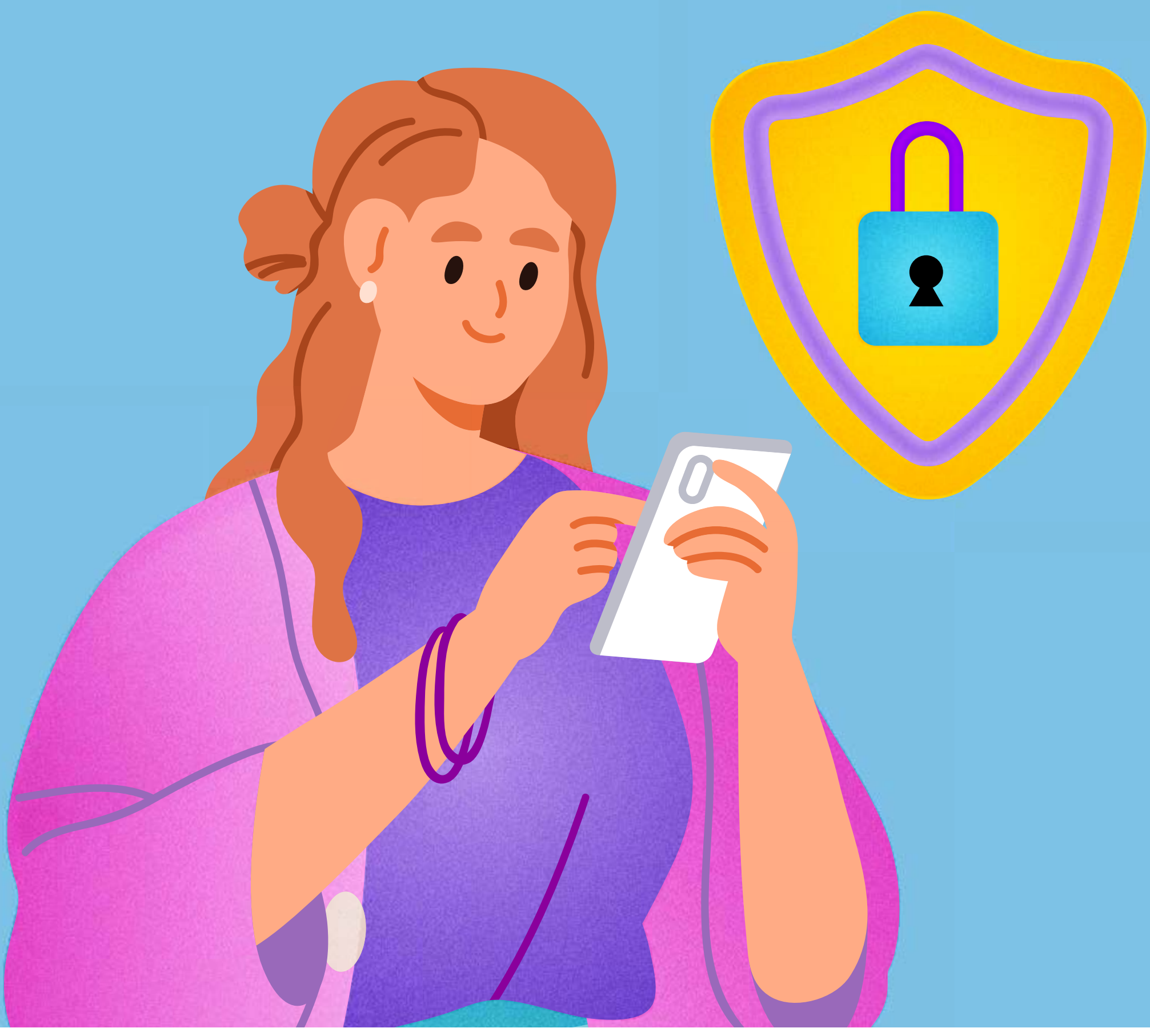
Sécurité Numérique lors d'un avortement

Un guide pour protéger votre confidentialité



CYBER COLLECTIVE

La Pilule

Vous cherchez des informations sur l'avortement, mais vous êtes préoccupée par la confidentialité de vos activités en ligne ?

Vous n’êtes pas seule !

