HAMEÇONNAGE
TESTEZ-VOUS !

Êtes-vous capable de faire un sans-faute sur la cybersécurité ?
Plusieurs réponses sont parfois possibles.

Q1- 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

Q2- Vrai ou Faux. Il est inutile de déposer plainte pour un message d'hameçonnage auquel j'ai répondu.

A- Vrai
B- Faux

Q3- 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 fournir toute information sur un site, je vérifie son adresse afin de m'assurer que je suis sur un site légitime
D- Je ne communique jamais d'informations sensibles par téléphone ou messagerie électronique

Q4- 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 -B mon numéro de carte bancaire	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

Du 1er au 31 octobre 2024
Devenez #CyberEngagés

Besoin de conseils ou d'assistance ?
Ayez le réflexe : Cybermalveillance.gouv.fr

PIRATAGE DE COMPTE
TESTEZ-VOUS !

Êtes-vous capable de faire un sans-faute sur la cybersécurité ?
Plusieurs réponses sont parfois possibles.

Q1- Bonnes pratiques. Parmi les propositions, quelles sont les trois bonnes pratiques à mettre en œuvre pour éviter le piratage de compte en ligne ?

A- J'utilise des mots de passe complexes et différents pour chaque site et application
B- Je ne fais jamais mes mises à jour
C- Je ne communique jamais mes mots de passe à un tiers
D- J'active la double authentification lorsqu'elle est disponible

Q2- Vrai ou Faux. Si votre boîte mail est piratée, il est utile de prévenir tous vos contacts

A- Vrai
B- Faux

Q3- Cherchez l'intrus. Parmi ces bonnes pratiques, quel est l'intrus :

A- J'applique de manière régulière et systématique mes mises à jour système et logiciels
B- J'utilise les réseaux WiFi publics en toute confiance
C- J'installe un antivirus et je vérifie qu'il fonctionne
D- J'évite les sites illicites ou non sûrs

Q4- Reliez les situations à leurs solutions :

Mon compte vient d'être piraté et je n'arrive plus à m'y connecter -A	1- Je n'ouvre pas la pièce jointe
Je viens de recevoir un e-mail suspect contenant une pièce jointe -B	2- Je change sans tarder le mot de passe du compte piraté sur tous les sites et comptes sur lesquels je l'utilisais
Je suis victime d'un piratage de l'un de mes comptes -C	3- Je me déconnecte systématiquement après chaque utilisation pour éviter que quelqu'un puisse y accéder après moi
J'ai fini d'utiliser mon compte -D	4- Je contacte le service concerné pour signaler le piratage et demander la réinitialisation de mon mot de passe

RÉPONSES

1/ A, C et D
2/ VRAI – Il faut prévenir tous vos contacts pour qu'ils ne soient pas victimes à leur tour des cybercriminels qui les contacteraient en usurpant votre identité.
3/ B – En effet, les réseaux Wifi publics sont souvent mal sécurisés et peuvent parfois être contrôlés voire usurpés par des cybercriminels.
4/ A4 B1 C2 D3

Du 1er au 31 octobre 2024
Devenez #CyberEngagés

Besoin de conseils ou d'assistance ?
Ayez le réflexe : Cybermalveillance.gouv.fr

RÉSEAUX SOCIAUX
TESTEZ-VOUS !

Êtes-vous capable de faire un sans-faute sur la cybersécurité ?
Plusieurs réponses sont parfois possibles.

Q1- Bonnes pratiques. Parmi les propositions, quelles sont les deux bonnes pratiques à mettre en œuvre pour éviter le piratage de compte ?

A- J'utilise des mots de passe complexes
B- J'utilise le même mot de passe sur tous mes réseaux sociaux car c'est plus simple à retenir
C- J'active la double authentification
D- Ce n'est pas utile de sécuriser mes réseaux sociaux car seuls mes amis peuvent voir mon profil

Q2- Vrai ou Faux. Je peux publier ce que je veux sur Internet si j'utilise un pseudonyme.

