Cybermois/s 2021

Quiz élaboré par le ministère de l'agriculture et de l'alimentation

à destination des apprenants de l'enseignement agricole

MINISTÈRE
DE L'AGRICULTURE
ET DE L'ALIMENTATION
Liberté
Égalité
Fraternité

Document pédagogique associé au quiz

Question 1 : Protéger la sécurité du smartphone et de la tablette

Au lycée, vous allez avoir besoin aujourd'hui de votre smartphone/tablette pour faire des recherches pour le prochain cours de SVT. Pour votre emploi du temps tout au long de la journée, vous décidez de :

A) Activer le verrouillage automatique de votre appareil après une courte période d'inactivité

B) Laisser le Bluetooth et le Wi-Fi activés pour gagner du temps

C) Faire la mise à jour du système d'exploitation et des applications que vous allez utiliser dans le magasin de confiance (App/Play/Store)

A ☐ ; B ☐ ; C ☐ ;

Les bonnes réponses sont A+C.

En verrouillant votre smartphone/tablette, vous évitez qu'une personne ait accès à vos données, notamment si vous avez oublié ou perdu votre smartphone.

Il est à noter que ce type de matériel doit être mis à jour régulièrement pour le maintenir en bonne sécurité (système d'exploitation et applications), comme un ordinateur.

En déplacement, il est vivement conseillé de désactiver les connexions inutiles Wi-Fi, Bluetooth, NFC qui pourraient permettre de voler vos données.

Ne les activer que si nécessaire.

☺ Je protège mon smartphone et ma tablette

*Qu'il s'agisse du **code de déverrouillage** ou du **code PIN**, ces protections complémentaires empêcheront une personne malintentionnée de pouvoir se servir facilement de votre appareil si vous en perdez le contrôle (perte, vol, abandon) et donc d'accéder à vos informations. Bien entendu, vos codes d'accès doivent être suffisamment difficiles à deviner (évitez 0000 ou 1234, par exemple).*

*Activez également le **verrouillage automatique** de votre appareil afin que le code d'accès soit demandé au bout de quelques minutes si vous laissez votre appareil sans surveillance.*

✋ **Les 10 bonnes pratiques à adopter pour la sécurité de vos appareils mobiles**

https://www.cybermalveillance.gouv.fr/medias/2019/11/Memo_appareils-mobiles.pdf

Pour aller plus loin, testez vos compétences numériques en matière de Protection et sécurité grâce à Pix, le service public en ligne pour évaluer, développer et certifier ses compétences numériques : https://pix.fr/

Question 2 : Séparer les usages professionnel/scolaire/personnel

Un ami vous remet une clé USB contenant un film que vous voulez absolument voir.

Ayant du temps à midi, vous décidez d'aller en salle informatique pour le visionner :

A) Vous branchez la clé sur un des ordinateurs de votre établissement

B) Vous la branchez sur un ordinateur de l'établissement puis vous l'analysez à l'aide de l'anti-virus

C) Vous la branchez sur votre ordinateur personnel puis vous l'analysez avant le visionnage

A ☐ ; B ☐ ; C ☐ ;

La bonne réponse est C.

Il est formellement interdit d'insérer dans le port USB d'un ordinateur professionnel ou partagé en salle dans votre établissement une clé USB, un disque dur, un smartphone ou tout autre matériel dont vous ne maîtrisez pas le contenu et l'intégrité.

En effet, il peut être porteur de virus ou de logiciel malveillant.

Ce virus ou logiciel malveillant pourrait en effet se propager ensuite sur le réseau de l'établissement, une fois l'ordinateur connecté sur le réseau.

☺ Je sépare mes usages professionnel, scolaire et personnel

Le développement des technologies mobiles (PC portables, tablettes, smartphones) offre désormais la possibilité d'accéder, depuis presque n'importe où, à ses informations personnelles mais aussi à son système informatique professionnel : la frontière numérique entre la vie professionnelle et personnelle devient de plus en plus poreuse.

Face à cette évolution, il est nécessaire d'adapter ses pratiques afin de protéger tant son entreprise/établissement que son espace de vie privée.

✋ **Les 10 bonnes pratiques à adopter pour la sécurité de vos usages pro-sco-perso, cliquez sur le lien suivant**

https://www.cybermalveillance.gouv.fr/medias/2019/11/memo_usages_pro_perso.pdf

Pour aller plus loin, testez vos compétences numériques en matière de Protection et sécurité grâce à Pix, le service public en ligne pour évaluer, développer et certifier ses compétences numériques : https://pix.fr/

Question 3 : Déplacement – Nomadisme / réseaux Wifi

Les vacances scolaires commencent ce soir. Vous quittez votre internat pour aller prendre votre train et rejoindre votre famille en région toulousaine.

