OUCH! Octobre 2022

Votre bulletin mensuel sur la sensibilisation à la sécurité

Déclencheurs émotionnels - comment les cyber-attaquants vous piègent-ils ?

Aperçu

Les cyber-attaquants innovent constamment pour nous inciter à faire des choses que nous ne devrions pas faire, comme cliquer sur des liens malveillants, ouvrir des pièces jointes d'e-mails infectés, acheter des cartes-cadeaux ou donner nos mots de passe. En outre, ils utilisent souvent différentes technologies ou plateformes pour tenter de nous tromper, comme l'e-mail électronique, les appels téléphoniques, les messages texte ou les réseaux sociaux. Si tout cela peut sembler accablant, la plupart de ces attaques ont un point commun : l'émotion. En connaissant les déclencheurs émotionnels utilisés par les cyber-criminels, vous pouvez souvent repérer leurs attaques, quelle que soit la méthode qu'ils utilisent.

Tout est une question d'émotions

Tout commence par les émotions. En tant qu'êtres humains, nous prenons bien trop souvent des décisions fondées sur des émotions plutôt que sur des faits. Il existe en fait tout un champ d'études sur ce concept appelé « économie comportementale », dirigé par des chercheurs tels que Daniel Khaneman, Richard Thaler et Cass Sunstein. Heureusement pour nous, si nous savons quels sont les déclencheurs émotionnels à rechercher, nous pouvons repérer et arrêter la plupart des attaques. Vous trouverez ci-dessous une liste des déclencheurs émotionnels les plus courants à surveiller. Parfois, les cyber-attaquants utilisent une combinaison de ces différentes émotions dans un même e-mail, message texte, message sur les réseaux sociaux ou appel téléphonique, ce qui les rend d'autant plus efficaces.

L'urgence : l'urgence est l'un des déclencheurs émotionnels les plus courants, car il est très efficace. Les cyber-criminels utilisent souvent la peur, l'anxiété, la pénurie ou l'intimidation pour vous pousser à commettre une erreur. Prenez, par exemple, un e-mail urgent de votre patron vous demandant que des documents sensibles lui soient envoyés immédiatement, alors qu'il s'agit en réalité d'un cyber-attaquant se faisant passer pour votre patron. Ou peut-être recevez-vous un message texte d'un cyber-attaquant se faisant passer pour le gouvernement, vous informant que vos impôts sont en retard et que vous devez payer immédiatement ou vous irez en prison.

La colère : vous recevez un message sur une question politique, environnementale ou sociale qui vous passionne - comme : « vous n'allez pas croire ce qu'a fait ce groupe politique ou cette entreprise ! »

La surprise / **La curiosité** : Parfois, les attaques qui ont le plus de succès sont celles qui en disent le moins. La curiosité est suscitée par la surprise ; nous voulons en savoir plus. C'est une réponse à quelque chose d'inattendu. Par exemple, un cyber-attaquant vous envoie un message vous indiquant qu'un colis n'a pas été livré et vous invitant à cliquer sur un lien pour en savoir plus, alors que vous n'avez rien commandé en ligne. Nous sommes impatients d'en savoir plus ! Malheureusement, il n'y a pas de colis, juste des intentions malveillantes si vous cliquez sur ce lien.

La confiance : les attaquants utilisent un nom ou une marque auxquels vous faites confiance pour vous convaincre d'entreprendre une action. Par exemple, un message prétendant provenir de votre banque, d'une organisation caritative connue, d'une organisation gouvernementale de confiance ou même d'une personne que vous connaissez. Ce n'est pas parce qu'un e-mail ou un message texte utilise le nom d'une organisation que vous connaissez et son logo que le message provient réellement d'elle.

L'excitation : vous recevez un SMS de votre banque ou de votre prestataire de services vous remerciant d'avoir effectué vos paiements à temps. Le message fournit ensuite un lien qui vous permet de réclamer une récompense - un nouvel iPad, comme c'est excitant ! Le lien vous conduit à un site web qui semble officiel, mais qui vous demande toutes vos informations personnelles ou vous demande de fournir des informations sur votre carte de crédit pour couvrir les petits frais d'expédition et de manutention. Il s'agit d'un cyber-attaquant qui ne fait que voler votre argent ou votre identité.

L'empathie / La compassion : Les cyber-attaquants profitent de votre bonne volonté. Par exemple, après qu'une catastrophe a fait la une des journaux, ils envoient des millions de faux e-mails en prétendant être une organisation caritative au service des victimes et en vous demandant de l'argent.

En comprenant mieux ces déclencheurs émotionnels, vous serez bien mieux préparé à repérer et à arrêter les cyber-attaquants, quels que soient le leurre, la technologie ou la plate-forme qu'ils utilisent.

Rédacteur Invité

My-Ngoc Nguyen est le PDG/principal de Secured IT Solutions. Forte de 20 ans d'expérience, elle possède une grande expérience de la gestion et de la maturation des programmes de cybersécurité et de gestion des risques, tant pour le gouvernement fédéral que pour le secteur privé. Elle apporte cette expérience en tant qu'instructeur certifié enseignant régulièrement le MGT512. https://www.linkedin.com/in/menop , My-Ngoc Nguyen | SANS Institute, @ MenopN.

Ressources

Ingénierie sociale: https://www.sans.org/newsletters/ouch/social-engineering-attacks/
Hameçonnage vocal - Attaques ou arnaques téléphoniques: https://www.sans.org/newsletters/ouch/vishing/
Les trois principales arnaques sur les réseaux sociaux: https://www.sans.org/newsletters/ouch/top-three-social-media-scams/
Attaques de messagerie / Smishing: https://www.sans.org/security-awareness-training/resources/messaging-smishing-attacks
Les attaques par hameçonnage deviennent de plus en plus travaillées: https://www.sans.org/newsletters/ouch/phishing-attacks-getting-trickier/

Traduit pour la communauté par : Juliette Busson