

ACTIVITÉ (DÉCONNECTÉE) - LE GRAND QUIZ : VIE PRIVÉE EN LIGNE

SÉCURITÉ > 4.2 PROTÉGER LES DONNÉES PERSONNELLES ET LA VIE PRIVÉE

CONVIENT POUR	AGE	NIVEAU DE COMPÉTENCE	FORMAT	DROITS D'AUTEUR	LANGUE(S)
Chercheurs d'emploi, Elèves (école secondaire), Jeunes en décrochage scolaire, Tous publics	Adolescents, Adultes, Seniors	Niveau 2	Fiche d'activité	Creative Commons (BY-SA)	Français

Cet atelier sous forme de quiz permet de faire un tour d'horizon des connaissances et bonnes pratiques vues lors des ateliers dédiés aux données personnelles.

Objectif général Connaissances

Temps de préparation pour l'animateur moins d'une 1 heure

Domaine de compétence 4 - Protection de l'identité et des données personnelles

Temps requis pour compléter l'activité (pour l'apprenant) 0 - 1 heure

Nom de l'auteur Nothing 2hide

Matériel supplémentaire Fiches Bristol de 5 couleurs différentes - Stylos

Ressource
originellement créée

Français

DÉROULÉ

1 Introduction

Cet atelier est à proposer à des personnes qui ont déjà participé à un ou plusieurs ateliers sur la thématique des données personnelles et de l'identité numérique. Voyons cela comme un grand oral, mais sous forme de quiz.

Il y aura deux parties. La première est une série de questions en vrai ou faux. La deuxième est composée de quatre thèmes : réseaux sociaux ; ma vie, mes droits ; sous le radar et souriez, vous êtes surveillés.

Au préalable, recopier sur des fiches Bristol les questions. L'idéal est donc d'avoir cinq couleurs différentes de fiche, une pour la première, quatre pour la deuxième (correspondant aux diverses thématiques).

Note à l'animateur.rice : Vous pouvez bien entendu afficher les questions via un vidéoprojecteur, et les adapter à votre sauce !

2 Vrai ou Faux

Poser une question à chaque groupe à tour de rôle, jusqu'à épuisement des questions. Chaque groupe doit simplement répondre vrai ou faux.

Conseil d'animation : Pour faire monter la pression, laisser 10 secondes de temps de réponse (l'équipe adverse peut chronométrer !), vous pourrez lire l'explication supplémentaire en donnant votre réponse.

Chaque bonne réponse vaut un point. Penser à noter les points à chaque fois, c'est important pour la suite, et l'esprit de compétition pourra stimuler les participant.e.s !

Question 1 - Utiliser Tor est illégal.

Faux - il a été développé pour un usage militaire américain, principalement la marine, afin de masquer leurs adresses IP et éviter le vol de données sensibles pendant les missions. Une fois que les militaires sont passés à des systèmes VPN internes hautement anonymes, TOR a été publié en tant que logiciel libre.

Il est donc parfaitement légal de l'utiliser ou de le télécharger.

Question 2 - en communiquant sur WhatsApp, mes données sont sécurisées.

Vrai - WhatsApp, et donc le groupe Facebook qui détient la messagerie ne peuvent pas lire les contenus des messages (messages qui correspondent à nos données personnelles).

Question 3 - en communiquant sur WhatsApp, mes métadonnées sont sécurisées ?

Faux - Facebook a accès aux métadonnées. Il s'agit de tout ce qu'il y a autour de la donnée, donc du contenu du message dans ce cas. Il s'agit donc du numéro de l'expéditeur et du destinataire, de la date et l'heure de l'envoi, etc.

Question 4 - il existe deux principaux types d'attaque pour pirater un mot de passe. Par dictionnaire ou par chiffres arabes.

Faux - les deux types sont par dictionnaire ou par force brute.

Par dictionnaire : le pirate possède des millions de mots de passe dans plusieurs fichiers et un programme les essaye un par un jusqu'à ce qu'il trouve le bon. Il existe des dictionnaires librement téléchargeables classés par langues, métiers, animaux, années, ...

Par force brute : (cette méthode n'a plus le vent en poupe supplantée par le fishing mail) le pirate utilise un logiciel qui va essayer toutes les combinaisons possibles de caractère.

Question 5 - Apple est plus transparent qu'Android en ce qui concerne la collecte et le partage d'informations personnelles.

Faux - Apple pratique la récolte massive de données. L'entreprise est même soupçonnée d'avoir collaboré avec des entreprises comme Facebook pour une collecte plus vaste.