A la gare, vous vous rendez compte avoir oublié d'envoyer la dernière version de votre rapport de stage suite aux remarques de votre référent. Vous vous connectez sur votre ordinateur pour l'envoyer. Pour protéger vos communications sur ce réseau public, vous devez toujours :

A) Trouver le réseau avec le plus fort signal wifi

B) Trouver une connexion wifi a accès libre, sans authentification

C) Utiliser systématiquement le réseau 4g/5g en partage de connexion avec votre téléphone personnel

A ☐ ; B ☐ ; C ☐ ;

La bonne réponse est C.

Que ce soit dans un cadre professionnel ou personnel, l'utilisation des outils numériques ne cesse de croître et de se diversifier. Ordinateurs de bureau ou portables, téléphones mobiles, tablettes, objets connectés... Ils font de plus en plus partie de notre quotidien. Cette intensification des usages représente pour les cybercriminels une opportunité de développer leurs attaques.

Le réseau 4G/5G des opérateurs mobiles permet à un utilisateur nomade de bénéficier d'Internet et de connexions à des applications ou des sites Internet en toute sécurité, depuis n'importe où, même depuis son domicile.

Evitez de vous connecter aux réseaux non maîtrisés (Wi-Fi d'hôtel, de gare, d'aéroport ou de café, bornes de recharge en libre-service, etc.).

☺ Je sécurise l'utilisation de mes outils **numériques en mode nomade**

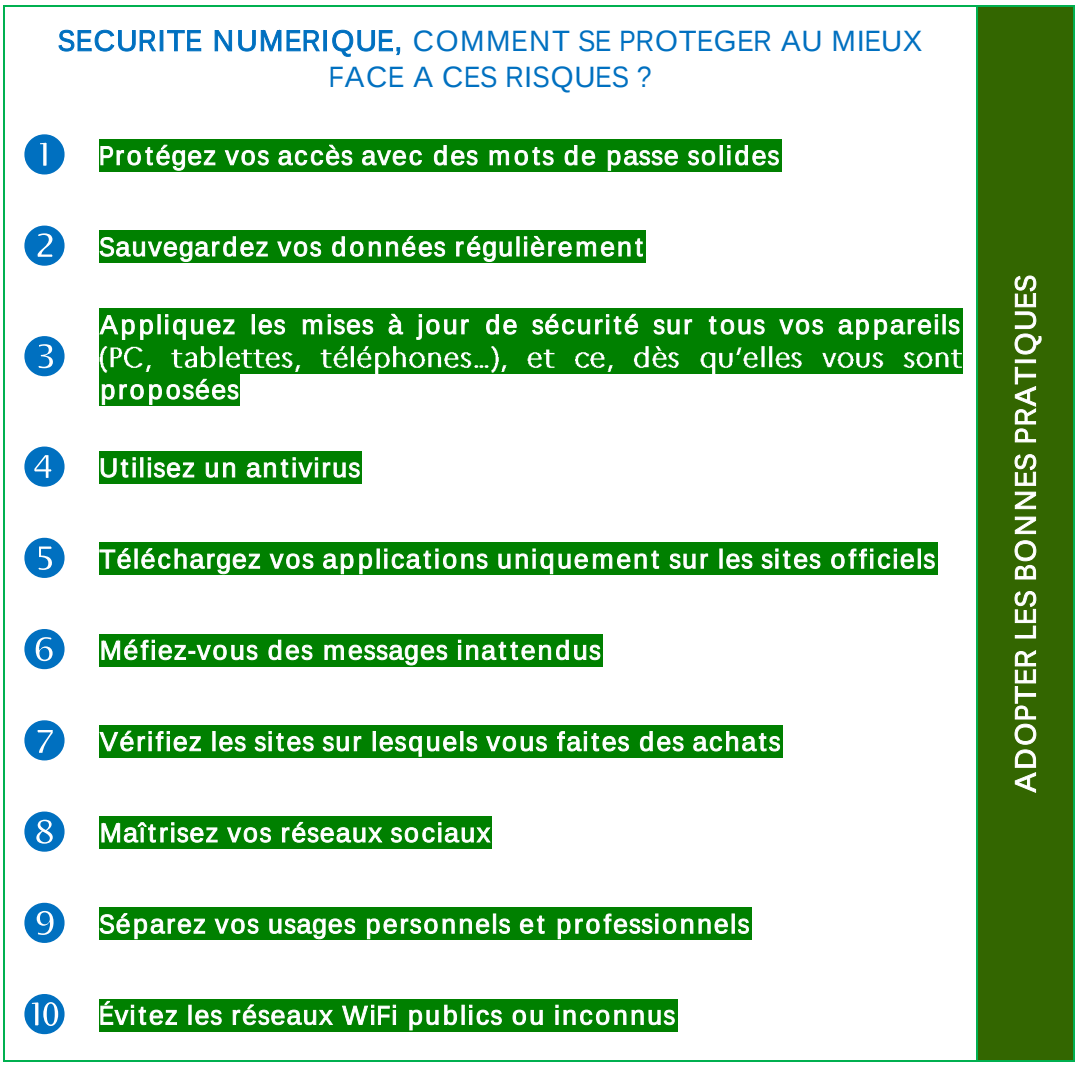
Les réseaux WiFi publics sont souvent mal sécurisés, et peuvent être contrôlés ou usurpés par des pirates qui pourraient ainsi voir passer et capturer vos informations personnelles ou confi-dentielles (mots de passe, numéro de carte bancaire...).

