

Sensibilisation Cybersécurité 2024



Règles et bonnes pratiques
Être vigilant
Phishing

Par l'apprenti Expert Cybersécurité



SOMMAIRE



Sécurité physique

Support amovible

L'authentification

La double authentification

Sécurité de l'information

Le phishing

Sécurité physique

Sécurisation du poste

Votre ordinateur doit être sécurisé à l'aide d'un câble antivol ou être mis sous clé.

En cas d'absence de câble, rapprochez-vous de votre service IT.

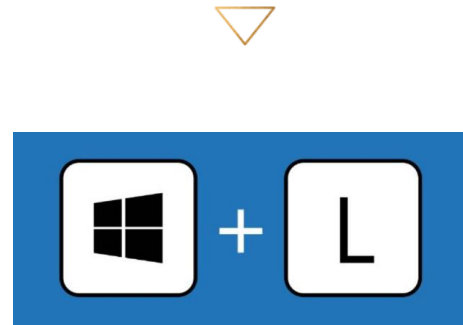


Confidentialité

Une pause-café s'impose ?

Besoin d'aller rendre visite à un/une collègue ?

On n'oublie pas de verrouiller son ordinateur !



Entretien du matériel

Votre ordinateur reste la propriété de BRI.

Il devra être retourné dans son état initial.

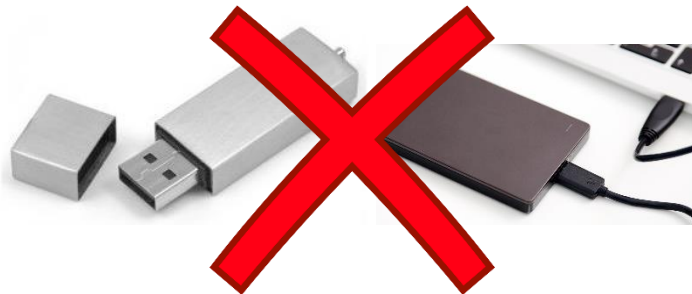
Aucun sticker ne doit y être apposés.



Support amovible

Stockage amovible

L'utilisation de tout type de matériel de stockage est interdite quel que soit sa provenance.



Chargement du smartphone

Le chargement de votre Smartphone doit se faire depuis une prise électrique.



Partage de fichiers

Teams et OneDrive sont les seules solutions approuvées par L'Oréal pour partager et stocker des documents (y compris avec des partenaires externes).



Authentification

Les mots de passe n'auront aucun secret pour vous

En béton armé !

12 caractères mélangeant minuscules, majuscules, chiffres et caractères spéciaux.

Il ne dit rien sur vous !

Evitez les rapports psycho-sociaux.

Pro et perso, 2 mots de passe différents !

Pour éviter les piratages en cascade.

Ne l'abandonner pas en pleine nature !

Un post-it, une boîte mail n'est pas un lieu de stockage sécurisé pour un mot de passe.

N'appliquez pas de compteur !

Exemple : toto!01 , toto!02 , etc.



Comment mémoriser un mot de passe fort ?

Phrase de passe

Utilisez une suite de mots au hasard
« Lunettes:Crayon:Poste:Chemin32 »
« JeSuisUnePetiteVoitureViolette-56 »

Utilisez la phonétique

« J'aime les vacances à deux avec Marie ! » → J'mLeVa@2aM!
« Deux cadeaux à Noël ?! » → 2KDO@nowel?!

Conservez les premières lettres d'une phrase, d'une citation, d'une chanson, etc.

« Le cœur d'une femme est un océan de secret ! »
devient
« Lcd'1f&1O2s! »

Double authentification (MFA)

Protection de vos données et autonomie sur la gestion de votre mot de passe



Activer la double authentification

Depuis un **PC L'Oréal**, se rendre sur
Le lien pour le MFA

Ajouter une méthode (Téléphone)

Entrer le SMS reçu

***Autonome sur la réinitialisation de mon mot de passe
depuis le lien pour réinitialiser son mot de passe***

Protection supplémentaire de mes données personnelles

Après votre arrivée, pour des raisons de cybersécurité, votre service IT ne vous distribuera plus votre mot de passe.