L'accès aux services d'avortement peut s'avérer difficile, particulièrement dans les régions où l'accès est restreint, mais il est essentiel de rester informée et de préserver votre sécurité numérique. Nous avons préparé des conseils pratiques pour vous aider à protéger votre vie privée tout au long du processus.

C'est parti !

1. Recherche de services ou d'informations sur l'avortement en ligne

Il est important de savoir que les navigateurs Internet ne sont pas privés. Les grandes entreprises technologiques enregistrent vos activités en ligne et les utilisent pour vous proposer des publicités ciblées. Ces données peuvent être communiquées aux autorités si elles en font la demande (bien qu'elles aient généralement besoin d'un mandat).

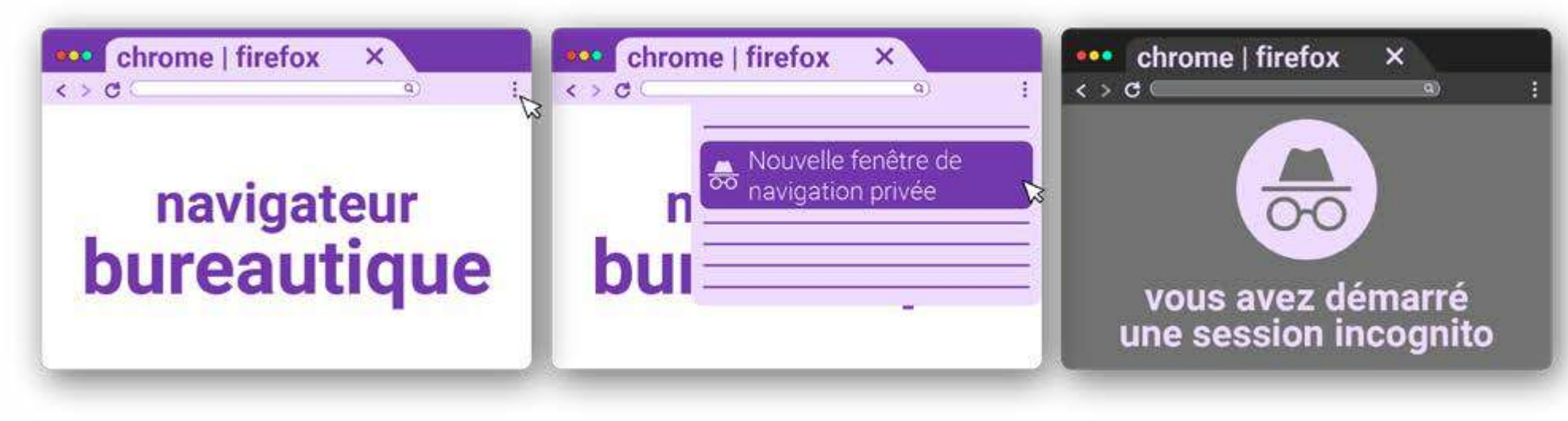
Que pouvez-vous faire pour vous protéger ?

- Utiliser un VPN rendra votre navigation internet plus sécurisée et privée.
    - Un VPN (réseau privé virtuel) chiffre vos données et masque votre adresse IP, protégeant ainsi votre activité de navigation, votre identité et votre localisation.

Si vous recherchez plus de confidentialité et d'autonomie, le VPN est la solution idéale.

Remarque : Le chiffrement est une technologie qui protège les données en les transformant en un code secret, accessible uniquement avec une clé numérique unique.

- Utilisez un navigateur axé sur la confidentialité comme Firefox Focus, Tor Browser ou DuckDuckGo. Si vous ne pouvez pas en télécharger un, vous pouvez utiliser le mode navigation privée pour empêcher votre navigateur d'enregistrer votre historique de navigation, vos cookies et les données de votre site, afin de préserver la confidentialité de vos activités sur les appareils partagés. Ce mode n'empêche pas totalement le suivi, mais il réduit le stockage des données. Lorsque vous avez terminé, il vous suffit de fermer la fenêtre navigation privée pour mettre fin à la session.
  - Sur la plupart des navigateurs de bureau, vous trouverez l'option de navigation privée en haut à droite en cliquant sur les trois points ou tirets, puis en sélectionnant "Nouvelle fenêtre de navigation privée". Sur Safari, cliquez sur “Fichier” dans la barre de menu et choisissez "Nouvelle fenêtre privée".



