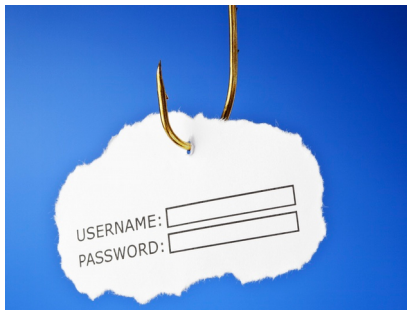
Région de gendarmerie Nouvelle-Aquitaine
Antenne Sécurité Économique et Protection des Entreprises de la formation administrative de Poitou-Charentes
Groupement de gendarmerie départementale de la Vienne.

PHISHING

PHISHING (hameçonnage - filouterie) : C'est une technique frauduleuse permettant de voler des informations numériques.

DE QUOI PARLE T-ON ?



C'est une attaque basée sur l'ingénierie sociale (faille humaine) qui consiste à duper la victime par l'intermédiaire d'un courrier électronique.
Ce courrier ressemble à s'y méprendre à celui d'une véritable société (commerce en ligne, banque, etc.)
Par le biais d'un formulaire factice, les pirates obtiennent des informations personnelles telles que numéro de compte bancaire, numéro client, code confidentiel, mot de passe.
Après avoir récupéré ces informations, les pirates réalisent des transactions financières frauduleuses et revendent parfois ces informations volées.

Explications :

L'attaque nommée Phishing est organisée à grande échelle. En effet la technique déployée est réalisée à l'aide de courriels envoyés massivement sur des boites aux lettres collectées au hasard. Des pièces jointes (page web factice) sont ajoutées à ces envois et précisent aux destinataires qu'il est nécessaire de cliquer sur les liens hypertextes en prétextant soit une intervention technique, soit une mise à jour sur le site visité (banque, compte en ligne etc.).
Ainsi, si le destinataire rentre son login et son mot de passe pour valider le message reçu, ses identifiants seront interceptés par le pirate qui n'aura plus qu'à rentrer sur le site officiel (banque, compte en ligne, etc.) et procéder à des achats ou des virements. Le pirate peut également revendre ces informations.
Malheureusement la confection d'un site factice, quasiment identique au vrai site, est de plus en plus facile à réaliser.
Une vigilance accrue est nécessaire lors de la réception de ce type de courriels.

Précautions :

Les quelques conseils ci-dessous vous permettront de limiter grandement le risque de phishing :
- Ne jamais cliquer sur un lien contenu dans un mail émis par une société, principalement, bancaire vous demandant de confirmer vos identifiants. Prendre attache avec la banque pour confirmer leur envoi de mail ;
- Il est préférable de saisir vous même l'URL pour accéder au service ;
- Si vous devez vous connecter sur des sites bancaires ou des sites d'achat en ligne, votre navigateur devra comporter le mode sécurisé (adresse commençant par https). Le cadenas qui indique un accès sécurisé apparaît en haut ou en bas de la fenêtre de votre navigateur ;
- Sensibiliser vos personnels sur ce type d'arnaques ;
- Méfiez-vous des adresses mail similaires à celles de certains organismes.

Réactions :

Lorsque vous êtes victime d'une arnaque de type phishing, il est nécessaire de réagir de la façon suivante :
- Modifier et renforcer rapidement vos mots de passe sur les sites concernés par ces attaques ;
- Aviser votre banque de l'attaque dont vous avez été victime ;
- Signaler la tentative d'escroquerie ou une attaque avérée sur le site suivant :
https://www.internet-signalement.gouv.fr/
- Faire une copie-écran et des sauvegardes, des mails des attaques ou des tentatives d'attaques.

Aucun organisme bancaire ou site de vente en ligne (e-commerce) ne vous demandera vos identifiants (login-mot de passe).

AU MOINDRE DOUTE, ALERTEZ IMMÉDIATEMENT LES FORCES DE L'ORDRE