A- Vrai
B- Faux

Q3- Cherchez l'intrus. Quelles sont les bonnes pratiques d'utilisation des réseaux sociaux :

A- Je fais preuve de discernement lorsque j'évoque mon travail car cela pourrait me porter préjudice ainsi qu'à mon entreprise
B- Sur les réseaux sociaux, je peux m'exprimer sans crainte que mes propos soient interprétés ou rediffusés
C- Je suis vigilant sur les contenus partagés par mes contacts, qui peuvent publier des contenus malveillants à leur insu
D- Je vérifie régulièrement qu'il n'y a aucune connexion sur mon compte depuis un appareil inconnu

Q4- Reliez les situations à leurs solutions :

Je n'utilise plus mon compte de réseau social -A

Je publie régulièrement sur les réseaux sociaux -B

En cas de publication gênante -C ou compromettante sur les réseaux sociaux

Je souhaite restreindre la visibilité -D de mes informations personnelles et de mes publications

1- En faisant preuve de discernement et sans diffuser d'informations personnelles

2- Je le supprime pour éviter que mon compte soit utilisé à mon insu ou que mes informations ne soient récupérées par des tiers

3- Je vais régler la configuration de mon compte dans les paramètres

4- Je demande la suppression du contenu au réseau social concerné

RÉPONSES

4/A2 B 1 C4 D3

3/ B – Même dans un cercle que l'on pense restreint, vos publications peuvent vous échapper et être rediffusées ou interprétées au-delà de ce que vous envisagiez

2/ FAUX – Internet n'est pas une zone de non-droit et l'anonymat n'y est pas absolu : les propos incitant à la haine ou à la violence, la pédophilie, le cyberharcèlement, l'atteinte au droit à l'image ou au droit d'auteur… sont punis par la loi.

1/ A et C

Du 1er au 31 octobre 2024
Devenez #CyberEngagés

Besoin de conseils ou d'assistance ?
Ayez le réflexe : Cybermalveillance.gouv.fr

JUIN 2024 - QUIZ RÉSEAUX SOCIAUX

SÉCURITÉ DES APPAREILS MOBILES
TESTEZ-VOUS !

Êtes-vous capable de faire un sans-faute sur la cybersécurité ?
Plusieurs réponses sont parfois possibles.

Q1- Bonnes pratiques. Parmi les propositions, quelles sont les deux bonnes pratiques à mettre en œuvre pour assurer au mieux la cybersécurité de vos appareils mobiles ?

A- Je ne fais jamais fonctionner le Wi-Fi 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

Q2- Vrai ou Faux. Je n'ai pas besoin de faire des sauvegardes de mon téléphone.

A- Vrai
B- Faux

Q3- 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

Q4- Reliez les situations à leurs solutions :

Je travaille régulièrement à l'extérieur -A	1- Je bloque ma ligne en appelant mon opérateur et mon téléphone en communiquant mon code IMEI et je dépose plainte
J'ai perdu ou je me suis fait voler -B mon téléphone	2- J'évite de me connecter à un réseau Wi-Fi public
Je télécharge un jeu sur mon téléphone -C	3- Je n'autorise pas l'accès à mes photos, mes contacts et mes messages

RÉPONSES

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

Du 1er au 31 octobre 2024
Devenez #CyberEngagés

Besoin de conseils ou d'assistance ?
Ayez le réflexe : Cybermalveillance.gouv.fr

SÉCURITÉ DES USAGES PRO/PERSO
TESTEZ-VOUS !

Êtes-vous capable de faire un sans-faute sur la cybersécurité ?
Plusieurs réponses sont parfois possibles.

Q1- 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

Q2- 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.

A- Vrai
B- Faux

Q3- 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

Q4- Reliez les situations à leurs solutions :

Je suis à la maison et je consulte mes messages professionnels -A	1- Je demande l'autorisation à mon employeur et prends des mesures de sécurité supplémentaires
Je stocke des documents professionnels sur un service en ligne personnel -B	2- Je ne le fais qu'à partir de mon ordinateur professionnel
Je réalise parfois des téléchargements illégaux depuis mon ordinateur professionnel -C	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 l'utilisation de la connexion qu'elle met à votre disposition.
4/ A – 2 B – 1 C – 3

Du 1er au 31 octobre 2024
Devenez #CyberEngagés

Besoin de conseils ou d'assistance ?
Ayez le réflexe : Cybermalveillance.gouv.fr

GÉRER SES MOTS DE PASSE
TESTEZ-VOUS !

Êtes-vous capable de faire un sans-faute sur la cybersécurité ?
Plusieurs réponses sont parfois possibles.

Q1- Bonnes pratiques. 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

Q2- Vrai ou Faux. J'ai un mot de passe très sécurisé. Je peux donc l'utiliser sur tous mes comptes et services.

A- Vrai
B- Faux

Q3- 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 mémotechnique

Q4- 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

4/A – 2 B – 3 C – 1

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.

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.

Du 1er au 31 octobre 2024
Devenez #CyberEngagés

Besoin de conseils ou d'assistance ?
Ayez le réflexe : Cybermalveillance.gouv.fr