Cyberrisques

Hameçonnage

L'hameçonnage désigne la « pratique frauduleuse qui consiste à envoyer des courriels censés provenir d'entreprises réputées afin d'inciter les gens à révéler des renseignements personnels, notamment des mots de passe, des informations financières et des numéros de cartes de crédit ».[1]

Par exemple, une personne pourrait recevoir de sa banque un courriel l'informant d'un problème urgent concernant son compte et la priant de cliquer sur un lien qui la redirigera vers un site Web externe où elle sera priée de fournir des renseignements personnels dans le but de régler le problème. Bien que le site Web puisse paraître authentique, la saisie de données personnelles comme il est demandé risque d'entraîner un vol d'identité et une fraude de crédit. D'autres modes d'hameçonnage sont utilisés à part le courriel.

Types courants d'hameçonnage[2]

- **Hameçonnage par courriel :** Courriel générique qui demande aux utilisateurs de cliquer sur un lien ou d'ouvrir et de télécharger une pièce jointe en raison d'une urgence.
- **Hameçonnage ciblé :** Analogue à l'hameçonnage par courriel, sauf que ce genre de courriel s'adresse à des personnes bien ciblées, utilisant des noms, des titres de poste et des adresses de courriel exacts.
- **Harponnage de cadre supérieur :** Courriel ciblant des cadres supérieurs et comportant des messages plus subtils.
- **Hameçonnage par message texte et hameçonnage vocal :** Utilisation de messages textes ou de conversations téléphoniques directes pour demander des renseignements personnels afin de régler une situation urgente.
- **Hameçonnage à la ligne :** Communication avec des personnes au moyen d'un média social pour les inciter à cliquer sur un lien ou à télécharger un logiciel malveillant.

L'hameçonnage peut également causer des dommages aux réseaux et systèmes. Par exemple, un courriel offrant l'installation gratuite d'un économiseur d'écran peut installer en même temps un logiciel malveillant, soit un logiciel conçu pour « perturber ou endommager un système informatique ou obtenir un accès non autorisé à celui-ci »,[3] lequel pourrait suivre les déplacements de l'utilisateur sur le Web, voler ses mots de passe et numéros de cartes de crédit et obtenir des données privées sur lui.

Comment éviter les arnaques par hameçonnage[4]

- Ne cliquez jamais sur un lien et ne fournissez jamais des renseignements personnels en réponse à un courriel ou un appel téléphonique demandant des renseignements. Communiquez directement avec l'entreprise au moyen du numéro de téléphone affiché sur son site Web et utilisez le site Web officiel de l'entreprise pour ouvrir les pages d'ouverture de session.
- Ne répondez jamais à un courriel, même pour vous désabonner ou pour décliner une offre, si vous avez des doutes au sujet de l'expéditeur. En répondant, vous confirmerez à l'expéditeur qu'il a joint un compte de courriel actif.

- •N'ouvrez jamais une pièce jointe à un courriel si vous avez des doutes au sujet de l'expéditeur. Il est facile de transférer un logiciel malveillant au moyen de fichiers joints à un courriel.
- Ne divulguez jamais un mot de passe. Le personnel de la technologie de l'information ne demande jamais un mot de passe.
- Installez un antivirus, un logiciel anti espion et un logiciel de sécurité réputés et mettez-les à jour régulièrement.

Outre le logiciel de sécurité, il est recommandé aux sociétés d'offrir aux employés une formation périodique sur l'hameçonnage. Les employés avisés sont mieux aptes à reconnaître et à éviter les tentatives d'attaques par hameçonnage.

Pour de plus amples renseignements, prière de parcourir le site cnacanada.ca.

1 Lexico (2019) (En anglais seulement) Tiré de https://www.lexico.com/en/definition/phishing
2 IT Governance (2019) (En anglais seulement) Tiré de https://www.itgovernance.eu/blog/en/the-5-most-common-types-of-phishing-attack
3 Lexico (2019) (En anglais seulement) Tiré de https://www.lexico.com/en/definition/malware
4 Digital Guardian (2019) (En anglais seulement) Tiré de https://digitalguardian.com/blog/phishing-attack-prevention-how-identify-avoid-phishing-scams