Sécurité numérique et gestion des risques

Séance n° 3 : Bonnes pratiques

2025

AFD AGENCE FRANÇAISE DE DÉVELOPPEMENT
Funded by the European Union
forus CONNECT SUPPORT INFLUENCE
INNOVUS

Sécurité numérique ? Je n'y connais rien !

Réfléchissons à la manière de nous protéger dans les médias numériques

Sécurité numérique et analyse des risques

Introduction à la sécurité numérique pour les organisations non gouvernementales (ONG) et les défenseurs des droits humains (DDH)

Comprendre l'environnement numérique, les acteurs présents et les menaces auxquelles nous sommes confrontés.

1

2

Il faut prendre soin des communications

Décider quels outils utiliser et comment les configurer pour améliorer la sécurité et la confidentialité.

3

Meilleures pratiques numériques

Élaborer un plan d'amélioration incluant les meilleures pratiques et les engagements d'utilisation.

Session n° 3 : Bonnes pratiques

Objectifs

- Que savons-nous de nos propres vulnérabilités et capacités de réponse ?
- Quelles sont les bonnes pratiques fondamentales que nous devons mettre en œuvre dans notre ONG ?
- Élaborez-vous et évaluez-vous un plan d'intervention en cas d'incidents cybernétiques ?

Passons en revue les concepts de l'analyse des risques

La recherche de l'équilibre...

Bonnes pratiques

Risques
Attaques
Vulnérabilités

RAPPEL

Risques numériques

Ce que nous voulons éviter

- Perte d'accès à un compte
- Perte d'informations
- Perte d'équipement
- Accès non autorisé aux informations
- Surexposition des informations personnelles
- Exposition de vos sources

Attaques fréquentes

Comment agissent nos adversaires

- Hameçonnage
- Exploitation des vulnérabilités
- Doxxing
- Logiciels espions
- Chantage
- Harcèlement en ligne
- Menaces en ligne
- Violence sexiste facilitée par la technologie