Quand vous le pouvez, privilégiez la connexion privée 3G ou 4G associée à votre abonnement mobile.

Si vous n'avez d'autre choix que d'utiliser un WiFi public, veillez à ne jamais y réaliser d'opérations sensibles (paiement par carte bancaire, etc.) et utilisez si possible un réseau privé virtuel (VPN).

✋ **Les 10 bonnes pratiques à adopter vous protéger sur Internet**

https://www.cybermalveillance.gouv.fr/tous-nos-contenus/actualites/les-10-regles-de-base-pour-la-securite-numerique



Pour aller plus loin, testez vos compétences numériques en matière de Protection et sécurité grâce à Pix, le service public en ligne pour évaluer, développer et certifier ses compétences numériques : https://pix.fr/

Question 4 : Les mots de passe

Vous devez vous identifier pour accéder à l'un de vos comptes (messagerie, application, internet…) :

A) Vous choisissez un mot de passe que vous utilisez déjà pour d'autres usages (messagerie personnelle, réseaux sociaux…)

B) Vous utilisez un mot de passe de 6 caractères se trouvant dans le dictionnaire ou correspondant à votre date de naissance.

C) Vous utilisez un mot de passe complexe d'au moins 8 caractères que vous écrivez sur un post-it pour qu'il soit accessible rapidement et utilisé également par une autre personne en cas de besoin.

D) Vous utilisez un mot de passe d'au moins 8 caractères, possédant lettres majuscules, minuscules, chiffres et caractères spéciaux. Vous ne le notez pas, car vous êtes sûr de vous en rappeler via un moyen mnémotechnique.

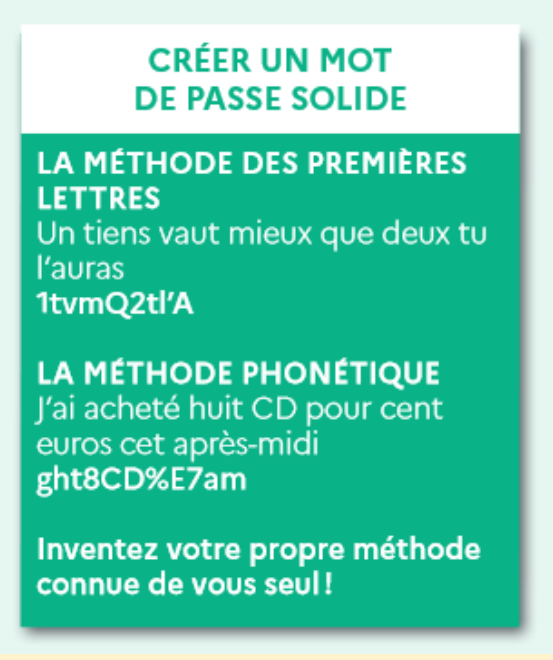
A ☐ ; B ☐ ; C ☐ ; D ☐ ;

La bonne réponse est D.

Le mot de passe est pour un usage unique et personnel, il ne peut être partagé.

Il doit être complexe, choisi de façon à pouvoir le retrouver via un moyen mnémotechnique tout en construisant un mot de passe robuste.

Tout appareil mobile (téléphone, tablette, etc.) doit être sécurisé par un verrouillage système ainsi que par un code PIN.