- Cela fonctionne également sur les navigateurs mobiles : appuyez sur les trois points ou tirets et sélectionnez "Nouvel onglet privé". Sur Safari, appuyez sur l'icône des onglets et sélectionnez "Privé" pour ouvrir un nouvel onglet en navigation privée.

- Désactivez votre identifiant publicitaire mobile et refusez les publicités ciblées. Les entreprises comme Google et Meta (Meta étant le propriétaire de Facebook, Instagram et WhatsApp) suivent vos activités en ligne pour afficher des publicités ciblées ; les bloquer renforce votre confidentialité sur ces plateformes.

  - Pour supprimer votre identifiant publicitaire sur les appareils Android, accédez à Paramètres > Confidentialité > Publicité. Appuyez sur « Supprimer l'identifiant publicitaire » et confirmez. Cela empêchera les applications d'y accéder à

l'avenir. Il se peut que cette option ne soit pas disponible sur les anciennes versions d'Android. Si vous ne la trouvez pas, allez dans les paramètres de confidentialité pour réinitialiser votre identifiant publicitaire et demander aux applications de ne pas vous suivre.

- Sur les appareils Apple, lorsque vous installez une nouvelle application, celle-ci peut demander l'autorisation de vous suivre. Pour gérer cela, allez dans Réglages > Confidentialité > Suivi et vous pourrez désactiver le suivi pour les applications individuelles que vous avez précédemment autorisées.

- Les grandes entreprises technologiques ont rendu plus difficile l'accès à des informations sur l'avortement sécurisé. Vérifiez toujours les informations et la réputation des services d'avortement que vous trouvez en ligne, car il existe de nombreux escrocs et de fausses cliniques (comme les centres de grossesse en crise).
    - Si les instructions semblent absurdes, y compris de longues périodes de jeûne et des exercices physiques intenses, méfiez-vous. Pendant un avortement par pilules, il est important de bien manger et de s'hydrater.
    - L'avortement est une procédure très sûre. Si les informations ne mettent en avant que les risques ou sont remplies d'images de fœtus, il pourrait s'agir d'une fausse clinique.

2. Que faire lorsque vous contactez: des organisations, conseillers, prestataires d'avortement ou cliniques via des services de messagerie (en ligne)

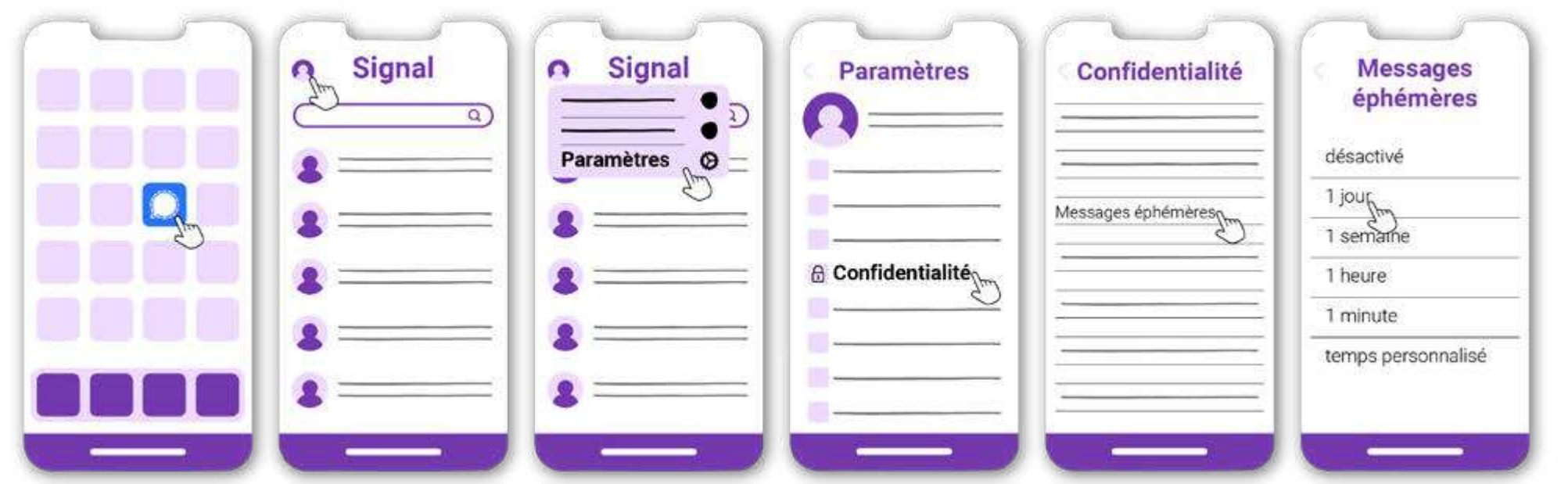
Vos messages SMS peuvent être lus par des membres de votre famille, votre partenaire ou même des amis s'ils ont accès à votre téléphone ou à votre facture téléphonique. Lorsque vous utilisez des services de messagerie, sachez que même si vous supprimez vos messages, ils peuvent rester stockés et être communiqués aux autorités sur demande (bien que cela nécessite généralement un mandat).

