Mois de la prévention de la fraude

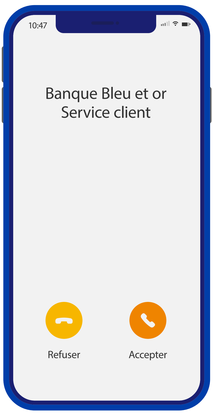
Repérer la fraude par hameçonnage : À savoir

Les cybercriminels comptent sur nous pour être distraits et baisser notre garde. Et lorsque cela se produit, ils peuvent nous piéger afin que nous leur communiquions nos renseignements personnels ou financiers en utilisant l'une de leurs tactiques favorites : l'hameçonnage.

Vous connaissez peut-être l'hameçonnage par courriel, mais ce n'est pas le seul type d'hameçonnage auquel vous pouvez être confronté. Les criminels utilisent également des sites Web, des SMS et des appels téléphoniques pour déployer leur arnaque d'hameçonnage.

Vous trouverez ci-dessous quelques formes courantes d'hameçonnage auxquelles vous pourriez être confronté et les signes avant-coureurs à surveiller.

Hameçonnage téléphonique



Les escrocs peuvent se faire passer pour un représentant d'une institution financière ou d'une carte de crédit afin de tromper les consommateurs en leur demandant de fournir leur numéro de compte, la date d'expiration, le code de sécurité à trois chiffres figurant au dos de leur carte de crédit ou d'autres renseignements sensibles.

Comment reconnaître l'hameçonnage téléphonique

1. Un appel téléphonique de « votre société de carte de crédit » ou de votre « institution financière », généralement de quelqu'un qui travaille au « service de la sécurité et de la fraude »
2. On vous dit que des transactions suspectes ont été signalées sur votre carte et que vous devez prouver que vous avez la carte en votre possession
3. Enfin, on vous demande de confirmer votre numéro de compte, la date d'expiration ou le code de sécurité à trois chiffres, un code d'accès unique qui vient de vous être envoyé, ou votre NIP

Hameçonnage par courriel

En général, vous recevez un courriel d'une société de confiance (telle que votre banque), vous demandant de cliquer sur un lien. Une fois que vous avez cliqué sur le lien, vous êtes dirigé vers un site qui semble identique au site que vous connaissez à partir duquel vous êtes susceptible de télécharger des logiciels malveillants sur votre ordinateur, tablette ou appareil mobile. Mais dans ce cas, il s'agit d'un site d'hameçonnage qui peut capturer vos identifiants et les utiliser pour éventuellement vider votre compte ou pour d'autres activités malveillantes.

Comment reconnaître un courriel d'hameçonnage

- L'adresse électronique ne correspond pas à la société
- Le courriel contient des erreurs de formatage, d'orthographe et de grammaire dans l'objet ou dans le corps du courriel
- Échéancier. Les escrocs peuvent imposer un échéancier et menacer de suspendre le compte pour ajouter un caractère d'urgence et tenter de déjouer votre prudence habituelle
- Hyperliens suspects. Évitez si possible de cliquer sur les hyperliens. Un simple clic peut provoquer l'infection de votre ordinateur par un logiciel malveillant
- Absence de coordonnées. Si quelque chose vous semble suspect, veuillez communiquer directement avec votre institution financière en utilisant le numéro de téléphone figurant au dos de votre carte
- Le courriel contient des demandes suspectes. Les institutions financières ne contactent pas les titulaires de cartes pour leur demander des renseignements sur leur compte. Toutefois, si un titulaire de carte communique avec une institution financière, on lui posera une série de questions personnelles pour valider son identi
- Le courriel ne s'adresse pas à vous en utilisant votre nom

Hameçonnage sous forme de message texte

Comme de plus en plus d'entreprises utilisent les SMS pour communiquer avec leurs clients, il est parfois un peu difficile de déterminer ce qui est légitime et ce qui est une fraude.

Comment reconnaître l'hameçonnage sous forme de message texte

- Le message contient un lien plutôt qu'un numéro de téléphone à appeler.
- Le texte que vous recevez ne contient pas le nom de la banque ni aucune autre information.
- Le texte vous demande de vous connecter à votre compte bancaire pour vérifier une transaction, de saisir votre NIP ou de fournir votre code de sécurité à trois chiffres.

Hameçonnagepar site Web

Les escrocs s'améliorent dans la conception de sites Web qui semblent légitimes. Et parfois, vous pouvez cliquer sur un lien provenant d'une recherche ou d'un courriel qui semble sûr, mais qui vous dirige plutôt vers un faux site géré par un escroc.

Comment reconnaître l'hameçonnage par site Web

- Vous remarquez quelque chose qui cloche avec l'adresse Internet ou la page elle-même. Recherchez les mots mal orthographiés, les substitutions ou les logos datés
- Sur le site, une fenêtre contextuelle inhabituelle vous demande de saisir les renseignements relatifs à votre compte
- Le site contient des liens HTML qui ne correspondent pas à leur destination

Avez-vous été victime d'une fraude par hameçonnage?

Si vous êtes victime d'une fraude par hameçonnage de quelque nature que ce soit qui utilise le nom de Visa, veuillez nous le faire savoir en communiquant avec nous à **phishing@visa.com.** Nous vous sommes reconnaissants de votre contribution et bien que nous ne puissions pas répondre à chaque courriel, nous enquêtons de manière approfondie sur chaque demande pour aider à mettre fin à la fraude à la source.

Pour plus de renseignements sur l'hameçonnage et d'autres fraudes informatiques, visitez le site Web Pensez cybersécurité du gouvernement du Canada à l'adresse **https://www.pensezcybersecurite.gc.ca/index-fr.aspx**