Fiche réflexe

Usages numériques et sécurité

Les utilisateurs et utilisatrices assurent un rôle essentiel pour limiter le risque des attaques. Aussi, il vous est demandé une vigilance accrue et le respect des bonnes pratiques dans vos usages numériques suivantes :

- Utiliser les outils disponibles à l'ENS : https://intranet.ens.psl.eu/fr/services-administratifs/centre-de-ressources-informatiques/informations-documentations/boite-outils
- Faire preuve d'une vigilance constante dans la gestion des courriers électroniques : Lorsqu'il s'agit d'un message dont l'expéditeur n'est pas connu, ne pas ouvrir le courriel en l'absence de vérification préalable, ne pas procéder au téléchargement des pièces jointes et ne pas activer les liens hypertextes
- Veiller à séparer les usages professionnel et personnels : utilisez des mots de passe différents pour tous les services professionnels et personnels auxquels vous accédez, utilisez la messagerie professionnelle et non personnelle pour vos envois professionnels
- Ne pas utiliser de services de stockage en ligne personnel à des fins professionnelles
- Dans le cadre d'échanges avec un interlocuteur connu et considéré comme de confiance : ne pas sous-estimer les risques d'usurpation d'identité et prêter une attention particulière à la pertinence du message, à la cohérence des propos, aux changements inhabituels dans le style d'écriture ou la police de caractères
- Changer de mot de passe régulièrement
- S'assurer de ne pas conserver, dans sa boîte mail, d'éventuelles pièces et informations contenant des données à caractère personnel (ne pas conserver dans sa boîte mail des copies de pièces d'identité, de diplômes, de RIB,…)
- Protéger les données sensibles (travaux de recherche, savoir-faire, publication en cours…) sur des infrastructures internes à l'Ecole et non sur un service de *cloud*
- Sauvegarder régulièrement les données sensibles (travaux de recherche, savoir-faire, publication en cours,…) sur un support externe
- Eviter les réseaux WI-FI publics ou inconnus

En cas de suspicion ou d'attaque informatique (phishing, rançonlogiciel,…) : prévenir immédiatement le RSSI : rssi@ens.psl.eu