ÉCOLE
NORMALE
SUPÉRIEURE
DE LYON

15 parvis René-Descartes
BP 7000, 69342 Lyon cedex 07
Tél. +33 (0)4 37 37 60 00
www.ens-lyon.fr

Présidence
Réf : JFP/LH/NS/VD/2022

Lyon, le 19 avril 2022

NOTE

à l'attention de tous.ens

Objet : Recommandations concernant la sécurité du système d'information

La sécurité du système d'information (SI) est un enjeu majeur notamment dans le contexte actuel où de plus en plus d'organisations voient leur fonctionnement désorganiser par des attaques sur leur SI. Ces derniers mois les services de l'École ont beaucoup œuvré pour garantir cette sécurité mais de nombreuses attaques ciblent les utilisateurs que nous sommes à un niveau individuel via des vols de mots de passe ou d'ordinateurs, ou encore en s'introduisant dans les ordinateurs pour récupérer des informations.

Votre vigilance est donc nécessaire et vous trouverez ci-après des mesures que nous vous demandons d'adopter.

1. Bonnes pratiques concernant l'ensemble des utilisateurs

Authentification forte : L'authentification forte est une mesure efficace contre les vols de mot de passe. Elle fait partie du socle de mesures essentielles transmises par l'ANSSI (agence nationale de la sécurité des systèmes d'information). Une fois activée, elle sécurise vos connexions en sollicitant, en complément de votre mot de passe habituel, un code temporaire généré par une application ou envoyé par SMS.

Une communication précise sera effectuée prochainement à ce sujet.

Messagerie/phishing : Le phishing ciblé consiste à voler nos mots de passe via des sites web dédiés ou des envois de messages en masse à des adresses @ens-lyon.fr. Parfois le phishing est grossier mais il peut arriver de se retrouver avec des pièges qui miment parfaitement nos quotidiens (par exemple renvoi vers un site qui semble correspondre à une application connue ou encore envoi de la part d'un nom que nous connaissons mais avec une adresse finale incohérente).

Aussi il convient de vérifier si :
- le nom d'expéditeur est bien habituel
- l'adresse d'expédition est bien cohérente
- l'objet n'est pas trop alléchant ou alarmiste
- l'apparence générale n'est pas suspecte (images/logos de mauvaise qualité)
- le texte contient beaucoup de fautes (orthographe, grammaire, texte traduit automatiquement)
- l'on vous demande des informations confidentielles
- le message n'est pas aguicheur ou inquiétant

Une plateforme de e-learning sera prochainement mise à disposition, dans un premier temps auprès de certains publics de la sphère administrative afin de repérer ce type de message. Son accès sera élargi à d'autres publics ultérieurement.

Si vous le souhaitez, vous pouvez également consulter le site https://phishingquiz.withgoogle.com/?hl=fr

ÉCOLE NORMALE SUPÉRIEURE DE LYON

15 parvis René-Descartes
BP 7000, 69342 Lyon cedex 07
Tél. +33 (0)4 37 37 60 00
www.ens-lyon.fr

Si vous avez un doute, n'hésitez pas à faire suivre le message suspect à **rssi@ens-lyon.fr**.

Messagerie/pièces jointes : Des pièces jointes peuvent contenir des virus. Les questions à se poser : connaissez-vous l'expéditeur, attendez-vous vraiment ce courrier, est-ce que le contenu du message est habituel ou au contraire incohérent. **Dans tous les cas, si l'ouverture de la pièce jointe entraîne une demande d'activation des macro, refusez.**

Comme pour le phishing une plateforme spécifique de e-learning va être mise à disposition, dans un premier temps auprès de certains publics de la sphère administrative, afin de repérer ce type de message

Sauvegarde : Stockez vos données dans un espace sauvegardé : de préférence sur un espace réseau (ensldfs, ged, etc..) ou en local seulement si votre poste est sauvegardé, voir https://intranet.ens-lyon.fr/documentation/sauvegarde-du-poste-de-travail

Mot de passe : Ne réutilisez jamais le mot de passe « ENS » sur un autre site. Il s'agit d'éviter qu'un vol de mot de passe sur un autre site (cela arrive régulièrement) mette en danger votre compte ENS. Le mot de passe ENS doit être complexe et unique.

2. **Bonnes pratiques concernant plus spécifiquement les *administrateurs* de leurs postes (enseignants-chercheurs, chercheurs…)**

Antivirus : Tout poste professionnel Windows ou Mac doit être équipé de l'antivirus fourni par l'ENS de Lyon. Rapprochez-vous de votre informaticien de proximité ou de la DSI si vous n'en disposez pas.

Mises à jour : Appliquez les mises à jour de vos équipements et logiciels. De nouvelles failles de sécurité apparaissent quotidiennement et sans mise à jour vous devenez une cible facile pour les attaquants. Pour plus d'informations : https://www.cybermalveillance.gouv.fr/tous-nos-contenus/bonnes-pratiques/mises-a-jour

Pare-feu : Activez le pare-feu de votre ordinateur. Rapprochez-vous de votre informaticien de proximité ou de la DSI si vous souhaitez vérifier ce point.

Chiffrement : Activez le chiffrement de votre disque dur : si votre machine est volée ou perdue il est fondamental que toute vos données (et une partie de celle de l'ENS) ne se retrouve pas en de mauvaise main. Voir https://intranet.ens-lyon.fr/documentation/chiffrement-des-donnees

Je vous remercie de bien vouloir diffuser ces mesures à vos collaborateurs et le cas échéant, pour toute information complémentaire sur ces sujets, vous pouvez contacter M. Nicolas SCHMITZ, responsable de la sécurité du système d'information (RSSI) de l'ENS de Lyon ou Viviane Delattre, DSI et RSSI suppléant, à l'adresse **rssi@ens-lyon.fr**

Jean-François PINTON
Président