Mantra teste la vigilance des salariés et les forme à repérer les tentatives de phishing

Créée l'année dernière, Mantra vient d'obtenir la confiance de OneRagTime, Axeleo et Bpifrance Digital Ventures qui ont investi 1,6 million d'euros dans la pépite de la cybersécurité.

Temps de lecture : minute

5 juillet 2021

Regarder avant de traverser. Ne pas monter dans la voiture d'un inconnu. Ne pas ouvrir une pièce jointe dont on n'est pas certain·e de la provenance. La cybersécurité est une affaire de réflexe, comme la sécurité du quotidien. Mais combien se sont déjà fait avoir ? Trop. Dont Gaspard Droz, qui travaillait alors en cabinet de conseil en stratégie. "*Nous avions eu une sensibilisation aux sujets de cybersécurité*, se rappelle l'entrepreneur. *Ça ne m'a pas empêché de me faire fisher... Les escrocs se sont fait passer pour l'équipe IT et m'ont demandé de changer mon mot de passe pour le récupérer* " . Un peu honteux en découvrant la supercherie, le jeune homme s'aperçoit pourtant qu'il est "l*oin d'être un cas isolé*" . Selon le rapport Internet Crime Report, rédigé par le FBI sur la cybercriminalité, le phishing est le type de fraude qui a fait le plus de victimes en 2020 : pas moins de 241 000 dans le monde.

Et pas question de croire que les victimes ne sont que des boomers ou des simples d'esprit peu rompus aux usages d'un Internet qu'ils ne comprennent pas - le cas de Gaspard Droz, diplômé d'HEC et fringant trentenaire, en témoigne. "*Les hackers sont assez doués pour faire intervenir des éléments psychologiques dans leurs mails, comme des arguments d'autorité en se faisant passer pour un supérieur hiérarchique*

ou un expert, par exemple, note le jeune homme. *Cela vient brouiller le jugement de la victime potentielle qui est prise par surprise face à des attaques de plus en plus ciblées et contextualisées.*"

Ces dernières années, les entreprises se sont dotées d'outils de plus en plus puissants pour armer leurs systèmes de défense. Mais la faille humaine reste critique. Et c'est là que Mantra, la solution imaginée par Gaspard Droz, avec Guillaume Charhon, intervient. "*Il faut entraîner les gens en conditions réelles, leur envoyer de faux emails de phishing pour les habituer à être vigilants*" , expose le co-fondateur de la startup, qui vient de lever 1,6 million d'euros auprès de OneRagTime, qui a leadé le tour, Bpifrance Digital Ventures et Axeleo.

Acquérir des réflexes

Pour acquérir ces nouveaux réflexes de cybervigilance, il faut compter plusieurs mois, puis une formation continue pour se tenir à jour des dernières techniques de fishing ; mais cela requiert aussi que les messages envoyés soient suffisamment crédibles pour risquer de ne pas être repérés par les victimes potentielles. C'est pourquoi Mantra a imaginé une solution permettant d'automatiser l'envoi de fausses campagnes de phishing au sein d'entreprises clientes. "*On commence par scanner le contexte de la société : qui sont les personnes-clés, les outils utilisés, dans quel département travaillent les salariés à former… Cela permet d'envoyer de faux mails très ciblés.*"