Question 6 - Snapchat peut récupérer mes messages éphémères.

Vrai - Snapchat crée et stocke localement les métadonnées (des données sur des données).

Celles-ci permettraient de récupérer les photos Snapchat expirées. Pour en savoir plus, allez donc lire le billet de blog "Les messages Snapchat sont-ils vraiment supprimés pour toujours ?" Sur Kaspersky.

Question 7 - Avez-vous le droit de réclamer que les décisions fondées sur un traitement automatisé qui vous concernent et qui sont fondées sur vos données soient prises par des personnes physiques et non par des ordinateurs ?

Réponse - Vrai : ils font partie de vos droits fondamentaux cités par la Direction générale de la concurrence, de la consommation et de la répression des fraudes (DGCCRF).

Si jamais les deux équipes sont à égalité, jouer à pile ou face pour la suite. Et oui, la vie est parfois une simple question de hasard, et de chance.

3 Quatre thèmes pour un gagnant

Les fiches sont séparées en quatre thèmes (avec des fiches de quatre couleurs différentes).

L'équipe qui a gagné la première manche du vrai ou faux a le droit de choisir le premier thème. Elle répond à toutes les questions du thème. Puis la deuxième équipe, choisit le thème suivant, et ainsi de suite.

Pour chacune des questions, le groupe a le droit de répondre directement ou de demander une liste de réponses. S'il répond directement, il gagne trois points, s'il demande une liste de réponses, il gagne un point. S'il ne trouve pas la bonne réponse, il ne gagne aucun point.

Voici les questions par thème, avec réponse.

Réseaux sociaux

Question 1 - Suis-je obligé.e de donner mon nom et mon prénom quand je crée un profil (plusieurs choix) ?

A - Tout dépend du site; il faut regarder quelles sont les conditions d'utilisation et les usages

B - Le nom est une obligation

C - Non, on peut très bien utiliser un pseudo

Réponse A - Cela dépend du site. Bien que certains utilisent des subterfuges, Facebook notamment demande à ce que vous mettiez votre nom réel. Si jamais votre compte est signalé et qu'on ne peut pas vérifier votre identité, votre compte peut être suspendu.

Question 2 - Combien de temps cela prend-t-il de lire l'ensemble des conditions générales d'utilisation sur Facebook ?

A - Une journée, on comprend que c'est trop

B - 15 minutes, si j'avais su, je l'aurais fait ! (Ne mentez pas, personne ici ne les a lues)

C - Une heure, bon je pourrais me motiver

Réponse C - Une heure : Alors, qui va le faire ? Notez que le temps de lecture est similaire pour les autres réseaux sociaux. Une version pédagogique existe même pour Instagram (voir la fiche : CGU : [Dans quoi je m'engage ?](#))

Question 3 - Pouvez-vous être licencié.e pour quelque chose que vous avez publié sur les réseaux sociaux ?

A - Non, c'est ma vie privée

B- Oui

C - Seulement si j'attaque personnellement un membre de ma direction

Réponse : B - Oui, cela est possible. Même si votre compte est personnel, vos statuts publics peuvent être vus par tou.te.s, y compris par votre entreprise. Plusieurs types de statuts peuvent être sujet à licenciement. Si vous vous en prenez ou insultez des collègues et membres de la direction, mais bien d'autres. Par exemple, un employé d'une entreprise de jardinage laissait entendre qu'il était parti en vacances, alors qu'il était en arrêt maladie. Son patron, qui a vu le post, n'a à priori pas tellement apprécié.

Question 4 - Vous habitez en France. Où sont stockées vos données Facebook ?

A - En France

B - Aux États-Unis, le pays où se trouve le siège mais aussi tous les serveurs de l'entreprise

C - On ne peut pas vraiment savoir

Réponse- B. Facebook dispose de centres de données dans plusieurs pays à travers le monde. Le fait que vous habitez en France ne l'oblige pas à stocker vos données dans l'Hexagone. Le droit européen lui impose de les stocker soit dans l'Union européenne, soit dans un pays qui a fait l'objet d'une décision d'homologation des autorités de l'UE, soit aux États-Unis, avec lesquels l'Union européenne a noué un

accord, le Privacy Shield.

