SÉCURITÉ DES SYSTÈMES D'INFORMATION

Du point de vue organisationnel

cartong

Avec la participation de

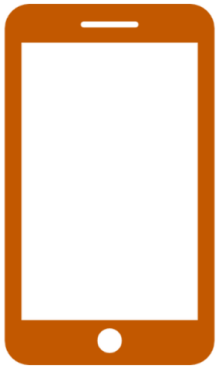
MINISTÈRE DE L'EUROPE ET DES AFFAIRES ÉTRANGÈRES

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 **plateformes mobiles**

Vos 2 priorités en matière de cybersécurité



Trouvez des solutions réalistes

SECURITE

FACILE A UTILISER

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

9 bonnes pratiques

1/ Sécuriser les postes de travail

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

—

Comment?

- Installer un **pare-feu et un antivirus nouvelle generation (NGAV)**
- Imposer la **mise à jour régulière** des logiciels et des antivirus
- Mettre en place de la **déconnexion automatique**
- Limiter l'**utilisation de supports mobiles externes**
- Fournir des outils de **synchronisation ou de sauvegarde**
- Interdiction du **BYOD** (“Utiliser vos appareils personnels”- *bring your own device*)
- Encourager l’utilisation 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/ Gerer les accès et authentification

Objectif: Identifier vos utilisateur·rices pour gérer leurs droits d'accès, avoir la possibilité d'autoriser l'accès qu'aux données dont l'utilisateur·rice a réellement besoin dès que l'on parle de données personnelles ou sensibles

—

Comment?

- Définir des **accès individuels** par utilisateur·rice et interdire les comptes partagés
- Forcer l'utilisation de **mots de passe suffisamment forts** (12 caractères, caractères spéciaux etc...)
- Mettre en place un **gestionnaire de mots de passe** au niveau de l'organisation et vérifier les pratiques d'hygiène associées
- **Limiter les tentatives d'accès à un compte**
- Retirer les **autorisations d'accès obsolètes**
- Envisager l'utilisation de l'**authentification à 2 facteurs pour les outils institutionnels le nécessitant**

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

3/ Faire face au 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·rice 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 institute)***

Comment?

- Activez la **double authentification** pour les sites/logiciels sensibles
- **Sensibiliser** vos collaborateur·rices au phishing et à comment y faire face (Formation, Fausses campagnes de phishing...)

cartong

Avec la participation de MINISTÈRE DE L'EUROPE ET DES AFFAIRES ÉTRANGÈRES

AFD AGENCE FRANÇAISE DE DÉVELOPPEMENT

4/ Sécuriser les échanges

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

Comment?

- Former les équipes pour savoir au besoin :
  - **Chiffrer les données** avant de les envoyer sur un support physique ou via le réseau.
  - **Pseudonomyser, anonymiser, agréger** des données lorsque cela est possible.
  - **Supprimez les métadonnées de vos fichiers** (par exemple, les coordonnées GPS de l'image).
- Mettre à disposition :
  - Une application de **messagerie sécurisée**
  - Un système de **partage des données sécurisé**
  - Un système de partage des **mots de passe sécurisé**

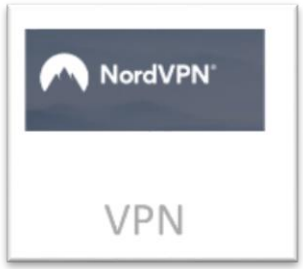
5/ Sécuriser les équipements mobiles

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

—

Comment?

- Fournir des **mesures de chiffrage** protégeant les disques durs et supports de stockage.
- **Contrôler la** mise en œuvre des mesures de **sauvegarde** ou de **synchronisation**
- S'assurer que les **systèmes de verrouillage** des équipements sont suffisamment solides
- Empêcher la connexion à un **Wi-Fi public** et utilisation recommandée de **VPN** dans les contexts le nécessitant



6/ Mesures de traçabilité

Objectif: Enregistrer certaines actions effectuées sur les systèmes informatiques afin de pouvoir identifier des accès frauduleux ou une utilisation abusive de données à caractère personnel, ou de déterminer l'origine d'un incident.

Comment?

- Favoriser les outils avec des mesures de traçabilité tels des log book (recueil des actions sur une base de données).
- **Examen** régulier **des logbook** afin de détecter d'éventuelles anomalies.

7/ Maitriser l'infrastructure informatique

Objectif: Tenir à jour **l'inventaire des infrastructures informatiques** (reseaux internes, connexions Wi-Fi, serveurs, dispositifs type USB, disque dur...) et des outils institutionnels de gestion de données pour mieux les protéger

—

Comment?

- Avoir une politique en matière **droits d'administration et de sécurité**
- Utiliser des **logiciels de confiance et audités** sur client.es et serveurs
- Tenir autant que possible les **mises à jour** les logiciels, drivers, etc.
- Utiliser un **logiciel d'inventaire d'équipement informatique**
- Utiliser des **protocoles sécurisés** pour les services et sites web (TLS/SSL...)

8/ Assurer la continuité

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

Comment?

- Effectuer des **sauvegardes fréquentes des données**
- Protéger les **sauvegardes de données**
- Créer un **plan de contigence informatique et de continuité des activités** et/ou un plan de réponse aux incidents
- Envisager une **cyber-assurance ou un soutien (de type CyberPeace builders)**

9/ 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/outillage pour que cela soit respecté et programmable.**
- **Effacer en toute sécurité les données du matériel** (avant de s'en débarrasser ou de l'envoyer en réparation) **et des logiciels utilisés.**

Et aussi....

- Planifier des **audits et des tests périodiques** (par exemple, test des procédures de restauration, test de penetration, audit sécurité, ...)
- Assurer l'**intégrité physique et la sécurité** de tous vos locaux
- Assurer le suivi de vos **sous-traitant.es** (partenaires ou fournisseur.ses) avec une documentation et des processus appropriés : processus de diligence raisonnable, clauses contractuelles spécifiques, calendrier de restitution et de suppression des données, organisation d'un audit de sécurité...
- Élaborer des **politiques organisationnelles générales et des procédures opérationnelles standard :** en matière de technologie, informatique, de gestion de données...

Sans oublier la sensibilisation et l'accompagnement....

N'oubliez pas : il incombe à l'ONG, avec les moyens et les connaissances dont elle dispose, de sensibiliser son personnel, ses partenaires (et les personnes concernées !).

En d'autres termes, **faire de la charte informatique/ des accords de partage de données plus qu'un simple papier...**

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 sur la sécurité des données

> **"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