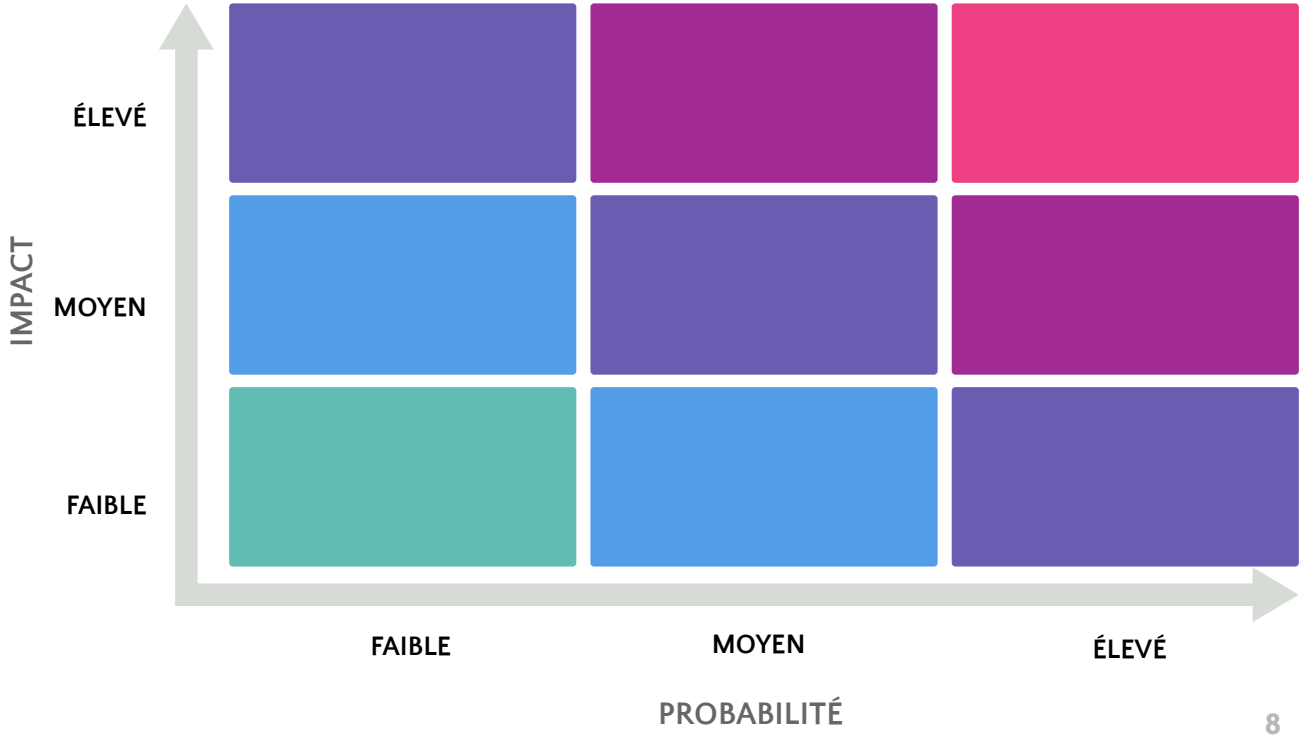
Vulnérabilités

Certaines choses qui nous mettent en danger

- Utiliser de mauvais mots de passe
- Ne pas verrouiller les appareils
- Ne pas utiliser la 2FA
- Ouvrir des pièces jointes inconnues
- Ne pas avoir de copie de sauvegarde
- Ne pas mettre à jour les programmes
- Utiliser des réseaux publics
- Utilisation d'applications de communication non sécurisées

Activité 1

Bref exercice d'analyse et de hiérarchisation des risques et des attaques



Bonnes pratiques

Éléments qui font pencher la balance

- ➔ Utilisez des mots de passe uniques et forts
- ➔ Protéger les appareils avec des mots de passe de démarrage
- ➔ Utiliser l'authentification à deux facteurs (2FA) pour tous les comptes
- ➔ Méfiez-vous des pièces jointes inconnues
- ➔ Effectuer régulièrement des sauvegardes
- ➔ Configurer votre confidentialité
- ➔ Maintenir les mises à jour à jour
- ➔ Crypter tout ce que vous pouvez crypter
- ➔ N'utilisez que des réseaux fiables
- ➔ Utilisez des applications de communication sécurisées

Activité 2

Brève analyse des risques et des attaques - identification des bonnes pratiques

Risque ou attaque	Vulnérabilités associées	Bonnes pratiques qui atténuent

Analyse des risques

Faire en sorte que l'effort en vaille la peine

L'**analyse des risques** est un excellent **outil** pour identifier les questions à traiter en priorité, mais la manière dont nous devons gérer les **risques** et les **attaques** potentielles dépendra de notre **volonté** d'atténuer les **vulnérabilités** et de notre **capacité** à intégrer les **bonnes pratiques** parmi les membres de l'organisation et au sein même de l'organisation.