Comment pouvez-vous vous protéger ?

- Utilisez un code PIN ou un mot de passe fort sur vos appareils. Si possible, créez un mot de passe alphanumérique, mélangeant majuscules et minuscules.

- Évitez d'utiliser X (anciennement Twitter), Tiktok, Facebook et Instagram pour des conversations sensibles.

- Si possible, utilisez Signal, une application à but non lucratif, sécurisée et indépendante pour les messages et les appels, qui ne stocke pas les images sur votre appareil. N'oubliez pas d'activer les messages éphémères dans Paramètres > Confidentialité > Messages éphémères. Si vous utilisez un appareil iOS, désactivez également l'option “Afficher les Appels dans Récents” dans Réglages.



- Pour envoyer des messages ou passer des appels avec des numéros ordinaires, utilisez un téléphone prépayé ou un service VOIP (type de service téléphonique via internet) au lieu de votre téléphone personnel (vous pouvez essayer une application comme Hushed).

- Si cela n'est pas possible, les appels et messages via des applications comme Signal, WhatsApp ou Telegram sont chiffrés et plus sécurisés que les appels téléphoniques et SMS ordinaires.

- N'oubliez pas de configurer les messages éphémères pour toutes ces conversations, y compris avec des amis proches et la famille, ou même lors de discussions avec Ally, notre chatbot dédié à l'avortement, sur WhatsApp.

  - Allez dans Paramètres > Confidentialité et appuyez sur "Délai avant disparition". Sélectionnez 24 heures ou 7 jours.

- N'enregistrez pas les contacts des prestataires sur votre téléphone. Si vous devez enregistrer le contact, utilisez un nom aléatoire qui n'attire pas l'attention. Sur WhatsApp, vous pouvez également verrouiller la conversation.

  - Sur Android : Appuyez longuement sur la conversation que vous souhaitez verrouiller. Appuyez sur les trois points en haut à droite, puis sur “ Verrouiller la discussion”. Vous pouvez aussi créer un code secret pour accéder à cette conversation.

  - Sur iOS : Maintenez la conversation enfoncée pour afficher différentes options, dont “Verrouiller la discussion”.

- Lors de l'envoi de courriels, utilisez une adresse email secondaire qui n'est liée à aucun de vos comptes existants, puis supprimez-la après utilisation. Vous pouvez créer un compte sur ProtonMail, qui chiffre tous vos emails. Cela signifie que même les administrateurs de ProtonMail ne peuvent pas accéder à leur contenu. Les messages reçus d'autres fournisseurs (comme Gmail, Hotmail) sont également chiffrés immédiatement.

