# ATTENTION !!
## Multi-tentatives de hameçonnage (*phishing*) à l'INUC

### Le *hameçonnage*, c'est QUOI ?

C'est une technique destinée à vous leurrer pour vous inciter à communiquer des données personnelles (comptes d'accès, mots de passe…).

La plupart du temps, pour qu'une attaque par mail fonctionne, il faut que la victime ait effectué une action dans le mail : cliquer sur un lien ou ouvrir une pièce jointe.

**Au moindre doute, il ne faut surtout pas cliquer sur un lien ou ouvrir une pièce jointe.**

Si le mail semble suspect ou trop beau pour être vrai : **MÉFIANCE** !


## *Comment détecter un mail de hameçonnage ?*

**Flashez le QR code pour découvrir les techniques de repérage d'un mail de hameçonnage**

**https://numerique.univ-jfc.fr/article/quest-ce-que-lhameconnage-phishing**

## *J'ai reçu un mail de hameçonnage, que faire ?*

### Je l'ai détecté

**Sans cliquer sur aucun lien ni pièce jointe :**

- Je le transfère à **spam@univ-jfc.fr**
- Puis je le supprime immédiatement

### J'ai un doute

**Sans cliquer sur aucun lien ni pièce jointe :**

- Je le transfère à **spam-doute@univ-jfc.fr**

et j'attends la réponse de la DSIUN

### Je ne l'ai pas détecté et j'ai été hameçonné·e

- **Je change mon mot de passe sur l'ENT le plus vite possible :** page d'authentification > *Changer votre mot de passe*
- **Je crée un ticket pour la DSIUN via la tuile helpdesk**

### Que risque-t-il de se passer ?

Votre compte pourrait être utilisé pour spammer d'autres utilisateurs (envoi de milliers de mails en quelques heures). Dans ce cas **votre compte sera bloqué par la DSIUN** et vous n'y aurez plus accès. RDV à la DSIUN pour le débloquer.

Attention, certains utilisateurs spammés par votre adresse pourraient répondre de façon virulente. Ne le prenez pas pour vous et n'en tenez pas compte.

Institut National Universitaire **Champollion**