☺ Je gère mes mots de passe

Messageries, réseaux sociaux, banques, administrations et commerces en ligne, réseaux et applications d'entreprise… la sécurité de l'accès à tous ces services du quotidien repose aujourd'hui essentiellement sur les mots de passe. Face à leur profusion, la tentation est forte d'en avoir une gestion trop simple. Une telle pratique serait dangereuse, car elle augmenterait considérablement les risques de compromettre la sécurité de vos accès.

Des mots de passe différents doivent être utilisés pour tous les services professionnels et personnels auxquels vous accédez.

✋ **Les 10 bonnes pratiques à adopter pour pour gérer efficacement vos mots de passe**

https://www.cybermalveillance.gouv.fr/medias/2019/11/Memo_mots-de-passe.pdf

Pour aller plus loin, testez vos compétences numériques en matière de Protection et sécurité grâce à Pix, le service public en ligne pour évaluer, développer et certifier ses compétences numériques : https://pix.fr/

Question 5 : Phishing, Spam, Ransomware

Vous venez de recevoir un message sur votre messagerie provenant d'une personne dont l'adresse est prenom.nom@educagri.fr ou gmail.com :

« Cher utilisateur,

Nous avons remarqué des activités de connexion inhabituelles autour de votre e-mail.

Veuillez cliquer ici pour examiner les activités de votre compte et mettre à jour votre sécurité.

Le fait de ne pas cliquer sur le lien ci-dessus entraînera la fermeture définitive de votre compte de messagerie.

Cordialement

Bureau d'aide »

A) Vous êtes sûr de la légitimité de l'adresse interne inscrite dans le mail et vous cliquez sur le lien

B) Vous l'envoyez à un autre élève pour avis et afin qu'il teste le lien

C) Vous ne cliquez pas sur le lien et transférez ce message au service informatique de l'établissement ou sur la plateforme « cybermalveillance.gouv.fr »

D) Vous ne répondez pas aux messages qui demandent de transmettre des données professionnelles ou personnelles

A ☐ ; B ☐ ; C ☐ ; D ☐ ;

La bonne réponse est C+D.

Un message avec une adresse en @gmail.com ou @educagri.fr ne possède pas pour autant une garantie d'authenticité. L'émetteur a pu lui-même être piraté ou bien on a usurpé son identité pour récupérer des données et envoyer des messages frauduleux.

La messagerie constitue la porte d'entrée favorite de toutes sortes d'indésirables :

- L'hameçonnage (***phishing*** en anglais) est une technique frauduleuse destinée à leurrer l'internaute pour l'inciter à communiquer des données personnelles (comptes d'accès, mots de passe…) et/ou bancaires en se faisant passer pour un tiers de confiance.
- Les rançongiciels (*ransomwares* en anglais) sont des logiciels malveillants qui bloquent l'accès à l'ordinateur ou à des fichiers en les chiffrant et qui réclament à la victime le paiement d'une rançon pour en obtenir de nouveau l'accès.

Dans tous les cas, si vous avez cliqué sur le lien, déconnectez la prise réseau de votre ordinateur et n'éteignez pas votre ordinateur puis prévenez rapidement votre informaticien.

☺ Je suis vigilant face à tout message douteux

La messagerie constitue la porte d'entrée favorite de toutes sortes d'indésirables : courriels non sollicités (spams), tentatives d'hameçonnage (phishing) ou de rançongiciel (ransomware). Ces menaces ont plusieurs objectifs : usurpation d'identité, vol, fuite de données ou chiffrement de vos données, voire le chiffrement non désiré d'un serveur bureautique interne.

Dans tous les cas, si vous avez cliqué sur le lien :

Déconnectez la prise réseau de votre ordinateur.

N'éteignez pas votre ordinateur.

Prévenez rapidement votre informaticien.

✋ **La fiche mémo pour savoir comment réagir en** cas d'hameçonnage

https://www.cybermalveillance.gouv.fr/medias/2020/01/Memo_hameconnage.pdf

✋ **La fiche mémo pour savoir comment réagir si** vous êtes victime d'un **rançongiciel**

https://www.cybermalveillance.gouv.fr/medias/2019/11/Memo_rancongiciels.pdf

Pour aller plus loin, testez vos compétences numériques en matière de Protection et sécurité grâce à Pix, le service public en ligne pour évaluer, développer et certifier ses compétences numériques : https://pix.fr/

Question 6 : Règles concernant l'usage d'internet / réseaux sociaux

Vous naviguez sur internet ou sur les réseaux sociaux. Vous êtes au top des abonnés sur votre compte de réseau social, vous avez des amis, des d'amis qui sont du monde entier :

A) Vous n'utilisez pas votre adresse mail d'apprenant (ex. adresse de messagerie d'ENT) pour ouvrir un compte sur la plateforme de streaming que vous préférez. Vous utilisez un compte personnel à part.