Sécurité de l'information

Ingénierie sociale

Manipulation consistant à obtenir un bien ou une information, en exploitant la confiance, l'ignorance ou la crédulité de tierces personnes

VIGILANCE SUR LES RÉSEAUX SOCIAUX ET LES OUTILS IA



MOT DE PASSE STRICTEMENT PERSONNEL



VIGILANCE FACE AUX REQUÊTES INHABITUELLES



Le phishing

Définition et conséquences

Le **phishing** (ou **hameçonnage**) est une technique frauduleuse **destinée à leurrer** l'utilisateur pour **l'inciter à communiquer** ses données personnelles (compte Microsoft, mot de passe, boîte mail, etc.)



ATTEINTE À LA NOTORIÉTÉ

En 2014, Sony a subi une attaque par Spearphishing, **provoquant une fuite des prochains films** à sortir au cinéma. Sa réaction jugée inadéquate a fait **perdre la confiance de ses parties prenantes**.

FUITE DE DONNÉES PERSONNELLES OU INDUSTRIELLES

En février 2023, la mairie de Lille a subi une **fuite des données personnelles des agents**. Les cybercriminels ont utilisé ces adresses pour faire une demande de rançon.

PERTE FINANCIÈRE

En 2018, Equifax (société de crédit américaine) a perdu 35% de sa valeur boursière soit une **perte de 3,4 milliards de dollars** en capitalisation boursière.

Le phishing

Ne mordez pas à l'hameçon !

Poste de travail infecté : nettoyage effectué

Service Desk <no-reply@helpdesk-supp0rt.com>

mer. 09/03

Cliquez ici pour télécharger des images. Pour protéger la confidentialité, Outlook a empêché le téléchargement automatique de certaines images dans ce message.

EXTERNAL EMAIL: BE VIGILANT

-- Message automatique du service informatique --

D'après notre analyse de vulnérabilité à l'échelle de l'entreprise, votre poste de travail a été infecté par [Storm Worm]

Suite à cette découverte, une procédure de nettoyage a été effectuée sur votre poste de travail. Au cours de cette procédure, plusieurs fichiers ont été supprimés de votre poste de travail.

La liste des documents en question est accessible via le lien suivant :

[Documents supprimés](#)

Pendant les prochaines 48 heures, vous pourrez récupérer certains documents supprimés en cliquant sur ce lien.

Nous sommes désolés pour la gêne occasionnée et vous remercions de votre compréhension.

Le centre d'assistance informatique

SUJET : il y a souvent un sentiment d'urgence créé pour vous encourager à agir rapidement et en toute confidentialité

DE : le message peut sembler provenir d'une source fiable, mais l'email est envoyé à partir d'une adresse mail frauduleuse

NOTICE : Cela devrait immédiatement vous faire douter de l'authenticité du message. La bannière « External mail » indique que le mail provient de l'externe (alors que le mail affiché semble être un mail interne)

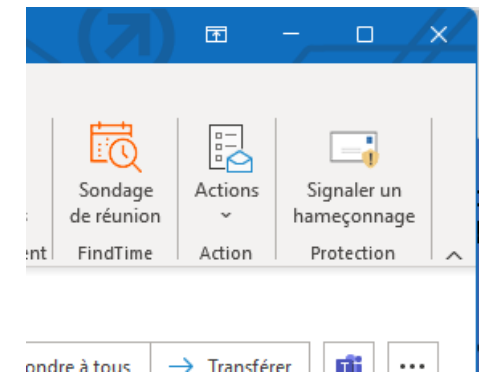
CONTENU :
La plupart des emails de phishing contiennent ces éléments :

- Contexte urgent (situation de crise qui ne peut attendre - hors des processus habituels)
- Incitation à ouvrir une pièce jointe
- Incitation à cliquer sur un lien (vous demandant de soumettre votre login et votre mot de passe, ou des données à caractère personnel afin de les transmettre à l'attaquant)



Ne dérogez jamais à la sécurité ou aux procédures en place. Au moindre doute, signalez le mail à l'aide du bouton « Report Phishing » pour analyse.

Comment signaler un email suspect ?



Merci pour votre attention



**Protégez vos données,
protégez votre avenir :
la cybersécurité, une
responsabilité partagée !**