SÉCURITÉ DES SYSTÈMES D'INFORMATION

Du point de vue de l'individu membre de l'ONG

cartong

Avec la participation de

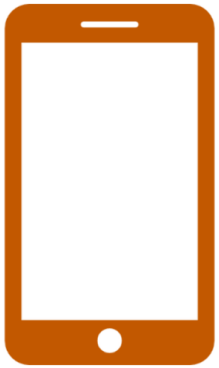
MINISTÈRE DE L'EUROPE ET DES AFFAIRES ÉTRANGÈRES

AFD AGENCE FRANÇAISE DE DÉVELOPPEMENT

Quelques chiffres

- **Les violation de données sont fréquentes** mais différentes de ce que l'on pense souvent:
  - 1 courriel sur 323 est **malveillant**
  - **82 % d'entre elles impliquent une action humaine**
  - **Plus de 75 % des cyberattaques ciblées partent d'un e-mail**
  - 70 % des fraudes en ligne sont commises par l'intermédiaire de **plates-formes mobiles**

Vos 2 priorités en matière de cybersécurité



Trouvez des solutions réalistes

SECURITE

FACILE A UTILISER

On ne peut avoir un systeme 100% secure, mais encore moins un systeme 100% secure et “user friendly”, il faut rester réaliste dans ce qu’on met en place pour que cela reste utilisé et utilisable,.

8 bonnes pratiques

1/ Sécuriser son poste de travail

Objectif: Prévenir les accès frauduleux, le lancement de virus ou la prise de contrôle à distance, notamment via Internet.

Comment?

- **Mise à jour régulière** des logiciels et des antivirus
- Se **déconnecter** lorsque l'on s'éloigne de son ordinateur
- Limiter l'**utilisation de supports mobiles externes**
- **Ne pas utiliser son matériel personnel** dans un cadre professionel (BYOD- "Bring your own device").
- Ne jamais se connecter à un **Wi-Fi public** et utilisation recommandée de **VPN** dans les contextes le nécessitant

Liste des pays où l'utilisation d'un VPN est interdite

- Bélarus
- Chine
- L'Iran
- L'Irak
- Corée du Nord
- Oman
- Russie
- Turquie
- Turkménistan
- Émirats arabes unis
- Ouganda

2/ Se protéger du hameçonnage

Objectif: Prévenir les accès frauduleux par du hameçonnage.

Définition: *communication frauduleuse qui se fait passer pour une source fiable afin de tromper l'utilisateur et l'inciter à communiquer des données sensibles ou à installer des programmes de malware. Ces attaques ont souvent lieu via des e-mails mais elles peuvent aussi survenir sur les réseaux sociaux* ***(source: CyberPeace institut)***

—

Comment?

- Ne **jamais cliquer sur un lien provenant d'un contact inconnu**
- **Vérifier l'adresse email** de l'émetteur·rice
- **En cas de doute, contacter l'émetteur par un autre moyen de communication pour confirmation**

cartong
Avec la participation de
MINISTÈRE DE L'EUROPE ET DES AFFAIRES ÉTRANGÈRES
AFD AGENCE FRANÇAISE DE DÉVELOPPEMENT

3/ Sécuriser les échanges

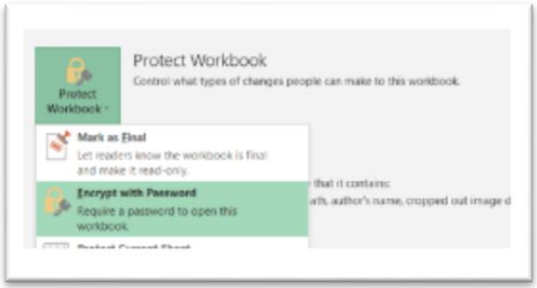
Objectif: Renforcer la sécurité de toutes les transmissions de données personnelles & sensibles

—

Comment?

- Déidentifier les données (par pseudonomisation, anonymisation, agrégation) lorsque cela est possible.
- Utiliser des **moyens de partage sécurisés** (plateforme dédiée etc).
- **Chiffrer les données** avant de les envoyer sur un support physique ou via le réseau.
- Si votre courriel et celui du répondant ne sont jamais chiffrés, **évitez les courriels.**
- Partager les **mots de passe en toute sécurité.**
- Si nécessaire, **supprimez les métadonnées de vos fichiers** (par exemple, les coordonnées GPS de l'image).
- **Sensibilisez votre interlocuteur·rice recevant les données !**

Exemples d'outils pour sécuriser les échanges



ProtonMail

PGP ENCRYPTED EMAIL

mockaroo

realistic data generator

PrivateBin

bitwarden

SIGNAL

SECURED MESSAGING APPS

Threema.

VeraCrypt

ENCRYPTION SOFTWARE FOR DISK OR USB

Windows 10 BitLocker

tresorit send

ENCRYPTED SHARED FILED

SDCMICRO: STATISTICAL DISCLOSURE CONTROL

7ZIP

cartong

Avec la participation de

MINISTÈRE DE L'EUROPE ET DES AFFAIRES ÉTRANGÈRES

AFD AGENCE FRANÇAISE DE DÉVELOPPEMENT

4/ Bien gérer l'authentification

Objectif: Sécuriser ses accès aux applications

—

Comment?

