L’hameçonnage : Ne soyez pas la prise du jour

Bienvenue à la deuxième semaine du Mois de la sensibilisation à la Cyber Sécurité! Cette semaine, nous nous penchons sur la fraude psychologique et sur la manière dont elle peut donner lieu à des attaques de type hameçonnage, hameçonnage par SMS et hameçonnage par téléphone. Si vous vous souvenez de l’article de la semaine dernière, nous avons parlé de la façon dont les médias sociaux peuvent fournir des renseignements que quelqu’un peut utiliser dans une attaque de fraude psychologique contre vous ou votre organisme. Mais qu’est-ce que cela signifie? Et à quoi ressemblerait une attaque?

Rappel : Fraude psychologique

La fraude psychologique consiste à utiliser la tromperie pour exploiter la nature humaine, nos habitudes et notre confiance afin d’obtenir des renseignements ou d’accéder à des systèmes d’information. Les auteurs de menaces veulent obtenir des renseignements confidentiels tels que des mots de passe et des identifiants de connexion, ou des renseignements personnels.

Par ici l’hameçonnage!

L’hameçonnage est la forme la plus courante d’attaque par fraude psychologique. Il se produit lorsqu’un auteur de menaces se fait passer pour une entité de confiance par l’entremise d’un courriel pour tenter d’obtenir frauduleusement des renseignements ou l’accès à des systèmes. Être pris dans un hameçonnage peut signifier cliquer sur un lien, fournir des renseignements, ouvrir une pièce jointe, télécharger un fichier ou donner un accès à distance à un poste de travail.

Repousser l’hameçonnage

Il est important de savoir ce qu’il faut rechercher pour détecter une attaque d’hameçonnage. Voici ce qu’il faut rechercher :

- Provient d’un utilisateur, d’un organisme ou d’un nom de domaine inconnu, c’est-à-dire le nom unique qui apparaît après le signe @ dans une adresse courriel.
- Provient d’une personne de l’organisme, mais avec un nom de domaine non organisationnel.
- Exprime un niveau inhabituel d’urgence.
- Contient des erreurs telles que des noms mal orthographiés, des termes organisationnels mal utilisés ou des logos mal représentés.
- Contient des pièces jointes avec des noms de fichiers ou des liens inhabituels.
- Animé par une motivation telle qu’un avantage financier ou un autre avantage.

La prise du jour par SMS

L’hameçonnage par SMS est une forme d’hameçonnage qui utilise des messages texte au lieu de courriels. Les messages de ce type d’hameçonnage peuvent arriver par SMS

(service de messages courts) comme iMessage, Facebook Messenger, WhatsApp et d'autres plateformes de messagerie.

Pas d'hameçonnage SMS pour moi, merci!

- Ne répondez pas au message texte, n'appelez pas le numéro et ne cliquez pas sur les liens contenus dans le message.
- Recherchez le numéro de téléphone et le message pour voir si d'autres personnes ont reçu des messages similaires.
- Communiquez avec l'organisme ou la personne directement – demandez si le message que vous avez reçu est légitime.

Pris dans le filet de l'hameçonnage par téléphone

L'hameçonnage par téléphone est une forme d'hameçonnage qui utilise les appels téléphoniques au lieu de courriels. Il est également appelé vishing. Il se produit lorsqu'un auteur de menaces se fait passer pour une entité de confiance par téléphone afin d'obtenir frauduleusement des renseignements sensibles ou l'accès à des systèmes. Les auteurs de menaces déguisent leurs numéros de téléphone pour faire croire qu'ils appellent d'un établissement légitime.

Ne vous faites pas hameçonner par téléphone

- Méfiez-vous des appels téléphoniques non sollicités d'établissements ou de personnes vous demandant des renseignements sensibles.
- Vérifiez les appels téléphoniques suspects en raccrochant et en rappelant l'établissement par le numéro publié de son service clientèle ou rappelez la personne avec un numéro de téléphone vérifié.
- Ne donnez jamais votre numéro d'assurance sociale, votre mot de passe ou votre NIP par téléphone et ne faites jamais d'opérations sur votre ordinateur si on vous le demande par téléphone.

Tendances récentes en matière d'hameçonnage

Saviez-vous qu'au cours de la même période de six mois, au début de la pandémie de COVID-19, 34 % des Canadiens ont subi une attaque d'hameçonnage? Dans le même temps, 14 % des personnes interrogées ont reçu des courriels d'hameçonnage en rapport avec la COVID-19. Il est important de réfléchir à la façon dont l'actualité peut nous attirer dans une attaque d'hameçonnage!

Pour plus d'informations, consultez ces Ressources sur l'Ingénierie Sociale.