B) Vous envoyez vos coordonnées bancaires à cet abonné qui vous « like » si souvent et qui vous a contacté car il n'a plus d'argent pour s'acheter un médicament dont il a absolument besoin

C) Vous n'ouvrez pas de compte sur les réseaux sociaux sans les mettre en privé et n'acceptez un suivi de votre profil de personnes que vous connaissez

D) Vous suivez le compte de votre établissement et n'hésitez pas à partager les informations publiées qui peuvent intéresser vos amis/contacts

A ☐ ; B ☐ ; C ☐ ; D ☐ ;

La bonne réponse est A+C.

On ne communique son adresse professionnelle/d'apprenant uniquement sur les sites institutionnels.

Il est fortement déconseillé de communiquer des informations sur son activité professionnelle/de formation hors de la sphère professionnelle/éducative.

Beaucoup d'adresses personnelles ou professionnelles avec identifiant et mot de passe se retrouvent sur des sites pirates (ou Darknet) et sont revendus contre de l'argent.

Sur les réseaux sociaux ou ailleurs, l'utilisateur doit faire preuve de vigilance, des personnes malveillantes peuvent essayer de récolter des informations afin d'usurper des identités et entrer par ce biais dans le système d'information.

Quand vous parlez de votre formation ou de la vie de votre établissement (ambiance, nouveaux projets…) sur les réseaux sociaux, même si vos propos ne sont pas négatifs, vous ne contrôlez pas vos lecteurs : la rediffusion ou l'interprétation qu'ils peuvent faire de vos informations pourraient nuire à votre établissement.

☺ Je suis vigilant sur les réseaux sociaux

Les réseaux sociaux sont des outils de communication et d'information puissants et facilement accessibles.

Verrouillez votre profil pour que tout ne soit pas public.

Avant de poster, demandez-vous toujours si ce que vous communiquez ne pourra pas vous porter préjudice, ou à votre établissement, si d'aventure vos propos ou messages étaient relayés par une personne malintentionnée.

✋ **Les 10 bonnes pratiques à adopter pour votre sécurité sur les réseaux sociaux**

https://www.cybermalveillance.gouv.fr/medias/2019/11/Memo_reseaux-sociaux.pdf

Pour aller plus loin, testez vos compétences numériques en matière de Protection et sécurité grâce à Pix, le service public en ligne pour évaluer, développer et certifier ses compétences numériques : https://pix.fr/

Question 7 : chantage à l'ordinateur ou webcam piraté

Vous recevez un message instantané (chat) via votre réseau social favori : le contact vous envoie des photos-montages vous représentant. Il vous a filmé à votre insu. Il accepte de ne pas diffuser les photos à vos amis et à vos professeurs si vous lui versez une grosse somme d'argent.

A) Vous comprenez tout de suite que ces photos sont un montage et faites des copies d'écran du compte. Vous faîtes un signalement et vous le bloquez.

B) Avec l'aide de votre frère et de son compte Bitcoin, vous versez la somme demandée pour éviter la diffusion des photos

C) Vous changez vos mots de passe de vos principales messageries et applications

A ☐ ; B ☐ ; C ☐ ;

La bonne réponse est A+C.

Aujourd'hui installés dans les usages personnels des internautes, mais aussi dans les usages professionnels des entreprises qui les utilisent comme vitrine de leur activité, les réseaux sociaux n'échappent pas aux activités malveillantes. Escroquerie, usurpation d'identité, chantage, vol d'informations, cyberharcèlement, désinformation, diffamation… sont autant de dangers auxquels sont confrontés les utilisateurs de ces réseaux.

Les cybercriminels utilisent notamment les réseaux sociaux pour commettre des escroqueries et voler des informations personnelles ou professionnelles. Soyez vigilants, car à leur insu, vos « amis » ou contacts peuvent également vous envoyer ou partager des contenus malveillants, surtout s'ils se sont fait pirater leur compte sans le savoir.

Vous pouvez être contacté par messagerie instantanée, par mail, par des personnes qui tentent d'obtenir de l'argent en vous dévoilant des informations qu'il a pu obtenir sur les réseaux sociaux ou par piratage d'un de vos comptes.

