INTERNET PANI BOBO !! CARNAVAL 2022

ACADÉMIE
DE MARTINIQUE
Liberté
Égalité
Fraternité

Mot de passe

1/ Bonnes pratiques

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

- [x] Choisir un mot de passe suffisamment complexe
- [x] Utiliser un mot de passe différent pour chaque accès

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/ Vrai ou Faux

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

- (•) 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/ Cherche l'intrus

Un mot de passe sécurisé :

- (•) est facile (suite logique, le prénom de mes enfants, ma date de naissance, etc.)

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/ Donne les solutions correspondantes aux situations

Je ne me souviens jamais de mes mots de passe.

- (•) Je fais confiance à Keepass, mon gestionnaire de mots de passe.

Je soupçonne qu'un de mes comptes ait été piraté.

- (•) Je change immédiatement de mot de passe.

Je travaille sur un ordinateur à la bibliothèque.

- (•) Je n'enregistre pas les mots de passe et me déconnecte après utilisation.

Hameçonnage

1/ Bonnes pratiques

Sur mon compte bancaire, je découvre une dépense 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, quelle(s) est(sont) la(es) bonne(s) pratique(s) à mettre en œuvre ?

- [x] Je vérifie auprès de ma banque l'origine du débit et fais opposition à celui-ci.
- [x] 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.

- (•) 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/ Cherche l'intrus

Comment se prémunir de l'hameçonnage ?

- (•) Je vérifie qu'il y ait bien un logo officiel dans le message reçu.

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/ Donne les solutions correspondantes aux situations

J'ai malencontreusement communiqué mon numéro de carte bancaire.

- (•) Je fais opposition auprès de ma banque et je dépose plainte.

J'identifie une adresse de site d'hameçonnage.

- (•) Je la signale à Phishing-Intiative (https://phishing-initiative.fr/).

Mon adresse de messagerie a été usurpée.

- (•) Je change immédiatement de mot de passe.

Sécurité des appareils mobiles

1/ Bonnes pratiques

Parmi les propositions, quelle(s) est(sont) la(es) bonne(s) pratique(s) à mettre en œuvre pour assurer au mieux la sécurité numérique de tes appareils mobiles ?

- [x] Je mets régulièrement mes appareils à jour.
- [x] Je les verrouille avec un code d'accès difficile à deviner.

2/ Vrai ou Faux

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

- (•) 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/ Cherche l'intrus

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

- (•) sur n'importe quel autre site.

Seuls les sites ou les magasins officiels vérifient que les applications que vous installez ne sont pas piégées.

4/ Donne les solutions correspondantes aux situations

Je travaille régulièrement à l'extérieur.

- (•) J'évite de me connecter à un réseau Wi-Fi public.

J'ai perdu ou je me suis fait voler mon téléphone.

- (•) Je bloque ma ligne en appelant mon opérateur. Je bloque mon téléphone en communiquant mon code IMEI à mon opérateur. Je dépose plainte.

Je télécharge un jeu sur mon téléphone.

- (•) Je n'autorise pas l'accès à mes photos, mes contacts et mes messages.

Sécurité des usages pro / perso

1/ Bonnes pratiques

Parmi les propositions, quelle(s) est(sont) la(es) bonne(s) pratique(s) à mettre en œuvre pour sécuriser au mieux mes usages numériques pro/perso ?

- [x] J'utilise des mots de passe différents pour tous les services professionnels ou personnels auxquels j'accède.
- [x] 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

Uniquement si vos propos ne portent pas préjudice à l'entreprise. Dans le cas contraire, vous risqueriez des poursuites judiciaires.

3/ Cherche l'intrus

Pour protéger mes usages numériques pro/perso :

- (•) J'utilise mon matériel professionnel pour des besoins personnels.

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/ Donne les solutions correspondantes aux situations

Je suis à la maison et je consulte mes messages professionnels.

- (•) Je ne le fais qu'à partir de mon ordinateur professionnel.

Je stocke des documents professionnels sur un service en ligne personnel.

- (•) Je demande l'autorisation à mon employeur et prends des mesures de sécurité supplémentaires.

Je réalise parfois des téléchargements illégaux depuis mon ordinateur professionnel.

- (•) Mon entreprise pourrait contrôler mon utilisation de la connexion Internet professionnelle et se retourner contre moi.

Arnaque au faux support technique

1/ Bonnes pratiques

Parmi les propositions, quelle(s) est(sont) la(es) bonne(s) pratique(s) à mettre en œuvre lorsqu'il m'est proposé un support technique suite à un ralentissement de mon ordinateur ?

- [x] Refuser tout paiement demandé.
- [x] Signaler l'arnaque.

2/ Vrai ou Faux

Après une tentative d'arnaque au faux support technique, il est judicieux d'en profiter pour changer ses mots de passe.

- (•) Vrai

3/ Cherche l'intrus

Pour me protéger des tentatives d'arnaque au faux support technique, je dois :

- (•) mettre à jour mon antivirus régulièrement.

4/ Reconstitue correctement les phrases :

En cas d'attaque au faux support technique, je dois entrer en contact avec...

- (•) ... le site Cybermalveillance (https://www.cybermalveillance.gouv.fr/) pour signaler l'arnaque.

En cas d'attaque au faux support technique, je ne dois pas entrer en contact avec.

- (•) ... le site proposant une intervention à distance pour réparer.

En cas d'attaque au faux support technique, il faut supprimer...

- (•) ... le cache de son navigateur Internet.

Questions supplémentaires

1/ Ton avis

Selon toi, quel est le meilleur mot de passe parmi cette liste :

- crk8mHDBUZ/

Un mot de passe doit comporter les différents types de caractères : lettres minuscules, lettres majuscules, chiffre, caractères spéciaux. Il ne doit pas être facile à trouver (date de naissance…). Dans le cas de la question, tous correspondent à ces critères mais deux sont reconnaissables car « logique » (à éviter). Dans les deux autres propositions, une suit les caractères du clavier. C'est donc celle qui est totalement aléatoire qui est la meilleure proposition de mot de passe.

2/ Vrai ou Faux

Il n'est pas très important de mettre un mot de passe pour accéder à mes équipements mobiles (smartphone, ordinateur, tablette…).

- Faux

En cas de perte ou de vol, ce mot de passe sera le dernier rempart à vos données.