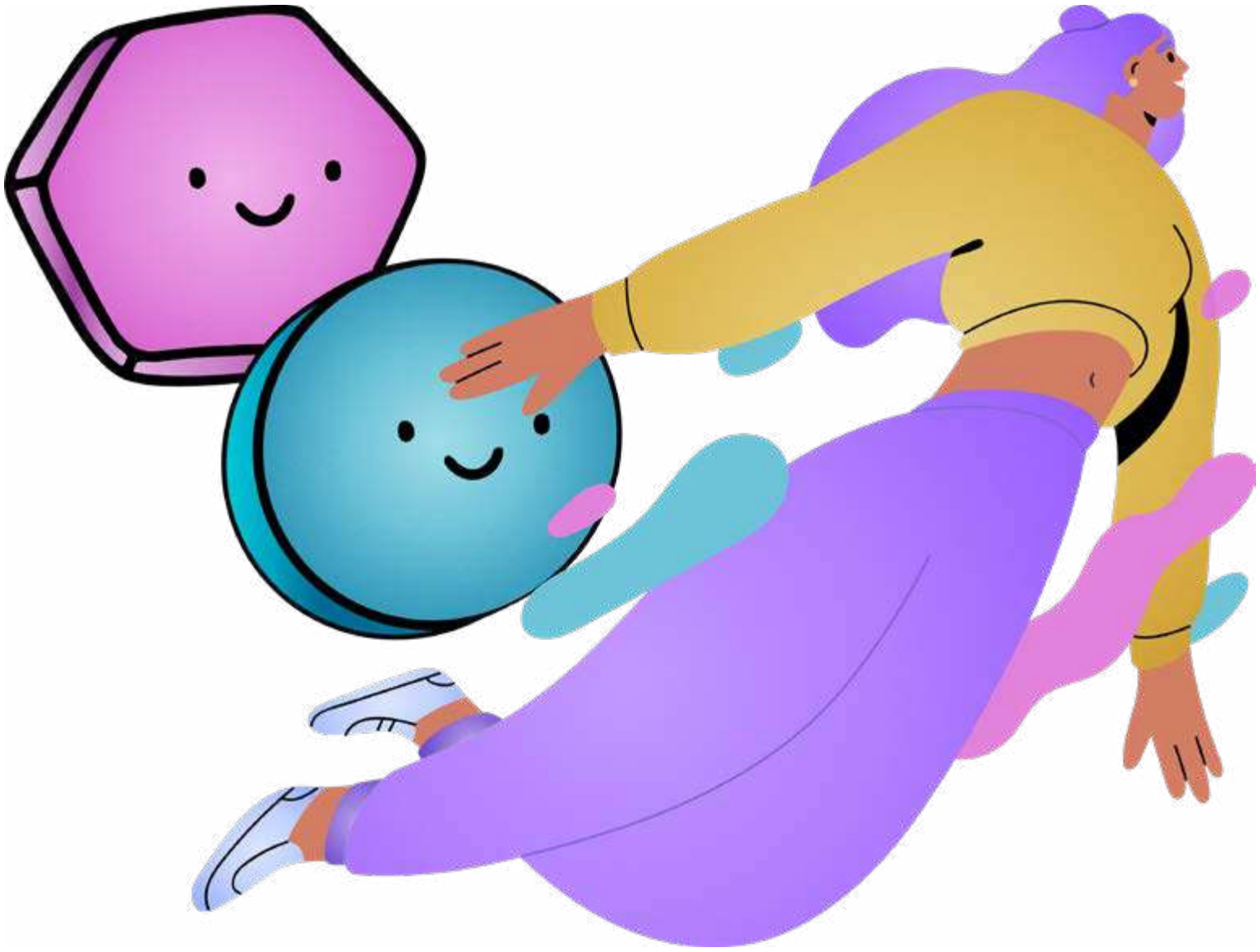
- Évitez de prendre et de partager des captures d'écran de ces conversations ou de sauvegarder des images compromettantes sur votre appareil. Vous pouvez également utiliser la fonction vue unique sur WhatsApp pour envoyer des images et des messages vocaux, garantissant leur disparition du chat après ouverture par le destinataire.

    - Sélectionnez "vue unique " à chaque envoi de message vocal, photo ou vidéo en cliquant sur l'icône avec le chiffre un dans la barre de texte. (1)

Attention : Lors du paiement pour des services d'avortement ou des soins médicaux, essayez d'utiliser des espèces pour éviter que les paiements par carte

ou les virements bancaires ne soient tracés. Si une carte prépayée est disponible dans votre pays, elle peut être une bonne option.

Remarque : Utilisez-vous votre navigateur pour contacter des prestataires d'avortement ? Protégez votre sécurité numérique et votre vie privée en suivant les mesures de sécurité de l'étape 1 : utilisez un navigateur axé sur la confidentialité, naviguez en mode navigation privée ou désactivez les publicités ciblées.



3.

