



SÉCURITÉ INFORMATIQUE

Les bonnes pratiques

UTILISEZ DES MOTS DE PASSE COMPLEXES

- pas trop courts;
- pas de lien avec soi (par ex: date de naissance)
- mélangez majuscules, minuscules et symboles.



N'UTILISEZ PAS LES MÊMES MOTS DE PASSE POUR UN USAGE PROFESSIONNEL ET PERSONNEL

NE DONNEZ JAMAIS VOTRE MOT DE PASSE

(les équipes de la DiSI ne vous demanderont jamais votre mot de passe)



EN CAS DE DOUTE SUR L'AUTHENTICITÉ D'UN MAIL:

- n'y répondez pas;
- ne cliquez pas sur les liens/PJ qu'il contient (risque de phishing);
- n'hésitez pas à contacter les services de la DiSI.

PRIVILÉGIEZ VOTRE ADRESSE MAIL UPJV LORS DE VOS ÉCHANGES PROFESSIONNELS

La DiSI assure une maintenance des serveurs mails garantissant une qualité de service optimale tant dans la rapidité que dans la sécurité.



PRIVILÉGIEZ LES LISTES DE DIFFUSION OU COPIES CACHÉES

afin de ne pas divulguer les adresses mails de vos correspondants

EFFECTUEZ DES SAUVEGARDES RÉGULIÈRES

- Pensez à utiliser *Nextcloud*



PENSEZ À VOUS DÉCONNECTER DE VOTRE ENT ET DES APPLICATIONS OUVERTES LORSQUE VOUS QUITTEZ VOTRE POSTE DE TRAVAIL

N'OUBLIEZ PAS DE PROTÉGER VOS APPAREILS PAR DES MOTS DE PASSE ET DE LES CONFIGURER POUR QU'ILS SE VERROUILLENT AUTOMATIQUÉMENT



ÉVITEZ D'UTILISER UN RÉSEAU WI-FI NON SÉCURISÉ

Privilégiez toujours le réseau UPJV dans les locaux de l'université, sinon utilisez votre VPN