5 PROTECTIONS CONTRE LE PHISHING

N'HESITEZ PAS À VOUS RENSEIGNER À LA DSI

Sous quelle forme trouve-t-on le phishing ?

Le phishing est un mail, un SMS ou encore un appel se faisant passer pour quelqu'un d'autres.

Quel est son objectif ?

Le but du phishing est de voler des informations personnelles ou professionnelles (mot de passe, compte, données bancaires...).

1 Ne pas ouvrir des mails d'expéditeurs inconnus

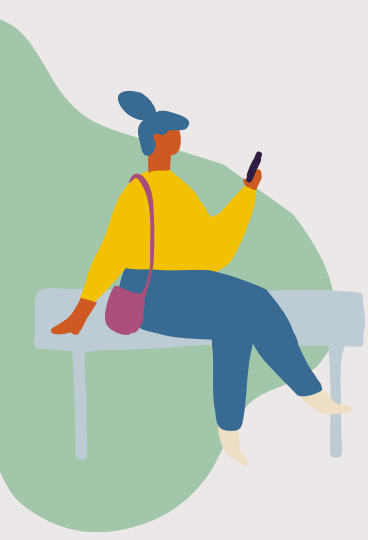
Les cybercriminels essayent de récupérer vos informations le plus souvent par email. Ne rentrez JAMAIS vos identifiants sur un lien envoyé par mail avant d'avoir demandé au service informatique.

2 Utiliser différents mots de passe

Créer des mots de passe différents pour les différents services de l'entreprise. Ne mettez jamais le même mot de passe que votre compte personnel.

3 Vérifiez l'URL du site web

Avant de rentrer vos informations d'identification veillez à vérifier le lien du site web. Le plus souvent un site web protégé commencera par "https".



4 Activer la double authentification

Activer la double authentification pour vous connecter. Cette technique permet d'éviter des nombreuses fraudes en devant rentrer un code unique à chaque connexion.

5 Si vous êtes victimes de phishing

Contacter immédiatement le service informatique de l'entreprise. Il fera le nécessaire pour éviter que la situation s'aggrave.