Accéder aux services d’avortement

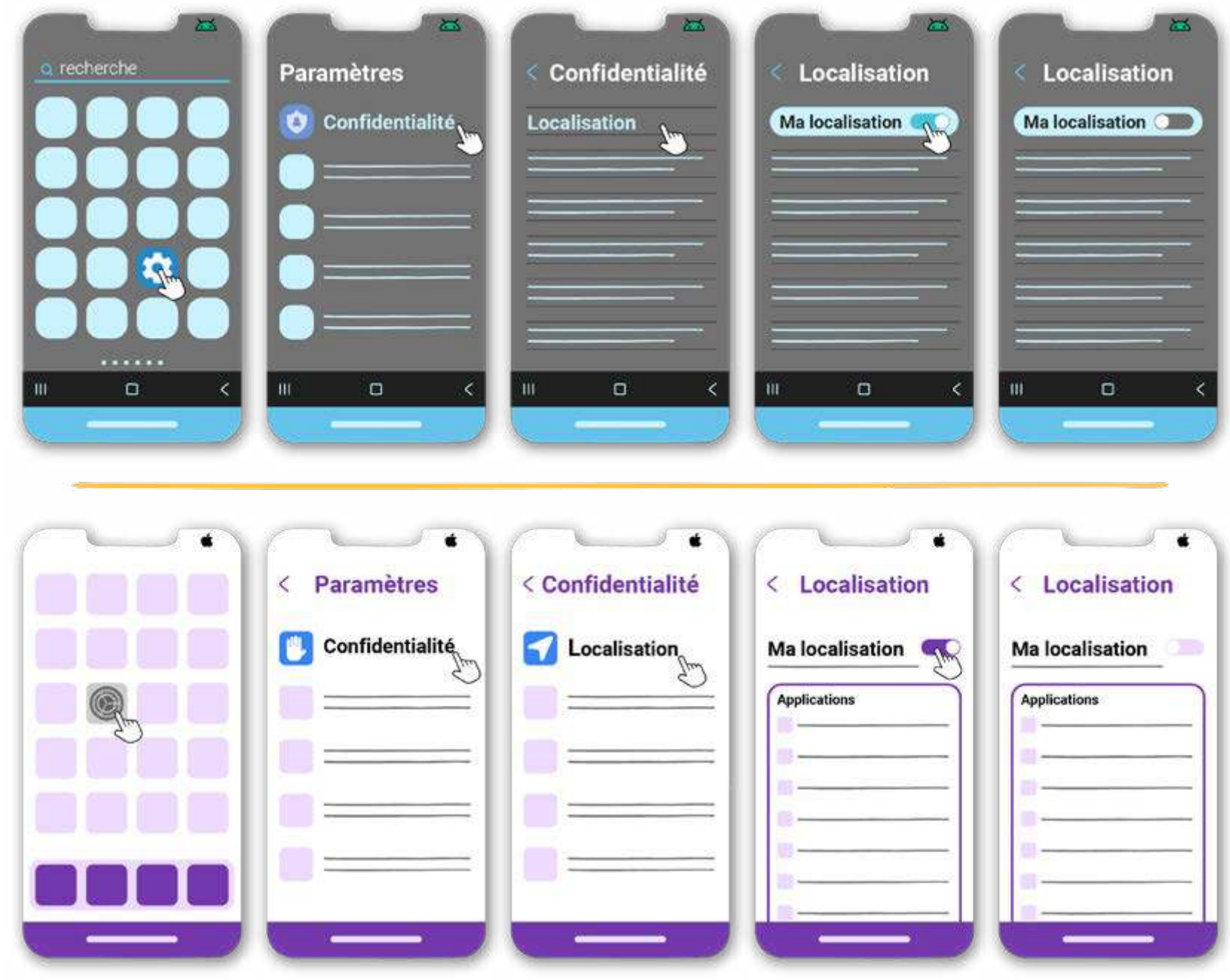
(en consultant un prestataire, en obtenant des pilules abortives, etc.)

Lorsque vous accédez à des services d’avortement, il est probable que vous ayez votre téléphone mobile avec vous. Cependant, votre téléphone émet des signaux, ce qui signifie que votre emplacement peut être suivi. Les opérateurs de téléphonie mobile peuvent fournir ces informations aux autorités si elles en font la demande.

Que pouvez-vous faire pour vous protéger ?

- Votre téléphone peut être suivi par son signal réseau, le Wi-Fi, le GPS, le Bluetooth, et d’autres méthodes. La meilleure option est d’éteindre complètement votre téléphone et d’être accompagnée d’une personne de confiance.