Question 5 - Parmi les proposition suivantes, la ou lesquelles sont vraies ? Sur Instagram (3 points si toutes les réponses sont justes, 1 point si c'est partiel) :

A - Instagram peut garder tes informations, les utiliser et les partager avec des entreprises connectées au réseau social. Cela inclut ton nom, ton adresse mail, ton école, où tu vis, tes photos, ton numéro de téléphone, tes "likes" et "dislikes", où tu vas, où tes amis vont, combien de fois tu utilises Instagram, ta date d'anniversaire, à qui tu parles ainsi que tes messages privés.

B - Instagram peut supprimer certains de tes posts sans te dire pourquoi.

C - Quand tu supprimes ton compte Instagram, le réseau social garde ces informations personnelles sur toi, tes photos, aussi longtemps que raisonnable dans un but financier.

Réponse : Toutes ! Retrouvez l'ensemble des [Conditions Générales d'utilisation d'Instagram](#) réécrites de manière pédagogique par une avocate.

Question 6 - Que signifie désactiver son compte Facebook ?

A - Je le mets simplement en veille, mais peux me reconnecter à tout moment. Mes données sont gelées mais toujours en ligne.

B - Je gèle mon compte, si je ne me reconnecte pas au bout de 30 jours, mon compte est supprimé et Facebook procède à l'effacement de mes données

C- Un utilisateur de Facebook a signalé mon compte qui a été gelé le temps de faire des vérifications sur mon identité et les contenus que je partage.

Réponse A - Je le mets simplement en veille, mais peut me reconnecter à tout moment. Mes données sont gelées mais toujours en ligne. Le délai de 14 jours est valable lors de la suppression d'un compte. Si vous avez fait la démarche de suppression de votre compte et que vous vous reconnectez dans les deux semaines qui suivent, la démarche est annulée, votre compte ne sera pas supprimé. La réponse C correspond quant à elle à un compte suspendu et non désactivé.

Question 7 - Quand je supprime mon compte Facebook, en combien de temps Facebook efface mes données personnelles ?

A - 9 jours

B- 90 jours

C - 9 mois

Réponse - Le compte sera supprimé sous 14 jours. Facebook vous laisse un laps de temps...si dans ces deux semaines vous vous reconnectez, alors la démarche est annulée et le compte n'est pas supprimé. Attention, il faut bien plus longtemps pour que Facebook efface les données personnelles. Selon lui, il lui faut environ 90 jours pour supprimer tout ce que vous avez publié, comme vos photos, statuts ou autres données stockées (comme votre date de naissance si vous l'avez donnée).

Question 8 - Instagram propose depuis peu à ses utilisateur.rice.s de télécharger toutes leurs données. Qu'est-ce que vous ne pourrez pas trouver dans le dossier que vous pourrez télécharger ? (3 points si toutes les réponses sont justes, 1 point si c'est partiel)

A - l'intégralité des messages privés que vous avez échangés avec vos contacts

B - l'historique de toutes les publications que vous avez « aimées »,

C - l'historique de vos recherches

Réponse : Aucune. Voici tout ce que contiendra votre dossier : les photos et vidéos publiées, les messages privés que vous avez échangés avec vos contacts, l'historique de toutes les publications que vous avez « aimées », celui de vos recherches et la date à laquelle vous vous êtes abonné(e) à vos comptes préférés

Ma vie, mes droits, mes réflexes

Question 1 - Quelle est l'autorité administrative compétente en France pour veiller au respect de la vie privée sur Internet ?

A- La commission nationale de l'informatique et des libertés

B- Le comité du respect des droits et de la vie privée sur Internet

C- Le think tank Mon Internet, ma bataille

Réponse : A - La commission nationale de l'informatique et des libertés (CNIL) est mise en place pour veiller au respect des droits de l'Homme sur le Web.

Question 2 - Je déménage à l'autre bout de la France. Je dois chercher un nouveau logement. Dans cette galère, je décide de créer une nouvelle adresse mail. Pour mon mot de passe, je choisis :

A - c'est une adresse temporaire, je choisis un mot de passe dont je me souviendrai facilement

B - Le mot de passe que j'utilise pour mon autre adresse de messagerie, mieux vaut ne pas l'oublier

C - Je crée une phrase de passe

Réponse : C - Plus c'est long, plus un pirate mettra du temps à trouver votre mot de passe. Il est donc recommandé d'écrire des phrases de passe car elles sont plus faciles à retenir que des mots de passe très compliqués.

Question 3 - Comment appelle-t-on toutes les traces que je laisse sur Internet, composées de mes données personnelles ?