Analyse des risques

Faire en sorte que l'effort en vaille la peine

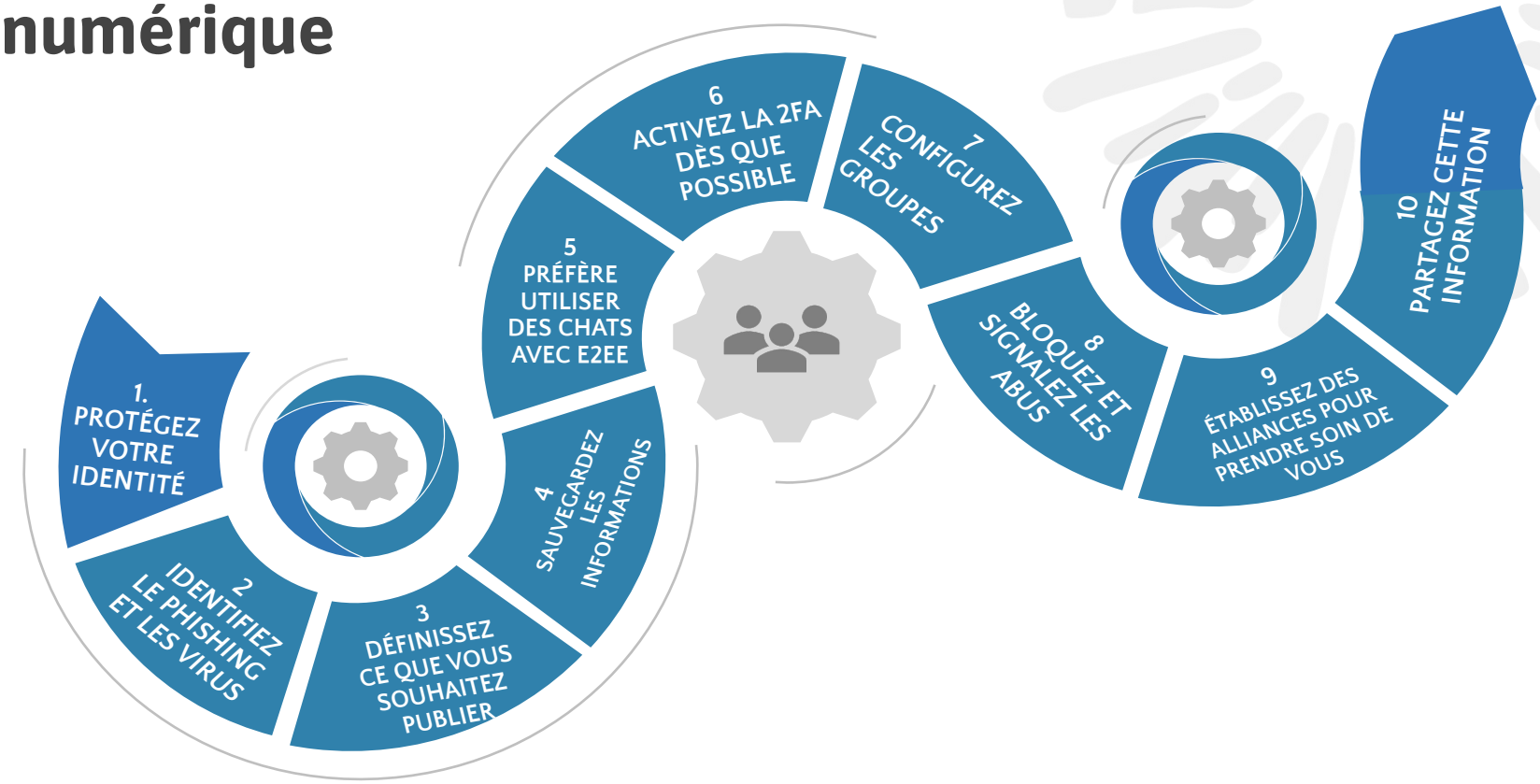
Une analyse des risques permet d'élaborer un plan d'amélioration, pour lequel il convient :

- Être réaliste quant aux ressources et aux capacités de l'organisation,
- Rechercher l'aide d'autres organisations,
- Allouer des ressources et du temps aux tâches en attente,
- Assurer un suivi continu.

La sécurité numérique est un processus dans lequel nous apprenons à prendre de meilleures décisions et développons un esprit critique et réfléchi vis-à-vis de la technologie.

Une voie possible

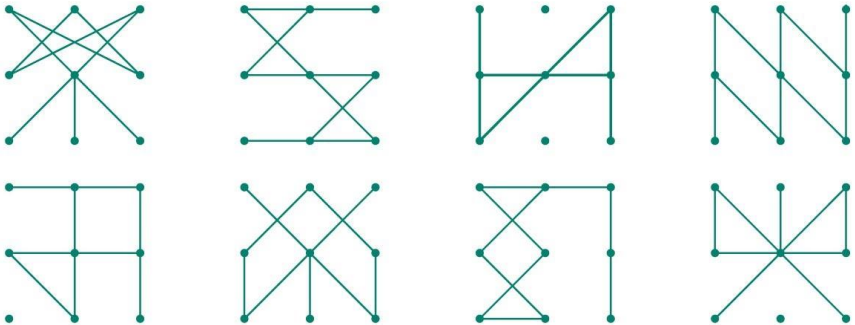
10 étapes pour améliorer notre sécurité numérique



10 recommandations fondamentales

1. Téléphones portables

- Avec un bon mot de passe
- Les empreintes digitales ou la reconnaissance faciale ne sont pas mauvaises en matière de sécurité, mais elles révèlent beaucoup d'informations.
- Faites des copies de sauvegarde.



2. Ordinateurs tiers.

Cafés Internet - espace public - ordinateur d'une autre personne

- Utiliser le mode incognito.
- Supprimer les fichiers téléchargés.

3. Outils sécurisés

- Évitez d'appeler et d'envoyer des SMS via le réseau cellulaire.
- Il vaut mieux utiliser WhatsApp.
- **Il est encore mieux d'utiliser Signal.**
- Il est important de persuader vos contacts d'utiliser des systèmes de communication plus sûrs.

