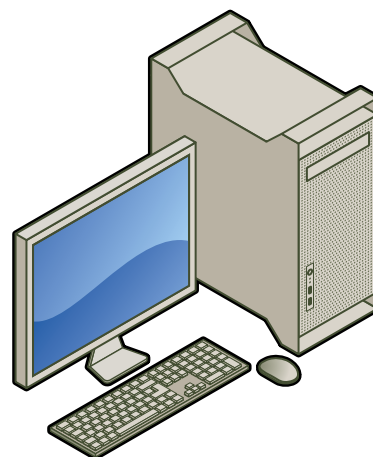


Cyberattaque : Phishing

Le phishing ou hameçonnage est une cyberattaque basée sur l'ingénierie sociale. En se faisant passer par courriel pour une entité connue (EDF, la CAF, une banque, un site de e-commerce etc.), le pirate essaie d'obtenir des informations personnelles sur sa victime ; pour à terme, l'escroquer, usurper son identité ou utiliser ces informations afin de mener une attaque informatique ciblée contre une entreprise ou une administration. Cette cyberattaque peut également être effectuée par SMS : il s'agit alors de SMishing.

Messagerie : réception d'un courriel émanant *a priori* d'une entité connue (EDF, Caf, Banque, site de e-commerce, etc.) et demandant à l'utilisateur de fournir des informations personnelles (date de naissance, mot de passe, numéro de carte de crédit, etc.). L'utilisateur est invité à **cliquer sur un lien et/ou remplir un formulaire par exemple**.



Si l'utilisateur « clique »,
une page web falsifiée
apparaît



Objectif du pirate informatique :
usurpation d'identité, escroquerie,
attaque ciblée contre une entreprise
ou une administration



Pour contrer l'attaque :

- Rester vigilant sur les courriels demandant de saisir ses paramètres d'authentification (données bancaires, login et mot de passe etc.)
- Enregistrer les pages régulièrement visités dans « favoris » et s'y connecter depuis cet onglet
- Faire attention à l'adresse indiquée dans la barre d'adresse de son navigateur
- Demeurer vigilant sur les liens intégrés aux courriels qui ne redirigent pas toujours vers le site internet concerné
- Contacter l'interlocuteur habituel de la société concernée si besoin
- Signaler les courriels à *Signal Spam* avec qui la Gendarmerie est partenaire et les liens de hameçonnage à *Phishing Initiative*