A- L'identité numérique

B - L'identité sociale

C - L'empreinte de Sureau

Réponse A - L'identité numérique. L'identité numérique est l'ensemble des informations que l'on trouve sur Internet vous concernant. C'est donc une identité de "données". Comme dans la vie réelle (ou IRL in real life comme disent les plus geeks d'entre nous), l'identité virtuelle est un mélange entre ce que je veux montrer, ce que je cache volontairement, ce qui m'échappe, et ce que les autres perçoivent de moi (comme quand vous pensez que votre voisine fait toujours la tête, alors qu'elle est très aimable, mais pas de nature à sourire tout le temps !)

Question 4 - Que puis-je faire si le moteur de recherche de Google affiche un contenu me concernant qui ne me plaît pas ?

A - Rien, personne ne peut lutter contre lui

B - Porter plainte (et vous rouler par terre au moment de la déposition)

C - Demander à Google de déréférencer la page

Réponse C - Vous pouvez demander à Google de déréférencer une page vous concernant, mais pas de la supprimer. Google ne peut de toute façon pas le faire : l'entreprise n'en a pas le pouvoir. Si Google

accepte votre demande, la page n'apparaîtra plus dans les résultats de recherche liés à votre nom. Comprenez bien, cette page existe toujours, il sera toujours possible de la retrouver avec d'autres mots-clés par exemple. Surtout, c'est un droit qui existe au sein de l'Union européenne. Cela signifie qu'une personne qui tape votre nom sur Google en dehors des pays de l'UE pourra voir le résultat s'afficher.

Question 5 - Comment appelle-t-on la possibilité de demander des informations qui me concernent auprès d'un organisme, d'une entreprise, etc ?

- A - Le droit de curiosité
- B - Le droit de la maîtrise
- C - Le droit d'accès

Réponse C - Le droit d'accès. Plus d'informations sur le site de la Cnil.

Question 6 - J'ai bien entendu la leçon, et je crée une phrase de passe différente pour tous mes comptes. Je ne fais pas confiance à ma mémoire alors :

- A- Je note tout dans un cahier : le nom du site et le mot de passe associé pour m'y retrouver
- B- J'utilise un générateur de mot de passe, puis je reste connecté.e à mes comptes.
- C - J'utilise un gestionnaire de mot de passe.

Réponse C : Si vous voulez vous aider d'un carnet, alors écrivez simplement le début de la phrase de passe ! Sinon, si quelqu'un vous le dérobe, vous êtes foutu.e.s ! Le générateur de mot de passe est une bonne solution, mais pas si vous restez connecté.e.s. Quant au gestionnaire de mots de passe, on vous le recommande vivement ! Il s'agit d'outils permettant de stocker à un seul endroit tous les mots de passe que vous utilisez. Ils prennent alors la forme d'un logiciel classique ou d'une simple extension dans le navigateur.

Question 7 - Quel nom donne-t-on aux courriers électroniques non souhaités, qui contiennent souvent une pub, et sur lesquels il ne faut surtout pas cliquer ?

- A- Coubelle (contraction de courriel et poubelle)
- B- Contenus sponsorisés
- C - Spam

Réponse C - Spam. Si beaucoup de spams ne sont que de la publicité, certains servent aux

hameçonnages, qui servent à récupérer vos données, et plus largement (quand un virus est installé dans votre appareil) tous vos contenus.

Question 8 - Si je veux modifier des informations présentes sur un site, je dois faire la demande auprès de l'organisme. De combien de temps dispose-t-il pour me répondre ?

A - Vous n'avez pas le droit de demander des modifications, c'est la magie d'Internet

B - Il dispose d'une semaine

C - Il dispose d'un mois

Réponse C - Pour toute demande suppression ou de modification de vos données, le délai est d'un mois maximum pour que l'organisme concerné vous réponde. Une fois ce délai passé, vous pouvez saisir la CNIL.

Souriez, vous êtes surveillé.e.s

Question 1 - Vous apparaissez sur une image Google Street. Pouvez-vous faire quelque chose ?

A - Non, je me trouve au mauvais endroit au mauvais moment

B - Oui, je peux demander à être effacé de l'image mais seulement si cela me porte préjudice (avis à ceux qui se baladent avec leur amant/maitresse)

C - Je peux demander à Google à être flouté

Réponse C - Vous pouvez demander à Google de flouter la partie de l'image dans laquelle vous apparaissez. Dans ce cas, cliquez sur "Signaler un problème", en bas à droite de l'image. Si dans un délai de deux mois, Google n'a pas réagi, vous pouvez vous plaindre auprès de la CNIL.

