Bonnes pratiques en matière de sécurité numérique

Que vous militiez ou non pour les droits humains, la sécurité numérique vous concerne : une bonne hygiène numérique réduit votre exposition aux attaques. Voici quelques conseils simples pour naviguer plus sûrement.

Sauvegardez vos données

C'est le meilleur moyen d'éviter la perte de vos données en cas de perte, de vol ou de panne d'un appareil.

Chiffrez vos appareils

Si vous perdez le contrôle physique de votre appareil, vos données seront mieux protégées par le chiffrement intégral du disque. Si le chiffrement est illégal dans votre pays, suivez ces alternatives.

Activez l'authentification à deux facteurs sur vos comptes

L'authentification à deux facteurs (2FA) protège votre compte même si votre mot de passe est compromis. Privilégiez toujours la 2FA par application plutôt que par SMS : vous pourrez ainsi accéder à vos comptes même sans réseau mobile. Consultez une liste de gestionnaires de mots de passe et d'outils 2FA recommandés.

Utilisez un VPN

Lorsque vous vous connectez à un VPN, toutes les données que vous envoyez (par exemple les requêtes adressées aux serveurs lorsque vous naviguez sur le web) semblent provenir du VPN, ce qui masque votre adresse IP et contribue à protéger votre vie privée (puisque l'adresse IP indique votre localisation approximative). Découvrez comment choisir le service VPN qui vous convient le mieux.

Naviguez en toute sécurité

Un navigateur sécurisé, comme Tor, vous aide à protéger votre trafic réseau sur les réseaux peu fiables, comme ceux des aéroports ou des hôtels. Évitez le wifi public autant que possible. Maintenez votre navigateur et ses modules complémentaires à jour. Bloquez les fenêtres publicitaires et utilisez un bloqueur de publicités. Naviguez en mode « navigation privée » ou activez l'option « ne pas me pister » de votre navigateur.

Maintenez vos appareils à jour

Un système entièrement à jour est plus difficile à compromettre et présente moins de vulnérabilités connues.

Interagissez avec ILGA World sur les réseaux sociaux en toute sécurité

Voici les comptes officiels d'ILGA World : Facebook – X – Instagram – LinkedIn – YouTube – TikTok (inactif) – Bluesky (inactif).

Utilisez un mot de passe robuste et UNIQUE pour chacun de vos profils sur les réseaux sociaux. Vérifiez que vous avez toujours accès à l'adresse électronique ou au numéro de téléphone indiqué lors de votre inscription. Si vous craignez que votre OSIEGCS soit révélée sans votre consentement,

réglez votre profil sur « privé ». Refusez les invitations de personnes que vous ne connaissez pas : sur les réseaux sociaux, les personnes ne sont pas toujours celles qu'elles prétendent être.

En cas de cyberattaque anti-LGBTI sur les réseaux sociaux : n'interagissez pas avec les trolls ; faites plutôt des captures d'écran de leurs messages, conservez-les et signalez-les. Ne cliquez pas sur les liens suspects reçus en commentaire ou en message privé, surtout s'ils proviennent de personnes que vous ne connaissez pas. Veillez à ce que votre antivirus et votre pare-feu soient à jour. Si le harcèlement s'intensifie, réglez votre profil sur « privé » ou désactivez les commentaires. **ILGA World ne vous demandera jamais vos mots de passe !**

Sources de ce guide : AccessNow ; GlobalPride2020 ; Security in a Box, par Frontline Defenders et Tactical Tech ; Surveillance Self-Defense, par l'Electronic Frontier Foundation