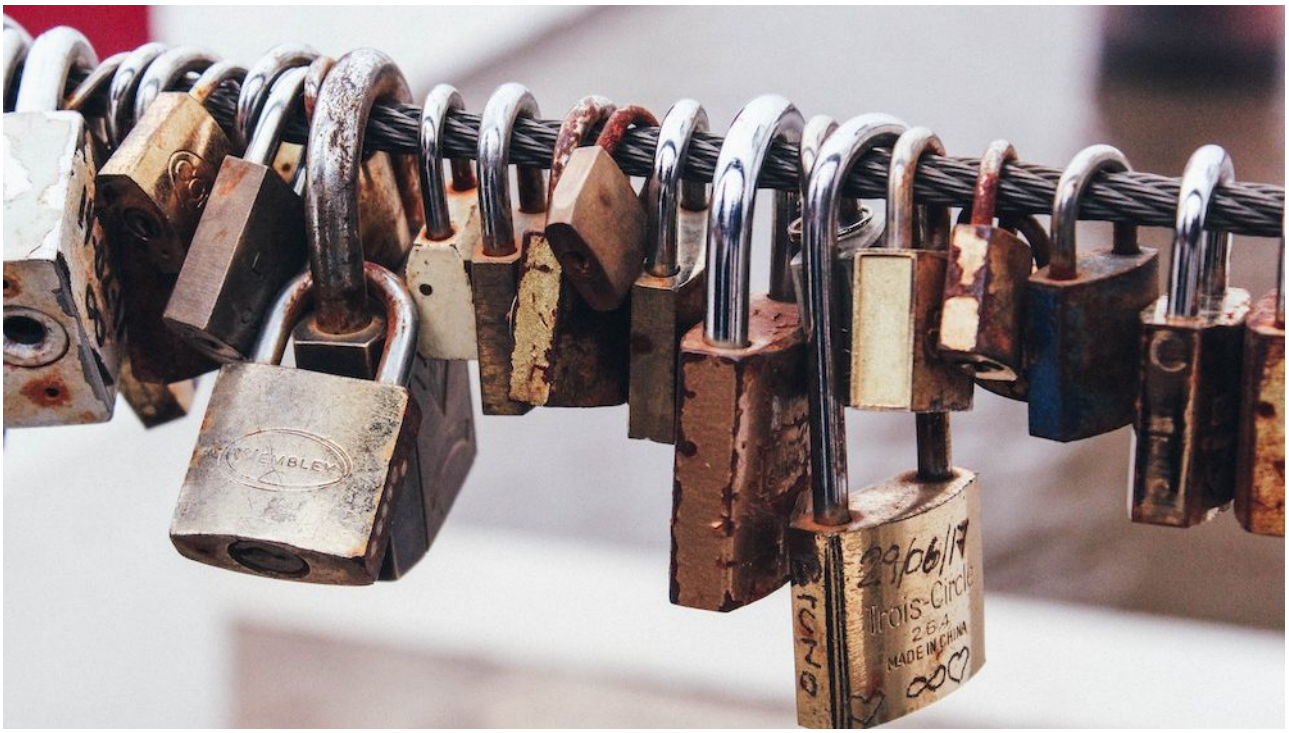
À lire aussi
Toujours plus nombreuses, les startups de la cybersécurité peinent à croître

Plus de 500 scénarios ont été imaginés à partir de quatre ou cinq grands types de fraudes : qu'il s'agisse d'un mail de redirection vers une page où il faut renseigner des informations sensibles ou de l'ouverture d'une pièce jointe qui permettrait aux hackers d'installer des rançongiciels, tous les cas d'école sont couverts avec une approche particulièrement réaliste. Pour limiter les crises de panique, à la fin de la simulation, le ou la salarié·e est prévenu·e qu'il s'agissait d'un test et est redirigé·e vers une page listant tous les détails qui auraient pu l'alerter.

Et afin de rendre la traque de ces faux mails ludique, la startup a créé un système de gamification associé : grâce à un module intégré au système de messagerie du client, les salarié·e·s ont la possibilité de signaler les mails potentiellement dangereux - et débusquer ainsi les fausses tentatives de fishing ; ce qui leur permet de gagner des points et d'acquérir sans en avoir l'air le réflexe de signaler ce qui leur permet louche.

Cibler les entreprises de taille intermédiaire

Créée l'année dernière, Mantra travaille déjà avec plusieurs scaleups comme Aircall ou Dataiku, avec lesquelles elle a signé des contrats longs. "*Nous avons une approche de long terme : les types d'attaques changent et il est donc indispensable de continuer à éduquer les salariés. Si on arrête les simulations, l'attention se réduit fortement*" , prévient Gaspard Droz. Les hackers le savent et, après s'être longtemps concentrés sur les grands groupes, ciblent aujourd'hui davantage les entreprises de taille intermédiaire (ETI), moins bien armées face aux attaques. C'est pour cela que Mantra a décidé de se concentrer aujourd'hui sur ce marché.



À lire aussi
Comment identifier vos besoins en cybersécurité ?

La levée de fonds récemment conclue doit d'ailleurs permettre à la toute fraîche startup de saisir cette "*opportunité de marché*" . Mais aussi de développer de nouveaux produits, complémentaires à la solution aujourd'hui commercialisée par Mantra, pour parfaire l'éducation des

salarié·e·s en matière de cybersécurité. "*La simulation, c'est une chose mais notre roadmap va bien au-delà*" , lance malicieusement Gaspard Droz.

Avec un coût pour les victimes estimé l'an dernier à plus de 54 millions de dollars, le phishing est un marché lucratif pour les escrocs... mais aussi pour les entreprises de la cybersécurité !

Article écrit par Geraldine Russell