Le cybercriminel annonce avoir des vidéos ou photos compromettantes de la victime réalisées avec sa webcam. Il menace de les publier à ses contacts personnels, ou même professionnels, si la victime ne lui paie pas une rançon. Cette rançon, qui va de quelques centaines à plusieurs milliers d'euros, est souvent réclamée en monnaie virtuelle (généralement en Bitcoin) ou coupon PCS.

QUE FAIRE EN CAS DE PROBLÈME ?

- **Réagir en cas de piratage de votre compte de réseau social** – Les conseils de la CNIL : www.cnil.fr/fr/prevenir-reperer-et-reagir-face-au-piratage-de-ses-comptes-sociaux
- **Demander la suppression d'une publication gênante ou compromettante sur les réseaux sociaux** – Les conseils de la CNIL : www.cnil.fr/fr/publication-genante-sur-les-reseaux-sociaux-signalez-pour-supprimer
- **Signaler une situation de cyber harcèlement** : contacter Net Écoute gratuitement au 0800 200 000 et sur www.netecoute.fr
- **Signaler un contenu illicite sur les réseaux sociaux** – Internet Signalement/Pharos (ministère de l'Intérieur) : www.internet-signalement.gouv.fr

☺ Je sais quoi faire si je suis victime d'une escroquerie, d'un chantage

Les réseaux sociaux sont des outils de communication et d'information puissants et facilement accessibles.

Vous pouvez être contacté par messagerie instantanée, par mail, par des personnes qui tentent d'obtenir de l'argent en vous dévoilant des informations qu'il a pu obtenir sur les réseaux sociaux ou par piratage d'un de vos comptes.

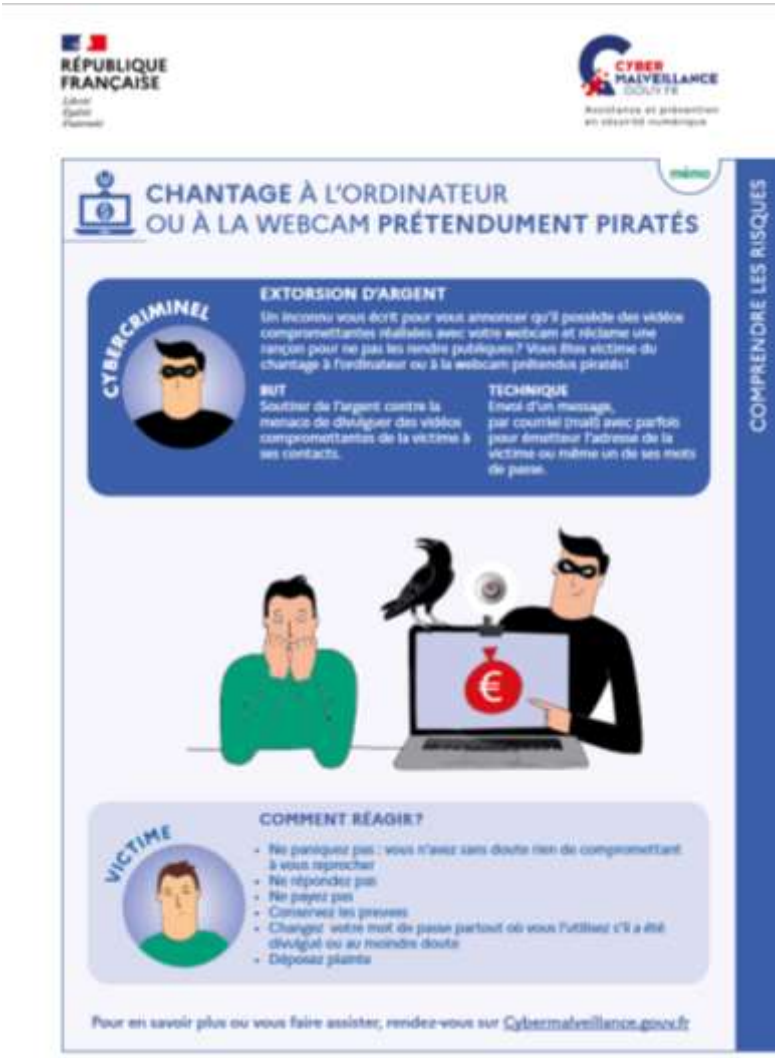
N'envoyez jamais d'argent à quelqu'un sans avoir vérifié son identité au préalable.

N'envoyez jamais de photos ou vidéos intimes à des contacts virtuels qui pourraient en profiter pour vous faire chanter.

Méfiez-vous des jeux concours, des gains inattendus, ou des « super affaires », qui peuvent cacher des escroqueries.

