Feuille d'exercice Mobile Money

MODULE 2

Exercice 1

Jouer et apprendre Quiz

Durée estimée

10 min

Matériel

Dispositif avec accès à Internet Papier et stylo

Instructions

Sur la page suivante, vous trouverez un quiz de 5 questions sur la sécurité en ligne !

Entourez les questions et trouvez les réponses avec les explications sur la troisième page – pas de triche !

:-)

1. Quel est le mode de transmission le plus courant des virus ?

A. Courriel

B. Message instantané

C. Téléchargement sur Internet

D. Supports portables

2. Lequel des mots suivants serait le meilleur mot de passe ?

A. Mon secret

B. Iw2c^tILV

C. Abc123

D. George1234

3. Votre sœur vous envoie un e-mail contenant un fond d'écran qui, selon elle, vous plairait beaucoup. Que devez-vous faire ?

A. Téléchargez-le sur votre ordinateur, car il provient d'une source fiable.

B. Transférer le message à d'autres amis pour le partager.

C. Appelez votre soeur et demandez-lui de vous aider à l'installer.

D. Supprimer le message.

4. Lorsque vous recevez un courriel d'un contact inconnu contenant une pièce jointe, vous devez.. :

A. Ouvrir la pièce jointe pour en visualiser le contenu

B. Supprimer le mail

C. Transférez l'e-mail à vos amis pour leur permettre d'ouvrir d'abord la pièce jointe.

D. Transférez l'e-mail vers votre compte de messagerie personnel afin de pouvoir l'ouvrir à la maison.

1. **Quel est le mode de transmission le plus courant des virus ?**

A. Courrier électronique

Le courrier électronique est la méthode la plus courante de transmission des virus. Les cybercriminels utilisent souvent le courrier électronique comme vecteur de diffusion de logiciels malveillants. Ces courriels peuvent sembler provenir de sources fiables, ce qui les rend particulièrement dangereux.
Lorsque le destinataire ouvre la pièce jointe ou clique sur le lien, le virus peut être téléchargé et exécuté sur son appareil.

2. **Lequel des mots suivants serait le meilleur mot de passe ?**

B. Iw2c^tILV

Parce qu'il respecte les principes clés de la création d'un mot de passe fort :
Complexité : il comprend un mélange de lettres majuscules, de lettres minuscules, de chiffres et de caractères spéciaux, ce qui le rend difficile à deviner ou à déchiffrer par force brute pour les attaquants.
Longueur : Il est suffisamment long, ce qui ajoute un niveau de sécurité supplémentaire. Les mots de passe longs sont généralement plus difficiles à déchiffrer.
Imprévisibilité : Le mot de passe ne comprend pas de mots ou de motifs faciles à deviner, qui sont soit courants, soit simples, soit liés à l'utilisateur.

3. **Votre sœur vous envoie un e-mail au travail avec un économiseur d'écran.**

D. Supprimer le message.

4 grands risques :

1. Certains fonds d'écran contiennent des virus.
2. Cliquer sur un lien malveillant peut infecter un ordinateur.
3. Les adresses électroniques peuvent être falsifiées. Par conséquent, même si l'e-mail indique qu'il provient d'une personne que vous connaissez, vous ne pouvez pas en être certain sans vérification.
4. Certains sites web et liens semblent légitimes, mais il s'agit en réalité de canulars conçus pour voler vos informations.

Soyez prudents et profitez du monde numérique !

Feuille d'exercice Mobile Money

MODULE 2

Exercice 2
Ce lien est-il sûr ?

Durée estimée
10 min

Matériel
Dispositif avec accès à Internet Papier et stylo

Instruction

Lire le texte
Réfléchir

Nous ferons l'exercice ensemble pour comprendre pourquoi le lien est sûr ou non.

1. Décider si le lien peut être consulté en toute sécurité :

Supposons que vous receviez un courriel d'une banque vous demandant de cliquer sur un lien comme celui ci-dessous et de soumettre des données personnelles, telles que votre nom d'utilisateur, vos mots de passe et les détails de votre carte de crédit.

http://url5423.eka.de/ls/click ?
upn=V1OaWNMSPs2Lb0JqHpnyTLRlk2703ToIFpo2vd2MKt5gB6dYAUvw1B-2FnC6T5iVsCdbug7l6pkTad-2FBfACSlC-2BKw-3D-3DhmuAs- OaWNMSPs2Lb0JqHpn-asDvdva

Ne vous précipitez pas, réfléchissez-y deux fois et décidez si vous pouvez visiter ce lien en toute sécurité.

Réfléchissez aux raisons.

La réponse.

Ce lien **n'**est **pas** sécurisé pour plusieurs raisons :

- Il utilise http au lieu de https.
- Le nom de domaine n'est pas lié au nom officiel de la banque. Le lien est
- étrangement long.
- Le nom de domaine du lien est différent du nom de domaine de l'adresse électronique de l'expéditeur.
- Une vraie banque ne demandera jamais de noms d'utilisateur, de mots de passe ou d'informations sur les cartes de crédit.

Feuille d'exercice Mobile Money

MODULE 2

Exercice 3

Votre score de sécurité en ligne

Durée estimée

10 min

Matériel

Les appareils disposant d'un accès à Internet sont soumis à un test en ligne.

Stylo pour le test hors ligne.

Instruction

Le test peut être réalisé individuellement ou en groupe . Il peut être utilisé en ligne ou avec un papier et un stylo. Les réponses sont OUI et NON.

Ce test vous donnera un score, votre formateur peut vous expliquer les résultats.

Répondre par OUI ou NON

1. Utilisez-vous l'authentification à deux facteurs sur vos appareils ? Par exemple, l'authentification par empreinte digitale et par mot de passe.
2. Utilisez-vous un coffre-fort pour vos mots de passe ? Il s'agit d'un endroit où tous vos mots de passe pour plusieurs comptes sont stockés ensemble en toute sécurité.
3. Utilisez-vous la navigation privée lorsque vous êtes en ligne ?
4. Est-ce que vous réglez tous vos paramètres sur les réseaux sociaux sur privé ?
5. Publiez-vous régulièrement sur les réseaux sociaux des photos de vous?
6. Vérifiez-vous régulièrement vos transactions bancaires pour vous assurer qu'il n'y a pas de dépenses dont vous n'avez pas connaissance ?
7. Avant de saisir les données de votre carte de crédit lors d'un achat en ligne, vous assurez-vous qu'il y a un cadenas ou une preuve que le site web que vous visitez est sécurisé ?
8. Votre ordinateur est-il équipé d'un logiciel de sécurité, tel qu'un anti-virus, un anti-logiciel espion ou un pare-feu ?
9. Si votre ordinateur vous invite à mettre à jour le logiciel, le feriez-vous immédiatement ?
10. Utilisez-vous un mot de passe différent pour chaque compte pour lequel vous avez un identifiant ?

Félicitations !

Votre score de sécurité en ligne est de ********_____*****

Vous êtes une super-star de la sécurité!