- Utiliser des outils permettant un **accès individuel**, éviter absolument les comptes partagés
- Halte aux mots de passe inscrits sur des **post-its**
- Utiliser des **mots de passe suffisamment forts** (12 caractères, caractères spéciaux etc...)
- Utiliser un **gestionnaire de mots de passe** au niveau de l'organisation (pour vous permettre de gérer facilement tous vos mots de passe)
- Envisager l'utilisation de l'**authentification à 2 facteurs pour les outils content des données personnelles ou sensibles**

Exemples d'outils pour améliorer l'authentification

cartong

Avec la participation de

MINISTÈRE DE L'EUROPE ET DES AFFAIRES ÉTRANGÈRES

AFD
AGENCE FRANÇAISE DE DÉVELOPPEMENT

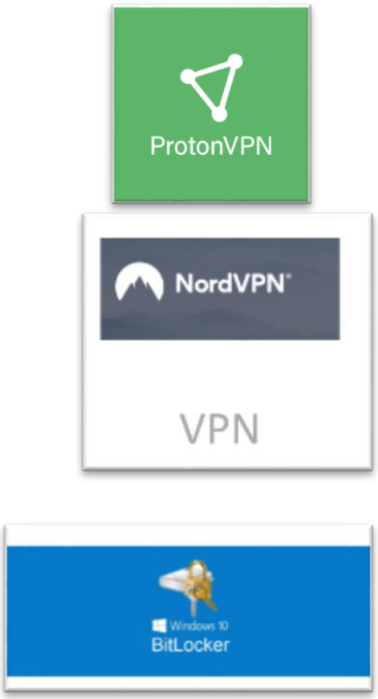
5/ Sécuriser les équipements mobiles

Objectif: Anticiper les violations de données potentielles liées au vol ou à la perte d'un support de stockage mobile

—

Comment?

- **Chiffrer** autant que possible les équipements mobiles et support de stockage (disques dur internes/externes ; smartphones; clés USB)
- **Contrôler la** mise en œuvre des mesures de **sauvegarde** ou de **synchronisation**
- S'assurer que les **systèmes de verrouillage** des équipements sont suffisamment solides
- Ne jamais se connecter à un **Wi-Fi public** et utilisation recommandée de **VPN** dans les contextes le nécessitant



6/ Chiffrer les données le nécessitant

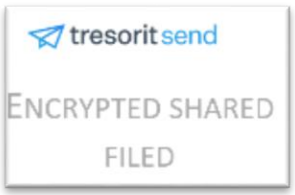
Objectif: Garantir l'intégrité et la confidentialité d'une donnée.

Définition *: codage d'un message ou d'une information de manière à ce que* ***seules les personnes autorisées*** *puissent y accéder et que celles qui ne le sont pas ne puissent pas le faire.*

—

Comment?

- Favoriser les outils permettant le chiffrement pour les données personnelles ou sensibles (par exemple SurveyCTO vs Kobo, Signal vs SMS...)
- S'assurer qu'ils utilisent un **algorithme** reconnu et **sécurisé** (par exemple SHA-256, AES-256...)



7/ Assurer la continuité

Objectif: Réduire les consequences d'une perte indésirable de données.

Comment?

- S'appuyer sur vos outils institutionnels si vous en avez (ou mettez les en place) pour effectuer des **sauvegardes fréquentes des données**

8/ Superviser la destruction des données

Objectif: Garantir la destruction correcte des données à la fin du cycle de vie du matériel et des logiciels.

—

Comment?

- **Prévoir sur tout jeu de données personnelles/sensibles une date de suppression/archivage** et des procedures pour que cela soit respecté.
- **Effacer en toute sécurité les données du matériel** (avant de s'en débarrasser ou de l'envoyer en réparation) **et des logiciels utilisés.**

Conclusion

- Gardez à l'esprit la **tension entre efficacité opérationnelle et harmonisation du stockage** des **données**

- Réfléchissez au niveau de **sécurité existant et souhaitables des outils organisationnels** utilisés pour la gestion **de données programmes (**collecte, stockage et analyse des données ...)

- La sécurité des données est un sujet qui nécessite, entre autres, un **soutien par des expert.es en cybersécurité**

C'est particulièrement important pour les ONG de défense des droits humains qui sont exposées à un risque très élevé de cyberattaques.

Deux citations pour bien terminer

> **"Our staff is the best firewall we can ask for as well as our last line of defense that can never be replaced by technology. We appreciate their efforts and willingness to partner with IT Security and treat them as such."**
>
> **– Oleg Bell, Global Head of IT Security, Open Society Foundations**

La culture organisationnelle peut représenter un **défi encore plus grand que les questions techniques**. La mentalité selon laquelle "toutes nos informations sont de toute façon disponibles" ou "s'ils veulent les données, ils trouveront un moyen de les obtenir" est omniprésente dans les **opérations** humanitaires.

Mai 2019 - Evénement à Wilton Park - OCHA

Remerciements

Cette présentation bénéficie du soutien de l'Agence Française de Développement (AFD) et du Centre de crise et de soutien du Ministère de l'Europe et des Affaires étrangères (CDCS). Néanmoins, les idées et les opinions présentées dans cette présentation ne représentent pas nécessairement celles de l'AFD ou du CDCS.

Cette présentation a été conçue en utilisant des ressources de Flaticon, Freepik et de The Noun Project.

cartong

Avec la participation de

MINISTÈRE DE L'EUROPE ET DES AFFAIRES ÉTRANGÈRES

AFD AGENCE FRANÇAISE DE DÉVELOPPEMENT