✋ **La fiche mémo pour savoir comment réagir en cas de chantage à** l'ordinateur ou à la **webcam prétendument piraté**

https://www.cybermalveillance.gouv.fr/medias/2020/10/Memo_chantage-webcam.pdf



Pour aller plus loin, testez vos compétences numériques en matière de Protection et sécurité grâce à Pix, le service public en ligne pour évaluer, développer et certifier ses compétences numériques : https://pix.fr/

Question 8 : Protection des données personnelles

Un mineur peut consentir seul à un traitement de ses données à caractère personnel à partir de quinze ans. Fort cette information, vous n'hésitez pas à charger les applications comme vos amis et créez vos comptes en quelques minutes.

Quelles sont vos actions pour profiter au plus vite dans les meilleures conditions de votre application :

A) Vous acceptez toutes les demandes de l'application pour accéder à vos photos, vos contacts, votre localisation, votre adresse, vos données personnelles comme votre date et lieu de naissance…

B) Vous modifiez les paramètres du compte créé pour ne pas partager avec l'application des informations et vous activez le suivi des publications qui peuvent vous mentionnez

C) Vous téléchargez une application sur votre smartphone ou tablette dans un but ludique, sans avis ou recherches préalables

A ☐ ; B ☐ ; C ☐ ;

La bonne réponse est B.

Par défaut, les paramètres de visibilité de vos informations personnelles (numéro de téléphone, adresse email…) et de vos publications sont souvent très ouverts.

Vos données peuvent ainsi être partagées à tous les abonnés d'un réseau social ou partagées avec d'autres applications et sites marchands.

Il est généralement possible de restreindre cette visibilité en réglant la configuration de votre compte, afin de garder la maîtrise de ce que les autres utilisateurs voient de vos informations et de vos activités. Vérifiez régulièrement ces paramètres de confidentialité qui peuvent être modifiés sans que vous ne le sachiez.

☺ Je protège mes données personnelles

Certaines applications proposent d'interagir avec votre compte de réseau social. Il peut s'agir de jeux, de quiz, de programmes alternatifs pour gérer votre compte. Ces applications demandent des autorisations qu'il faut examiner avec attention car une fois données, ces applications peuvent avoir accès à vos informations personnelles, vos contacts, vos publications, vos messages privés, etc.

Ne les installez que depuis les sites ou magasins d'applications officiels.

Si l'application vous semble trop intrusive dans les autorisations qu'elle demande, ne l'installez pas.

Enfin, pensez à désinstaller ces applications ou en révoquer les droits si vous ne vous en servez plus.

✋ **Les 10 bonnes pratiques à adopter pour votre sécurité sur les réseaux sociaux**

https://www.cybermalveillance.gouv.fr/medias/2019/11/Memo_reseaux-sociaux.pdf

Pour aller plus loin, testez vos compétences numériques en matière de Protection et sécurité grâce à Pix, le service public en ligne pour évaluer, développer et certifier ses compétences numériques : https://pix.fr/

Question 9 : Sauvegarde de données

Les 6 derniers mois, j'ai :

A) j'ai sauvegardé mes documents importants sur un support externe à mon ordinateur

B) j'ai téléchargé sur un disque dur externe toutes les informations et données importantes de tous mes appareils (mobile, tablette, ordinateurs…)

C) j'ai mis à jour mon mot de passe de Cloud et augmenté ma capacité de stockage

D) je n'ai pas besoin de sauvegarde

A ☐ ; B ☐ ; C ☐ ; D ☐ ;

La bonne réponse est A et/ou B et/ou C

Toutes les sauvegardes sont utiles pour préserver durablement vos données qu'il s'agisse de documents ou photos.

Dans nos usages personnels ou professionnels, nous utilisons de nombreux appareils numériques pour créer et stocker des informations. Ces appareils peuvent cependant s'endommager ou être endommagés, entraînant une perte, parfois irréversible, de vos données. Afin de prévenir un tel risque, il est fortement conseillé d'en faire des copies pour préserver vos données à long terme.

Si vous êtes victime d'un virus comme un rançongiciel et que votre sauvegarde est connectée à votre ordinateur ou au réseau de votre entreprise, elle peut également être affectée par le programme malveillant qui pourrait la détruire. Déconnectez votre support de sauvegarde de votre ordinateur ou de votre réseau informatique ou mettez-le hors ligne lorsque vous ne l'utilisez plus.

☺ **Je sauvegarde mes données**

En cas de piratage, mais également en cas de panne, de vol ou de perte de votre appareil, la sauvegarde est souvent le seul moyen de retrouver vos données (photos, fichiers, contacts, messages…).

