FICHE RÉFLEXE

PHISHING ET EMAILS FRAUDULEUX

DÉFINITION DU PHISHING

Le phishing est le vecteur de cyberattaque le plus fréquent dans le secteur de la santé. Il s'agit d'un e-mail, d'un site web ou d'un sms visant à vous duper !

#1 L'EXPÉDITEUR

- **Avant le @ :** Vérifier l'identité de la personne qui vous contacte
- **Après le @ :** Méfiez-vous des variations subtiles au niveau du nom de l'entité

⚠ Attention aux domaines très proches du vrai : chesquirol-limoges.fr /= ch-esquirol-limoges.fr

#2 L'OBJET

- **Soyez vigilant sur les messages inattendus,** alarmistes, trop irréaliste, même s'ils semblent provenir d'une source connue Ex : « Agissez immédiatement ! », « Votre compte/carte sera désactivé en 24h. »
- **Les cybercriminels jouent** souvent sur l'aspect psychologique et **sur la peur.** Leur objectif est de capter votre attention et de vous faire douter
- **Vérifiez l'heure d'envoi du mail.** Un envoi de mail la nuit sera plus suspect que la moyenne !

#3 LE CORPS DU MESSAGE

- **Une salutation générique ou une erreur dans la nomination** de la personne est suspecte
- Recherchez **des incohérences** dans le ton ou le style du message
- **Les attaquants imitent** parfois les logos officiels et les adresses proches de celle légitime
- **Évitez de transmettre des informations sensibles** sur sollicitation : aucun service légitime ne vous demandera par email ou SMS vos identifiants, ou des données patients nominatives

#4 LE LIEN ET LA PIÈCE JOINTE

- En cas de doute, **évitez de cliquer** directement sur les liens
- Dans le cas où vous avez cliqué, **comparer avec le lien du site officiel** si possible (Ex : go**0**gle.com /= google.com).
- **Méfiez-vous des pièces jointes** inattendues, surtout si l'expéditeur prétendu ne vous en enverrait pas habituellement
- **Toujours se connecter via les portails officiels**

#5 LA SIGNATURE

- **Comparez la signature** avec des mails provenant de la même source
- **Vérifiez la cohérence de l'expéditeur** avec la signature du mail

SIGNALEZ IMMÉDIATEMENT

- SI VOUS TROUVEZ UN MAIL SUSPECT, ET QUE VOUS AVEZ LE MOINDRE PETIT DOUTE
- Si vous avez cliqué par erreur sur un lien suspect
- Si vous avez saisi des identifiants sur un site potentiellement frauduleux.
- Si vous pensez avoir identifié un courriel d'hameçonnage

Avertir le service informatique
1017 ou 05 55 43 10 17
ou nous contacter sur
informatique@ch-esquirol-limoges.fr

Transférer l'email suspect **au service informatique**

Demander à parler au **Référent Sécurité**

Supprimer le message **après vérification**