RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

CYBER MALVEILLANCE .GOUV.FR
Assistance et prévention en sécurité numérique

TESTEZ VOS CONNAISSANCES

GÉRER SES MOTS DE PASSE

1/ Bonnes pratiques

Parmi les propositions, quelles sont les deux bonnes pratiques à mettre en œuvre pour assurer la sécurité de vos mots de passe ?

- ☐ **A** Les noter sur un post-it pour s'en souvenir
- ☐ **B** Choisir un mot de passe suffisamment complexe
- ☐ **C** Les confier à un tiers en cas de besoin
- ☐ **D** Utiliser un mot de passe différent pour chaque accès

2/ Vrai ou Faux

J'ai un mot de passe très sécurisé. Je peux donc l'utiliser sur tous mes comptes et services.

☐ **Vrai** ☐ **Faux**

3/ Cherchez l'intrus

Un mot de passe sécurisé :

- ☐ **A** est facile (suite logique, le prénom de mes enfants, ma date de naissance, etc.)
- ☐ **B** comporte 12 caractères mélangeant des majuscules, des minuscules, des chiffres et des caractères spéciaux
- ☐ **C** suit un moyen mnémotechnique

4/ Reliez les situations à leurs solutions

Je ne me souviens jamais de mes mots de passe	**A** ☐	☐ **1**	Je n'enregistre pas les mots de passe et me déconnecte après utilisation
Je soupçonne qu'un de mes comptes ait été piraté	**B** ☐	☐ **2**	Je fais confiance à Keepass, mon gestionnaire de mots de passe
Je travaille sur un ordinateur à la bibliothèque	**C** ☐	☐ **3**	Je change immédiatement de mot de passe

RÉPONSES

1/B et D – Vos mots de passe sont la porte d'entrée de vos appareils numériques et de l'accès à vos comptes, qui peuvent contenir des données sensibles. Protégez vos accès en utilisant un mot de passe complexe et unique pour chaque accès.
2/FAUX – Il vaut mieux utiliser un mot de passe différent et complexe pour chaque accès ou service. En effet, en cas de perte ou de vol d'un de vos mots de passe, vous limitez les risques d'accès frauduleux au seul compte lié à ce mot de passe.
3/A – Un mot de passe trop simple ou facile à deviner n'offre pas un niveau de sécurité suffisant, ce qui pourrait faciliter la tâche des cybercriminels.
4/A – 2 B – 3 C – 1

HAMEÇONNAGE

1/ Bonnes pratiques

Sur mon compte bancaire, je découvre un débit que je ne reconnais pas. Je crains d'être victime d'un «hameçonnage» lié à un message douteux auquel j'ai répondu il y a deux semaines. Parmi les propositions, quelles sont les deux bonnes pratiques à mettre en œuvre ?

- ☐ **A** Je vérifie auprès de ma banque l'origine du débit et fais opposition à celui-ci
- ☐ **B** Je laisse passer quelques jours pour m'assurer qu'il s'agit vraiment d'un débit frauduleux
- ☐ **C** Je dépose plainte au commissariat de police ou à la gendarmerie la plus proche

2/ Vrai ou Faux

Il est inutile de déposer plainte pour un message d'hameçonnage auquel j'ai répondu.

☐ **Vrai** ☐ **Faux**

3/ Cherchez l'intrus

Comment se prémunir de l'hameçonnage ?

- ☐ **A** Si j'ai un doute concernant un message électronique ou un appel, je contacte directement l'organisme concerné pour en confirmer l'authenticité
- ☐ **B** Je vérifie qu'il y ait bien un logo officiel dans le message reçu
- ☐ **C** Avant de cliquer sur un lien douteux, je positionne le curseur de ma souris sur le lien sans cliquer pour vérifier l'adresse vers laquelle il pointe
- ☐ **D** Je ne communique jamais d'informations sensibles par téléphone ou messagerie électronique

4/ Reliez les situations à leurs solutions

Mon adresse de messagerie a été usurpée	**A** ☐	☐ **1**	Je fais opposition auprès de ma banque et je dépose plainte
J'ai malencontreusement communiqué mon numéro de carte bancaire	**B** ☐	☐ **2**	Je la signale à Phishing Intiative
J'identifie une adresse de site d'hameçonnage	**C** ☐	☐ **3**	Je change immédiatement de mot de passe

RÉPONSES

1/A et C
2/FAUX – Si vous avez malencontreusement communiqué des informations sensibles, comme votre numéro de carte bancaire, déposez plainte au commissariat de police ou à la gendarmerie la plus proche. Les cybercriminels pourraient, en effet, en faire un usage frauduleux. Pour être conseillé en cas d'hameçonnage, contactez le service Info Escroqueries au 0805 805 817 (appel gratuit).
3/B – Le fait qu'il y ait dans un message le logo officiel d'un organisme ne signifie pas nécessairement que le message ait été envoyé par l'organisme concerné.
4/A – 3 B – 1 C – 2

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

CYBER MALVEILLANCE .GOUV.FR
Assistance et prévention en sécurité numérique

SÉCURITÉ DES APPAREILS MOBILES

1/ Bonnes pratiques

Parmi les propositions, quelles sont les deux bonnes pratiques à mettre en œuvre pour assurer au mieux la sécurité numérique de vos appareils mobiles ?

