huridocs
human rights information and documentation systems

Brèves informations de base sur la sécurité numérique pour les défenseurs des droits de l'homme

Cette note fournit des informations générales sur les pratiques de base en matière de sécurité numérique que les défenseurs des droits humains (DDH) peuvent prendre en compte dans le cadre de leur travail. Il ne fournit pas d'informations exhaustives sur la manière de traiter chaque incident de sécurité numérique. Il est donc conseillé aux défenseurs des droits humains de consulter également des sources d'informations fiables pour leur sécurité numérique.

SÉCURISEZ VOTRE ORDINATEUR

- Assurez-vous que votre ordinateur reçoit des mises à jour régulières et évitez d'utiliser des logiciels ou des programmes sans licence.
- Utilisez un mot de passe fort pour l'autorisation de l'utilisateur.
- Activez votre pare-feu.
- Activez le chiffrement complet de votre disque.
- Installez un antivirus fiable (par exemple, Malwarebytes).
- Veillez à ce qu'aucune donnée sensible n'est stockée sur votre ordinateur et envisagez de stocker les données sensibles dans un compte cloud sécurisé.
- Utilisez toujours des mots de passe forts pour tous les comptes et n'utilisez pas les mêmes mots de passe pour plusieurs comptes.
- Utilisez un gestionnaire de mots de passe pour stocker tous vos mots de passe forts et uniques pour chaque comptes.
- Protégez vos comptes avec l'authentification à 2 facteurs (2FA) à l'aide d'une application (par exemple Google Authenticator) et n'optez pas pour l'authentification par SMS. Dans la mesure du possible, générez des codes de sauvegarde comme option 2FA secondaire et stockez-les dans un gestionnaire de mots de passe ou dans un autre endroit sécurisé préféré.
- Nettoyez régulièrement votre ordinateur des données inutiles.
- Utilisez toujours un réseau privé virtuel (VPN) lorsque vous travaillez dans des lieux publics (cafés, bibliothèques, aéroports) et lorsque vous vous connectez à des réseaux publics.
- Vérifiez les paramètres de votre navigateur et assurez que vos informations de connexion (noms d'utilisateur et mots de passe) ne sont pas enregistrées dans le navigateur.
- Pensez à effacer régulièrement les cookies, le cache du navigateur et l'historique du navigateur

SÉCURISEZ VOTRE TÉLÉPHONE

- Assurez-vous que votre téléphone est a jour avec le dernier système d'exploitation et reçoit des mises à jour de sécurité régulières.
- Téléchargez uniquement des applications à partir de sites et de ressources autorisés et sûres (Google Play Store, Apple Store).
- Utilisez un mot de passe fort pour verrouiller votre téléphone.
- Désinstallez les applications que vous n'utilisez pas et dont vous n'avez pas besoin.
- Supprimez les fichiers sensibles et les fichiers inutilisés et envisagez d'effacer le texte et l'historique des appels.
- Désactivez l'affichage du contenu des messages dans les notifications (par exemple, dans Signal: Paramètres →Notifications →Afficher →choisissez « Nom uniquement » ou «Aucun nom ni message»).

SÉCURITÉ PHYSIQUES

- Soyez discret avec les appareils numériques et gardez-les à portée de vue et près de vous à tout moment.
- Soyez vigilant et conscient de votre environnement (salle de réunion, espace de coworking, inconnus).
- Méfiez-vous des étrangers qui expriment une curiosité générale pour votre travail.
- Méfiez-vous des appareils abandonnés ou abandonnés (USB, tablettes et même ordinateurs portables), surtout lorsque vous travaillez dans un espace public.

Suivez-nous pour plus de conseils et de mises à jour pour les défenseurs des droits de l'homme, ou contactez-nous pour collaborer.

www.huridocs.org

hello@huridocs.org