Question 2 - Que puis-je faire pour que Google ne connaisse pas mes positionnements géographiques ?

A - Je désactive ma position sur mon smartphone

B - Je désactive ma position sur mon smartphone, ainsi que la conservation de l'historique de mes positions

C- Je désactive ma position sur mon smartphone, ainsi que la conservation de l'historique de mes

positions puis pour chaque application que je télécharge, chaque site que je consulte via mon smartphone, je dois refuser l'accès à ma position

Faux - Refuser ou désactiver la conservation de l'historique de géolocalisation dans des applications Google (telles que Google Maps et Google Search) ne suffit pas à empêcher Google de conserver des coordonnées géographiques de l'utilisateur. Le géant peut continuer d'utiliser et enregistrer ponctuellement la position approximative du smartphone à travers des applications. Par exemple quand vous consultez la météo.

Question 3 - Combien de temps peuvent être conservées les images issues de caméra de surveillance ?

A - Un mois (sauf en cas de procédure pénale)

B - Un an (sauf en cas de procédure pénale)

C - Indéfiniment

Réponse A - Les images issues d'une caméra de surveillance peuvent être conservées au maximum pendant un mois. En cas de procédure pénale certaines images peuvent être extraites et conservées uniquement dans ce cadre.

Question 4 - Les services de renseignement ont-ils le droit d'écouter mes conversations téléphoniques ?

A - Oui

B - Non

C - Selon certaines conditions, ils ont le droit

Réponse C - Les services de renseignement peuvent écouter les conversations de certains suspects sans passer par un juge, ou à la demande d'un juge. Sans passer par un juge, on appelle ça les interceptions de sécurité (captation de l'activité sur Internet compris!). La demande est autorisée ou non par le premier ministre après avis d'une commission (les principaux motifs étant la lutte contre le terrorisme et la criminalité organisée), la Commission nationale de contrôle des techniques de renseignement (CNCTR). Quand le juge ordonne une écoute, on appelle les écoutes judiciaires.

Question 4 - Sur Skype, qui, en dehors des deux interlocuteurs, peut avoir accès au contenu d'une conversation ?

A - Google, c'est toujours la faute de Google

B - Facebook, à qui appartient Skype

C - Microsoft, à qui appartient Skype

Skype permet d'avoir une conversation chiffrée avec son ou ses interlocuteurs cependant celle-ci n'est pas chiffrée de bout en bout par défaut : Microsoft dispose des clés de chiffrement et déchiffrement et peut techniquement avoir accès au contenu de votre conversation. Pour avoir une conversation vraiment confidentielle sur Skype il faut utiliser l'option "démarrer une conversation privée".

Question 5 - Dans quel cas mon employeur peut-il utiliser un dispositif de géolocalisation sur mon véhicule professionnel ?

A - Localiser le véhicule en cas de vol

B - Suivre le temps de travail

C - Contrôler le respect des limitations de vitesse

Réponses A et B. Le détail des conditions est à retrouver sur le site de la CNIL, à la page : ["La géolocalisation des véhicules des salariés"](#).

Question 6 - A quoi sert un cookie ?

A - Étudier et cibler les comportements des potentiels acheteurs en ligne

B - A se faire un super goûter (Chocolat-noisettes, mon préféré !)

C - A bloquer les virus de type Cheval de Troie provenant de sites malveillants

Réponse A - Le cookie est un petit fichier texte que les sites web ont l'autorisation de déposer sur votre ordinateur via votre navigateur. Historiquement il a été créé dans les années 1990 par souci de confort pour les internautes et pour pallier les problèmes des premiers sites d'achat en ligne qui en cas d'interruption de connexion vidaient le panier du client. Avec l'évolution des sites marchands, l'utilisation du cookie s'est transformée et la plupart des régies publicitaires les utilisent désormais pour étudier et cibler les comportements des potentiels acheteurs en ligne.

Question 7 - Il existe des moyens de se protéger des trackers publicitaires. Citez un des modules disponibles (3 points, si les participant.e.s ne trouvent pas, proposez les réponses pour 1 point. Les participant.e.s doivent dire celui qui n'est pas un module contre les trackers).

A - PrivacyBadger

B - uBlock

C - VPN

Réponse - C Un VPN n'est pas un module pour bloquer les trackers publicitaires.

Question 8 - Un centre commercial a-t-il le droit de tracer votre mobile pour analyser votre parcours dans les boutiques ?

A - Non mais vous rigolez, je suis dans un pays libre à la fin !