- Si ce n'est pas possible, envisagez au moins de désactiver le partage de votre localisation :
  - Sur Android, allez dans Paramètres, tapez sur “Localisation ”, cliquez sur “Accéder à ma localisation” et désactivez-la.
  - Sur IOS, allez dans Paramètres, puis tapez sur “Confidentialité et sécurité ” et désactivez “Services de localisation ”.

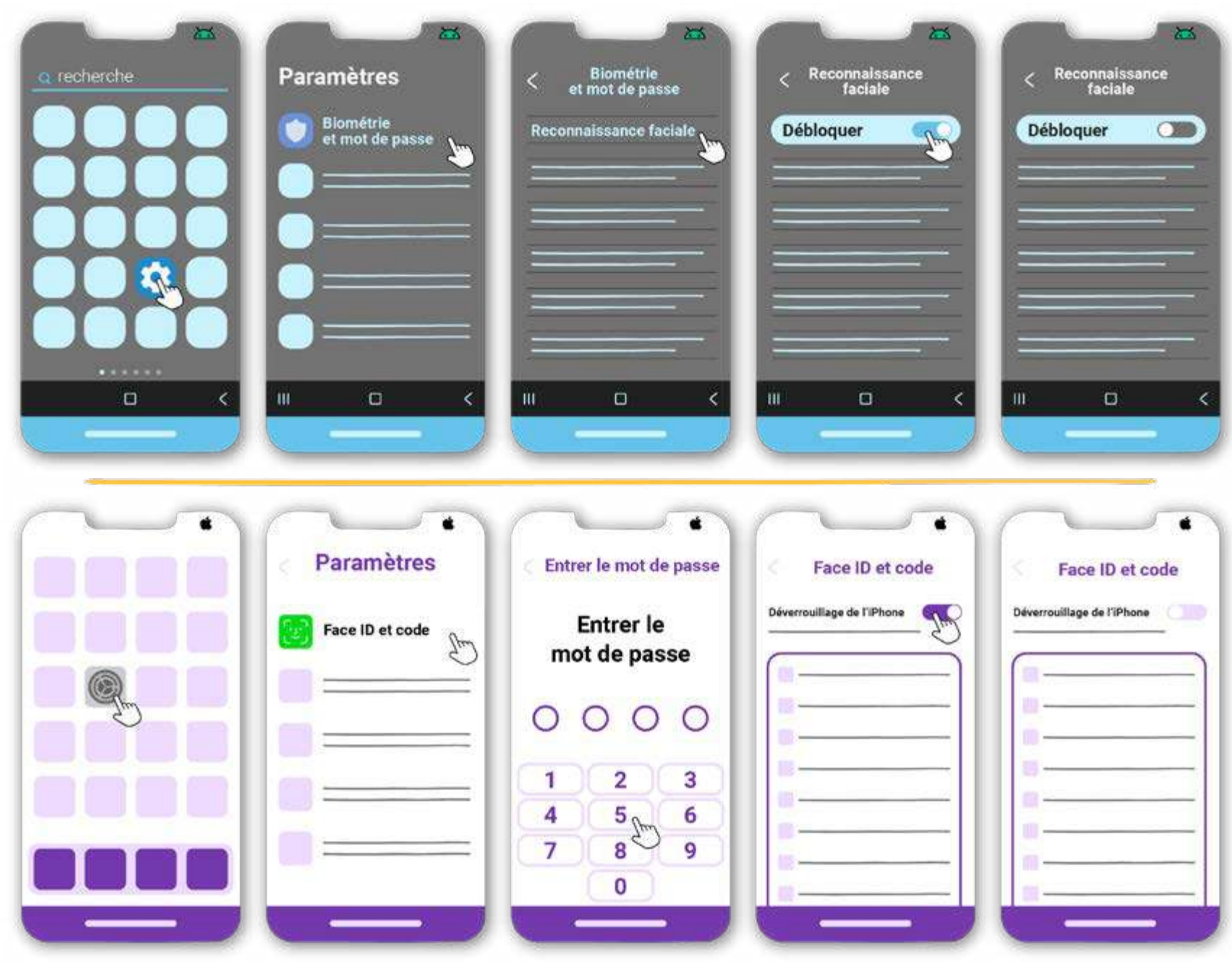


  - Si vous vous déplacez en voiture et que vous n'êtes pas sûr qu'elle dispose d'une technologie permettant de suivre votre position, envisagez d'utiliser les transports en commun ou de vous garer loin de l'endroit où vous devez vous rendre.

