien officier de la GNR

En effet, si quelqu'un est contacté par quelqu'un qui prétend être un membre des forces de l'ordre, la meilleure chose à faire est de lui dire que vous rappellerez et raccrocherez. Recherchez ensuite les coordonnées de l'agence ; ne vous fiez pas au numéro fourni par l'appelant, conseille Werner.

Au lieu de cela, j'ai laissé Marco continuer à parler, trop vite pour que je puisse l'interrompre.
Il a dit que même s'il savait que j'étais innocent, aux yeux de la loi, j'étais impliqué dans l'activité criminelle parce que c'était mon nom et mon passeport qui étaient utilisés pour la mener.

Je pourrais laver mon nom en parlant à sa collègue des autorités internationales qui gèrent l'affaire et essaient d'attraper les criminels, mais seulement si j'aidais l'enquête de la manière dont elle me l'avait demandé et si j'avais suivi ses instructions à la lettre.
J'ai laissé Marco transférer l'appel à Dobra Volska, qui prétendait travailler pour la Cour internationale de Justice.

C’est là que j’ai fait un autre faux pas, car ce type de coercition aurait dû m’alerter que quelque chose n’allait pas.
Mais ma peur avait pris le dessus et j’ai paniqué à l’idée de perdre tous mes biens, même pour la modeste somme d’argent que j’avais sur mes deux comptes bancaires.
Alors j’ai continué.

Le plus proche

Marco s’est occupé de la mise en place, tandis que Dobra était le plus proche.

Le travail de Dobra consistait à souligner qu’en 45 minutes – elle a été très précise – les autorités saisiraient tous les comptes bancaires à mon nom qui étaient associés aux crimes présumés, mais que cette action affecterait également mes comptes légitimes. Pour sécuriser mes fonds « durement gagnés », elle m’a proposé de créer un « coffre-fort numérique sécurisé » pour tous mes actifs.
On m’a assuré que le gouvernement ne contrôlerait le coffre-fort que le temps nécessaire pour saisir les comptes, et que mon argent me serait rendu immédiatement après.

Au cours des heures qui ont suivi, j’ai fait tout ce que cette femme m’a dit de faire, y compris partager l’écran de mon ordinateur portable, effectuer des virements bancaires et télécharger diverses applications, y compris une application appelée MoonPay afin d’acheter des bitcoins.
J’ai transféré la crypto-monnaie dans un portefeuille contrôlé par les criminels.

Cette urgence est un autre indice que j’ai été victime d’une arnaque, comme le dit Malik de KnowBe4, mais j’étais trop frénétique pour le reconnaître.

« L’escroquerie est conclue en instillant un sentiment d’urgence », explique Malik.
« Cela oblige la victime à agir immédiatement et, ce faisant, peut créer un sentiment de vision étroite dont il devient de plus en plus difficile pour la victime de s’échapper. »

Cette vision étroite rend la victime incapable de se sortir de la situation, même si elle le veut désespérément, dit Werner.
Je n’arrêtais pas de demander à Dobra d’attendre, que j’avais besoin de réfléchir ; elle m’a répété que nous n’avions pas le temps, que nous devions agir maintenant et que mes comptes seraient saisis si je ne faisais pas ce qu’elle disait.

À deux reprises, j’ai demandé à ce qu’on me vérifie qu’elle était bien celle qu’elle prétendait être.
Les deux fois, elle m’a fait raccrocher et son « collègue » m’a appelé depuis le numéro réel de la Cour internationale de justice de La Haye – il est clair que le numéro de téléphone avait été usurpé.
Alors que je persistais à poser des questions et à prendre le temps de réfléchir, la voix de Dobra a commencé à devenir plus forte et plus insistante.
À un moment donné, elle s’est lancée dans une tirade de menaces contre moi qui était si véhémente que j’ai fondu en larmes.