B - Il le peut, le centre commercial est une zone privée, j'accepte ses conditions quand j'y mets un pied

C- Oui, mais il ne peut pas connaître mon identité, et mon consentement doit être très clair

Réponse C - Oui, mais il y a des conditions. Les données émises par le téléphone "doivent être supprimées lorsque son porteur sort du magasin", les données collectées ne doivent pas permettre de pouvoir retrouver l'identité du client, le consentement "préalable et éclairé" du client est nécessaire. Il doit se manifester par une action concrète, par exemple, explique la CNIL, "accoler son téléphone sur un boîtier spécifique" (Citer la source, la CNIL, seulement si la question sur l'entité est déjà passée).

Sous le radar

Question 1 - Que veut dire TOR ?

A - Tools of Rebirth

B - The Onion Router (Le Routeur Oignon)

C - Tout ou rien

Réponse C - The Onion Router.

Question 2 - Que signifie son symbole, l'oignon ?

A - Il représente les couches de protection comme des pelures d'oignon

B - Les informaticiens qui ont créé Tor raffolaient des oignons frits : c'est un hommage à leurs soirées passées ensemble à créer le réseau en grignotant

C - Symbole de puissance dans l'Antiquité, l'oignon représente alors le réseau qui contrecarrera le web en clair

Réponse A - Il représente les couches de protection comme des pelures d'oignon

Question 3 - Sur Protonmail (messagerie sécurisée et chiffrée), tout est chiffré sauf une chose, quelle est-elle ?

A- Les pièces-jointes

B - L'objet du mail

C - L'adresse mail de mon ou mes destinataires

Réponse : B, l'objet du mail. Mieux vaut ne pas mettre d'informations compromettantes dedans !

Question 4 - Les mails chiffrés sont assurés entre utilisateur.rice.s de Protonmail. Il existe un moyen pour envoyer un mail de manière sécurisée depuis mon Protonmail aux réfractaires qui ne se sont pas mis à cette messagerie. Comment faire ?

A - Il faut cliquer sur le cadenas dans ma fenêtre de mail et attribuer un mot de passe à mon destinataire, que je lui envoie de manière chiffrée par un autre moyen

B- Il faut cliquer sur le S (pour secure) dans ma fenêtre de mail et attribuer un mot de passe à mon destinataire, que je lui envoie de manière chiffrée par un autre moyen

C - C'était un piège, il n'y a aucun moyen. Venons tous sur Protonmail et vivons heureux.

Réponse A - Notons que le S de Secure est celui compris dans les adresses web pour signifier qu'il y a une couche de chiffrement.

Question 5 - Quand vos communications n'ont aucune couche de protection, que vous n'avez utilisé aucun outil, logiciel ou moyen de chiffrement pour vous protéger. On dit que vos conversations sont...

- A - En carton
- B - En clair
- C - En light web

Réponse B - En clair. Quand vous utilisez le réseau GSM (donc les textos et les appels directement depuis votre téléphone, vos conversations sont en clair). Quand vous utilisez la 3G/4G, cela dépend de l'application utilisée !

Question 6 - Quelle est l'application la plus sûre aujourd'hui pour communiquer de manière chiffrée ?

- A - Telegram
- B - Snapchat
- C - Signal

Réponse C - Signal ! Pour en savoir plus, allez jeter un oeil sur la fiche : ["Sous le radar: communiquer avec Signal"](#)

Question 7 - Que ne puis-je pas faire avec Signal ?

- A - Créer une conversation de groupe
- B - Envoyer des messages éphémères qui s'effacent après lecture
- C - Recevoir des messages éphémères qui s'effacent après lecture

Réponse - Aucune. Tout est possible. Signal est aussi facile à utiliser et à les mêmes fonctionnalités qu'une application non chiffrée, type WhatsApp.

Question 8 - Comment s'appelle l'option sur Messenger qui promet d'avoir une conversation chiffrée de bout en bout ?

A - Conversation secrète

B - Dark conversation

C - Viva la libertad

Réponse A - c'est la conversation secrète. Nous préconisons tout de même d'utiliser Signal, sait-on jamais.

Maintenant, il n'y a plus qu'à compter les points !!!

4 Pour aller plus loin

Pour mettre en pratique les connaissances sur les données personnelles, inviter les participant.e.s à réaliser des *serious game* chez eux.elles. Ielles seront plongé.e.s dans une mise en situation. Nous conseillons notamment "[Datak](#)" et "[Jaccepte](#)". Compter quelques heures pour chacun, à faire un peu sur plusieurs jours.