Phishing / Hameçonnage

On vous incite à communiquer des informations sensibles ? Ne tombez pas dans le piège.

QUE SE PASSE-T-IL ?

1. Vous recevez un courriel piégé

Le courriel suspect vous invite à :
- cliquer sur une pièce-jointe ou un lien piégé ;
- communiquer des informations sensibles.

2. L'attaquant se fait passer pour un tiers de confiance

L'attaquant est alors en mesure :
- de prendre le contrôle de votre système ;
- de faire usage de vos informations.

LES 7 BONNES PRATIQUES

Conseil n°1 : Ne communiquez jamais d'informations sensibles par mail.
Aucune administration, société commerciale sérieuse, ne vous demandera vos données bancaires ou vos mots de passe par message électronique ou par téléphone. Ne communiquez pas d'information sensibles par ces canaux.

Conseil n°2 : Soyez extrêmement vigilant vis à vis des mails provenant d'internet.
L'ensemble des messages provenant d'internet ont pour objet *[Internet]* sur votre messagerie interpersonnelle ou sont reçus dans le répertoire *non-officiel* de votre messagerie organique, et doivent donc être considérés avec méfiance.

Conseil n°3 : Ne faîtes pas confiance au nom affiché dans le champ expéditeur.
La tactique de phishing préférée des cybercriminels consiste à usurper le nom indiqué dans le message électronique. Le nom de l'expéditeur est alors celui choisi par l'attaquant ("Gendarmerie Nationale" par exemple), cependant l'expéditeur réel peut-être n'importe quelle adresse mail (type gmail, outlook, etc.).

Conseil n°4 : Regarder les liens mais ne cliquez pas !
Les cybercriminels adorent intégrer des liens malveillants dans les messages en apparence légitimes. Lorsque de tels liens sont présents dans le corps du message, survolez-les avec votre souris pour voir où ils mènent, mais ne cliquez pas !

Conseil n°5 : Prenez garde aux menaces exagérées
Les attaquants vont tenter d'exercer une pression psychologique afin de vous faire céder (tel que la suppression de vos accès) et de vous inciter à transmettre des informations sensibles.

Conseil n°6 : Ne cliquez pas sur les pièces jointes des expéditeurs inconnus.
Joindre des documents contenant des virus et des logiciels malveillants est une tactique de phishing courante. Ces logiciels malveillants peuvent endommager votre ordinateur, voler vos mots de passe ou encore vous espionner à votre insu.

Conseil n°7 : Un doute ? Cherchez les fautes d'orthographe.
Les entreprises et institutions sont consciencieuses dans leurs communications. Généralement, les messages légitimes ne contiennent donc pas de fautes graves d'orthographe ou de grammaire.

COMMENT RÉAGIR ?

Il vous reste des doutes malgré tout ?

- **Interrogez** vos collègues afin d'avoir leur avis ;
- **Contacter** la société, l'interlocuteur concerné pour confirmer le message ou l'appel reçu ;
- **Demander conseil** à votre SOLC.

Que faire ?
- **Prévenir** vos collègues du phishing afin qu'ils n'en soient pas victime
- **Ne transférez pas : Transmettez** le mail suspect en tant que pièce jointe à l'adresse : signal-spam@gendarmerie.interieur.gouv.fr

Fiche de sensibilisation élaborée à partir de conseils SSI provenant de ProofPoint, de l'ANSSI, CyberMalveillance.gouv.fr ainsi que de la CNIL.