« Si la personne au téléphone ne comprend pas que vous avez besoin de temps pour vérifier qui elle est ou y réfléchir, c’est un signal d’alarme », prévient Werner.

« Toute personne bien intentionnée vous dira : « Prenez votre temps, allez au poste de police le plus proche, appelez votre banque » et vous donnera du temps avant de prendre d'autres mesures.

Isolez la victime

Dobra m'a également averti de ne dire à personne – pas même à mes amis ou à mes proches – ce qui se passait, car cela pourrait les impliquer d'une manière ou d'une autre dans les crimes que j'étais censé avoir commis.
Pire encore, ils pourraient être impliqués dans l'escroquerie.

J'ai envoyé un texto à mon petit ami de longue date pendant cette épreuve, mais je n'ai donné aucun détail.
J'ai juste dit que j'avais été victime d'un vol d'identité et que cela tournait au cauchemar. Quand Dobra m'a averti de ne parler à personne, j'ai arrêté de lui envoyer des messages. Il a noté plus tard que si je lui avais dit ce qui se passait, il m'aurait dit de raccrocher immédiatement.

Si j'avais suivi mon instinct et continué à parler avec mon petit ami, j'aurais peut-être échappé à l'escroquerie sans perdre d'argent, dit Werner.

« Au milieu d'une attaque, il s'agit vraiment de se sortir immédiatement de la situation », dit-il.
« Quoi que vous disiez, ils auront une réponse.
Donc, si vous le pouvez, vous devriez mettre fin à la situation, vous en sortir et essayer d'impliquer quelqu'un en qui vous avez confiance.

Pas de honte à se faire jouer

De nombreuses parties de mon histoire sont similaires à l'épreuve d'hameçonnage vocal de plusieurs heures qui a récemment pris au piège la journaliste du New York Times Charlotte Cowles, où elle a fini par placer 50 000 $ en espèces sur la banquette arrière d'une Mercedes conduite par l'un des criminels.

Elle écrit sur la honte déchirante qu'elle a ressentie plus tard pour avoir été trompée, quelque chose que j'ai également vécu dans les jours qui ont suivi l'arnaque.
J'ai passé quelques jours à m'en vouloir d'avoir fait quelque chose d'aussi stupide alors que j'aurais dû être mieux informé.
Après avoir partagé mon histoire avec des amis et des connaissances, je sais maintenant qu'il y a beaucoup de victimes.

Werner avait des mots de réconfort pour tous ceux qui sont tombés dans le piège d'un hameçonnage vocal ou d'un autre type d'escroquerie cybercriminelle.

« N'ayez pas honte de ce qui s'est passé », dit-il.
« Ces [cybercriminels] sont très organisés.
Ils savent exactement comment vous agiriez de l'autre côté et comment vous agiriez pour vous sortir de la situation.

Le principal conseil pour quiconque, des professionnels de la cybersécurité aux personnes qui n'ont jamais entendu parler de l'hameçonnage vocal, est d'essayer d'éviter de s'engager dès le départ, afin que les jeux

psychologiques auxquels se livrent les escrocs ne puissent pas être utilisés contre vous, selon les experts.
Si quelqu'un reçoit un appel qui semble suspect ou même déroutant, posez d'abord quelques questions avant de répondre ou de croire l'histoire de la personne qui appelle.

Former les gens à repérer tous les signaux d'alarme que j'ai ignorés peut les aider à éviter de tomber dans la compromission, tout comme leur conseiller de contacter immédiatement un membre d'une équipe de sécurité d'entreprise s'ils reçoivent un appel téléphonique suspect ou rencontrent une activité en ligne inattendue.

« Il est important que les employés disposent de méthodes simples et fiables pour signaler tout appel téléphonique suspect ou toute autre activité afin que les équipes de sécurité puissent intervenir en cas de besoin », explique M. Malik.

Recherche et mise en page par:
Michel Cloutier
CIVBDL
20240321
"C'est ensemble qu'on avance"