Sauvegardez régulièrement les données de vos PC, téléphones portables, tablettes.

Conservez toujours une copie de vos sauvegardes sur un support externe à votre équipement (clé ou disque USB) que vous débranchez une fois la sauvegarde effectuée.

✋ **Les 10 bonnes pratiques à adopter pour faire vos sauvegardes**

https://www.cybermalveillance.gouv.fr/medias/2019/11/Memo_sauvegardes.pdf

Pour aller plus loin, testez vos compétences numériques en matière de Protection et sécurité grâce à Pix, le service public en ligne pour évaluer, développer et certifier ses compétences numériques : https://pix.fr/

Question 10 : Signalement de cas de cybermalveillance

En cas d'acte de cybermalveillance, je peux :

A) faire un signalement via l'application concernée ou le réseau social en désignant le cybercriminel

B) me former pour apprendre à utiliser en sécurité et avec de bons réflexes des applications, appareils connectés, mobiles, tablettes, ordinateurs

C) Faire un signalement via la plateforme : https://www.internet-signalement.gouv.fr/

A ☐ ; B ☐ ; C ☐ ;

La bonne réponse est A et/ou B et/ou C

Internet est un espace de liberté où chacun peut communiquer, découvrir et s'épanouir. Les droits de chacun, quel que soit son âge, son origine ou ses affinités, doivent y être respectés, pour que la « toile » reste un espace d'échanges et de respect.

Vous pensez être victime d'un acte de cybermalveillance ? Un dispositif conseille et oriente les victimes de cybermalveillance.

Cybermalveillance.gouv.fr a pour missions d'assister les particuliers, les entreprises, les associations, les collectivités et les administrations victimes de cybermalveillance, de les informer sur les menaces numériques et les moyens de s'en protéger.

Ce service est gratuit et délivré exclusivement en ligne au travers d'une plateforme. L'outil d'assistance en ligne va vous permettre de réaliser le diagnostic de votre problème et d'appliquer des conseils adaptés pour y remédier.

Il vous sera également possible, si besoin, de solliciter l'aide d'un professionnel de proximité référencé par le dispositif. Cette prestation est susceptible d'être facturée par le professionnel qui vous assistera.

Vous souhaitez signaler une escroquerie en ligne ou un contenu illicite sur Internet ou bien vous souhaitez porter plainte, cliquez sur le lien suivant

https://www.cybermalveillance.gouv.fr/diagnostic/accueil

QUE FAIRE EN CAS DE PROBLÈME ?

- **Réagir en cas de piratage de votre compte de réseau social** – Les conseils de la CNIL : www.cnil.fr/fr/prevenir-reperer-et-reagir-face-au-piratage-de-ses-comptes-sociaux
- **Demander la suppression d'une publication gênante ou compromettante sur les réseaux sociaux** – Les conseils de la CNIL : www.cnil.fr/fr/publication-genante-sur-les-reseaux-sociaux-signalez-pour-supprimer
- **Signaler une situation de cyber harcèlement** : contacter Net Écoute gratuitement au 0800 200 000 et sur www.netecoute.fr
- **Signaler un contenu illicite sur les réseaux sociaux** – Internet Signalement/Pharos (ministère de l'Intérieur) : www.internet-signalement.gouv.fr

☺ **Je sais comment réagir si je suis** victime d'un acte de cybermalveillace

Vous pensez être victime d'un acte de cybermalveillance ?

Un dispositif conseille et oriente les victimes de cybermalveillance.

https://www.cybermalveillance.gouv.fr

L'outil d'assistance en ligne va vous permettre de réaliser le diagnostic de votre problème et d'appliquer des conseils adaptés pour y remédier.

Pour aller plus loin, testez vos compétences numériques en matière de Protection et sécurité grâce à Pix, le service public en ligne pour évaluer, développer et certifier ses compétences numériques : https://pix.fr/

Message à l'apprenant en fin de quiz :

« *Bravo ! Tu as participé au cybermoi/s 2021.*

Tu veux être un acteur de ton apprentissage du numérique ? Développe tes compétences numériques en matière de Protection et sécurité grâce à Pix, le service public en ligne pour évaluer, développer et certifier ses compétences numériques : https://pix.fr/

Sur Pix, tu pourras aussi tester tes connaissances sur 4 autres domaines du numérique : Information et données, Communication et collaboration, Création de contenu et Environnement numérique.

La sécurité du numérique ? Tous impliqués ! »