- ☐ **A** Je ne fais jamais fonctionner le Wifi et le Bluetooth en même temps
- ☐ **B** Je mets régulièrement mes appareils à jour
- ☐ **C** Je les verrouille avec un code d'accès difficile à deviner, en plus du code PIN
- ☐ **D** J'équipe mes appareils d'une coque et d'une protection d'écran

2/ Vrai ou Faux

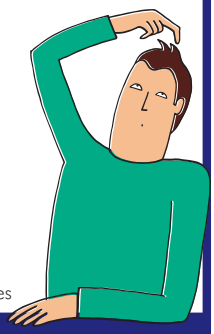
Je n'ai pas besoin de faire des sauvegardes de mon téléphone.

☐ **Vrai** ☐ **Faux**

3/ Cherchez l'intrus

J'ai besoin d'une application mobile. Je la télécharge :

- ☐ **A** sur le site officiel du fournisseur
- ☐ **B** sur les magasins officiels d'applications comme Google Play ou App Store, par exemple
- ☐ **C** sur n'importe quel autre site



4/ Reliez les situations à leurs solutions

Je travaille régulièrement à l'extérieur **A** ☐
J'ai perdu ou je me suis fait voler mon téléphone **B** ☐
Je télécharge un jeu sur mon téléphone **C** ☐

- ☐ **1** Je bloque ma ligne en appelant mon opérateur et mon téléphone en communiquant mon code IMEI et je dépose plainte
- ☐ **2** J'évite de me connecter à un réseau Wi-Fi public
- ☐ **3** Je n'autorise pas l'accès à mes photos, mes contacts et mes messages

RÉPONSES

1/B et C
2/FAUX – Votre appareil mobile contient de nombreuses données, comme votre répertoire de contacts, vos messages, vos photos et vidéos. En cas de perte, de panne ou de vol de votre appareil, vous pourriez ne plus retrouver vos données.
3/C – Seuls les sites ou les magasins officiels vérifient que les applications que vous installez ne sont pas piégées.
4/A – 2 B – 1 C – 3

SÉCURITÉ DES USAGES PRO / PERSO

1/ Bonnes pratiques

Parmi les propositions, quelles sont les deux bonnes pratiques à mettre en œuvre pour sécuriser au mieux mes usages numériques pro/perso ?

- ☐ **A** J'utilise des mots de passe différents pour tous les services professionnels ou personnels auxquels j'accède
- ☐ **B** Peu importe l'usage, je n'utilise que mes dossiers professionnels
- ☐ **C** Au travail, je mélange fichiers personnels et professionnels
- ☐ **D** Je ne mélange pas mes messages pro et perso dans ma messagerie personnelle

2/ Vrai ou Faux

J'ai le droit de m'exprimer sur mon travail ou mon entreprise sur les réseaux sociaux lorsque j'utilise mon ordinateur personnel.

☐ **Vrai** ☐ **Faux**

3/ Cherchez l'intrus

Pour protéger mes usages numériques pro/perso :

- ☐ **A** J'utilise un stockage de données professionnelles distinct du stockage de données personnelles
- ☐ **B** J'utilise ma connexion professionnelle uniquement pour mes besoins professionnels
- ☐ **C** J'utilise mon matériel professionnel pour des besoins personnels
- ☐ **D** J'effectue les mises à jour de mes systèmes très régulièrement

4/ Reliez les situations à leurs solutions

Je suis à la maison et je consulte mes messages professionnels **A** ☐
Je stocke des documents professionnels sur un service en ligne personnel **B** ☐
Je réalise parfois des téléchargements illégaux depuis mon ordinateur professionnel **C** ☐

- ☐ **1** Je demande l'autorisation à mon employeur et prends des mesures de sécurité supplémentaires
- ☐ **2** Je ne le fais qu'à partir de mon ordinateur professionnel
- ☐ **3** Mon entreprise pourrait contrôler mon utilisation de la connexion Internet professionnelle et se retourner contre moi

RÉPONSES

1/A et D
2/VRAI – Uniquement si vos propos ne portent pas préjudice à l'entreprise. Dans le cas contraire, vous risqueriez des poursuites judiciaires.
3/C – Bien que l'utilisation d'une connexion Internet professionnelle à des fins personnelles soit tolérée, gardez à l'esprit que votre utilisation peut mettre en cause votre entreprise. Elle pourrait se retourner contre vous si vous commettiez des actes répréhensibles. Par ailleurs, votre entreprise est en droit de contrôler votre utilisation de la connexion qu'elle met à votre disposition.
4/A – 2 B – 1 C – 3

DOCUMENT RÉALISÉ AVEC NOS MEMBRES : cpme CONFÉDÉRATION DES PME — France Victimes — UFC Que Choisir