

Le 29 novembre 2024,

NOTE D'INFORMATION N°21/2024

Objet : Aide au phishing

Cette note a pour objectif de vous apporter quelques conseils :

Phishing. Mais concrètement c'est quoi ?

Il s'agit de mails et/ou de SMS envoyés par des personnes malveillantes qui se présentent comme ayant été envoyés par un membre de la société et dont l'objectif est de piéger afin d'obtenir des informations.

Ils peuvent vous demander de cliquer à travers de liens ou de vous attirer à vous connecter sur un site, jusqu'à saisir votre nom et votre mot de passe... Éléments que ces personnes vont utiliser à vos dépens.

Aujourd'hui certains mails sont proches de la perfection, mais ne sont pas envoyés par la société.

Merci de retenir ces points d'aide :

- Attention notamment aux fautes ou aux messages véhiculant un sentiment d'urgence ou de gravité
- Ne cliquez jamais sur un lien sans être certain de l'expéditeur !
- Préférez la recherche sur internet pour vous diriger vers la page officielle
- Choisissez un mot de passe sûr, composé d'au minimum de 12 caractères et qui doit :
 1. Intégrer des majuscules, des minuscules, des chiffres et caractères spéciaux.
 2. Éviter des données facilement devinables (date de naissance, nom, prénom,..)
 3. Renouveler régulièrement le mot de passe (90 jours)
 4. Jamais le même mot de passe sur des sites ou applications différents.
- Si vous êtes victime d'un mail malveillant :
 - Modifiez immédiatement votre mot de passe.
 - Restez vigilants : surveillez votre compte bancaire, mais aussi les mails que vous pourriez continuer à recevoir (une des techniques des malveillants est d'utiliser des informations volées pour obtenir la confiance et voler ainsi d'autres informations)

Enfin, sachez que la société a obligation de porter plainte dans les 72 heures en cas de cyber-attaque.

Je suis à votre disposition pour tout renseignement complémentaire et vous aider dans la démarche.

Abilio MATIAS
Responsable Informatique