- Pensez à désactiver la reconnaissance faciale ou l’empreinte digitale, surtout en cas de risque de saisie de votre appareil.

  - Sur Android, allez dans Paramètres, puis “Biométrie et mot de passe ”, choisissez “Empreinte digitale ” et/ou “Reconnaissance faciale ”, entrez votre mot de passe, puis désactivez ces options.

  - Sur IOS, allez dans Réglages, puis “Face ID et code ”, accédez à “Utiliser Face ID” et désactivez “ Déverrouillage de l’iPhone ” ou “ Déverrouillage de l’iPad”.



- Si possible, évitez d'utiliser des applications de navigation comme Google Maps ou Waze pour vous rendre à l'adresse. Si ce n'est pas possible, assurez-vous qu'elles ne conservent pas votre itinéraire dans leur historique.

    - Si nécessaire, vous pouvez nettoyer vos données sur Google Maps en ouvrant l'application, en tapant sur votre photo de profil ou initiales. Cliquez sur "Vos données" dans Maps, puis "Activité sur le Web et les applications : Voir et supprimer l'activité". Lorsque vous voyez les entrées que vous souhaitez supprimer, appuyez sur "Supprimer".

- Si vous cherchez une alternative plus sûre, essayez OsmAnd, une application de cartographie hors ligne qui n'enregistre pas vos données.

Partagez ces informations avec toute personne qui pourrait en avoir besoin.

Ensemble, rendons l'accès à l'avortement plus sûr pour tout le monde !

Références:

1. “Keep Your Abortion Private & Secure.” Digital Defense Fund, 2021, www.digitaldefensefund.org/ddf-guides/abortion-privacy/. Accessed October 2024.

2. “Practical Guide to Strategies and Tactics for Feminist Digital Security.” CFEMEA, 2017, www.cfemea.org.br/index.php/pt/radar-feminista-lista/livros-guias-e-estudos2/4670-guia-pratica-de-estrategias-e-taticas-para-a-seguranca-digital-feminista. Accessed October 2024.

3. “Abortion Access Activist, Worker, or Patient.” SSD, https://ssd.eff.org/fr/playlist/es-un-proveedor-de-servicios-de-salud-reproductiva-los-estas-buscando-o-los-defiendes. Accessed October 2024.

4. “Digital Privacy Tips for Abortion Seekers.” *Asian Americans Advancing Justice*, 2022 www.advancingjustice-aajc.org/digital-privacy-tips-abortion-seekers. Accessed October 2024.

5. “Digital privacy for your private parts.” *Vagina Privacy Network*, 2019 www.vaginaprivacynetwork.org. Accessed October 2024.

6. “A certification for online abortion counselors.” safe2choose, www.safe2choose.org/abortion-counseling/online-abortion-training-course. Accessed October 2024.

7. Gomez, Noelia. “Digital conservatism: search engines’ strategy to hide information about abortion.” La Política Online, 2024 www.lapoliticaonline.com/politica/los-buscadores-incentivan-el-conservadurismo-digital-y-suprimen-informacion-sobre-el-aborto/. Accessed October 2024.

8. "Internet Street Smarts Course". Cyber Collective, www.cybercollective.org/internet-street-smarts. Accessed November 2024.

SÉCURITÉ NUMÉRIQUE POUR L'AVORTEMENT

Cet outil a été créé en partenariat entre **LaPilule.org** et **Cyber Collective**.

LaPilule.org est une communauté en ligne gérée par des personnes dévouées qui croient que tout le monde, quel que soit l'endroit où elles vivent, devrait avoir accès à une option d'avortement sans risque. **www.lapilule.org**

Cyber Collective permet aux gens de se sentir plus en sécurité et en confiance dans leurs expériences numériques MAINTENANT, afin que nous puissions avoir un avenir meilleur. **www.cybercollective.org**

Illustrations et conception graphique par Ana Ibarra. **www.behance.net/anafriedbanana**

Endorsed by:

CENTER FOR INTIMACY JUSTICE

CYBER COLLECTIVE

La Pilule