

Situation 4 : Je reconnais les mails frauduleux et je sécurise mon compte

Durée : 1,5 heure

OBJECTIFS SPÉCIFIQUES :

- Identifier les mails frauduleux
- Prévenir les dangers liés à l'utilisation du mail
- Sécuriser son compte

CHAMPS À QUESTIONNER

- Quels sont les différents dangers liés aux emails ?
- Que faire face à ces dangers ?
- Quels sont les comportements à adopter pour prévenir ces dangers ?
- Pourquoi est-ce utile de connaître les dangers ?

REPRÉSENTATIONS INITIALES SUR LA CARTE MENTALE

Le bénéficiaire complète sa carte mentale en individuel. Il échange ensuite ses représentations avec le/la formateur.rice et ses pairs.

ACTIVITÉ

Lors de cette activité, le bénéficiaire est invité à consulter différentes ressources portant sur les dangers liés à l'utilisation de l'email.

- Rendez-vous sur le site PMTIC : « Les arnaques sur internet » :
<https://www.pmtic.net/contenu-en-ligne/communication/e-mail/les-dangers/decouvrons/les-arnaques-sur-internet>
- **Ou** sur le site Safeonweb, surfez en toute sécurité : <https://safeonweb.be/fr/surfez-en-toute-securite>
- Échangez ensuite avec le bénéficiaire à propos des principes de base nécessaires à la reconnaissance des mails frauduleux, sur les démarches à faire en cas de doute et en cas de réception d'un faux message.
- Proposez-leur ensuite de s'exercer à la reconnaissance de quelques mails frauduleux (en individuel ou en groupe) :
 - Site PMTIC-exerçons-nous : <https://www.pmtic.net/contenu-en-ligne/communication/e-mail/les-dangers/exercons-nous/legitime-ou-frauduleux>
 - Site Safe on web : <https://safeonweb.be/fr/quiz/test-du-phishing>
- Sur le site de Safeonweb, consultez la ressource « utilisez des mots de passe sûrs » :
<https://safeonweb.be/fr/utilisez-des-mots-de-passe-surs>

ÉVALUATION 1

Demandez au bénéficiaire de lister dans un document Word ou Writer les principes de base au sujet de la reconnaissance et la prévention de mails frauduleux sous forme de recommandations.

Le bénéficiaire doit envoyer son document en fichier attaché à l'ensemble du groupe de bénéficiaires.

Consignes pour la réalisation du document :

- Une page A4 maximum
- Le document doit aborder les éléments suivants : les différents dangers liés aux mails, les principes de reconnaissance de ces dangers et les bonnes pratiques à mettre en place face à ces dangers
- Identifier les ressources intéressantes à partager avec ses pairs

Le groupe identifie ensuite le document qui lui semble être le plus clair et le plus complet. Le document sera affiché dans le local de formation.

Critères :

- Les différents éléments sont abordés (dangers identifiés, principes de reconnaissance et prévention/traitement de ces dangers)
- Le document est lisible et compréhensible
- Les sources sont citées
- Le document tient en une page A4.

ÉVALUATION 2

Transfert : Le bénéficiaire est invité à aller dans sa boîte mail personnelle afin de s'assurer de la sécurité de cette dernière. Il est ensuite invité à créer un mot de passe sécurisé :

<https://pwdtest.bee-secure.lu/>

Lors de cette étape, le formateur.rice a l'occasion de s'assurer de la réelle maîtrise des fonctionnalités principales de l'email.

Ressources à disposition des bénéficiaires	
« Phishing : détecter un message malveillant »	https://www.cnil.fr/fr/phishing-detecter-un-message-malveillant
« Pourquoi sécuriser au maximum le mot de passe de votre boîte email ? »	https://www.cnil.fr/fr/pourquoi-securiser-au-maximum-le-mot-de-passe-de-votre-boite-email
Site PMTIC : « Les arnaques sur internet » et « Le phishing »	https://www.pmtic.net/contenu-en-ligne/communication/e-mail/les-dangers/decouvrons/les-arnaques-sur-internet
Surfez en toute sécurité	https://safeonweb.be/fr

Les conseils de la CNIL pour un bon mot de passe	https://www.cnil.fr/fr/les-conseils-de-la-cnil-pour-un-bon-mot-de-passe
Utilisez des mots de passe sûrs	https://safeonweb.be/fr/utilisez-des-mots-de-passe-surs

ENRICHISSEMENT DE LA CARTE MENTALE

Le bénéficiaire est invité à enrichir sa carte mentale avec les nouveaux concepts acquis en lien