4. Navigation sur Internet.

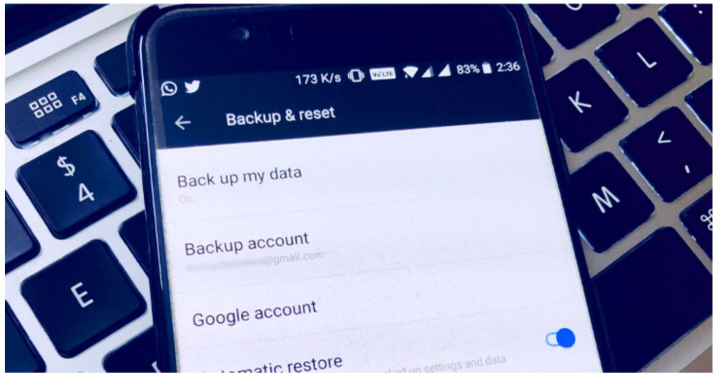
- Vérifier les paramètres de sécurité du navigateur.
- Désactivez les systèmes de suivi tels que les cookies tiers.
- Supprimer les historiques de navigation compromettants.
- Maintenir le navigateur à jour.
- Selon les circonstances, utilisez un VPN ou TOR.

5. Copies de sauvegarde.

- Sauvegarde, sauvegarde, sauvegarde

Google to Encrypt Android Cloud Backups With Your Lock Screen Password

October 15, 2018 Swati Khandelwal



In an effort to secure users' data while maintaining privacy, Google has announced a new security measure for Android Backup Service that now encrypts all your backup data stored on its cloud servers in a way that even the company can't read it.

Exemples de méthodes pour effectuer des copies de sauvegarde.

VeraCrypt

Google Drive

iCloud

6. Publications sur Internet.

- Veillez à ne pas rendre publiques :
  - Informations personnelles.
  - Numéros d'identification
  - Numéros de téléphone
  - Adresses
  - Localisation
- Faites attention lorsque vous taguez des personnes ou utilisez des étiquettes en général.
- Déterminez avec soin qui peut voir ou non chaque publication.

7. Mots de passe.

- Mots de passe longs et complexes (chiffres, lettres, majuscules et minuscules).
- Évitez de réutiliser les mêmes mots de passe pour plusieurs comptes.
- Changez-les de temps en temps.
- Si vous devez inévitablement mettre un mot de passe sur l'ordinateur d'un tiers, changez-le dès que possible.
- Facultatif : utilisez un gestionnaire de mots de passe tel que KeePassXC.

8. Informations sensibles.

- Où sont-elles stockées ?
- Où sont-elles stockées ?
- Qui peut y avoir accès ?

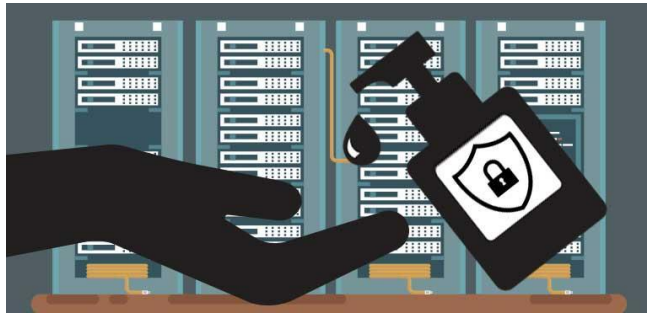
- Chiffrez, Chiffrez, Chiffrez.
- Options: PGP, 7-Zip, Veracrypt.

9. Protéger vos comptes sur les réseaux sociaux.

- Mots de passe sécurisés
- Pour les fan pages ou celles où il est possible d'attribuer des rôles (administrateur, éditeur, modérateur, etc.) et des autorisations.
- Activez l'authentification à deux facteurs (2FA) avec des authentificateurs tels que Authy ou Google Authenticator au lieu du numéro de téléphone pour éviter le sim swapping * et la sauvegarde.

*Escroquerie par échange de carte SIM

10. Cyberhygiène



- Prendre soin de soi sur Internet et dans le monde réel
- Maintenir les systèmes d'exploitation et les logiciels à jour.
- Vérifiez régulièrement les paramètres de sécurité et de confidentialité.
- Faites le ménage (supprimez les anciens logiciels ou ceux que vous n'utilisez plus, supprimez les anciens fichiers ou ceux qui sont inutiles).

Merci !

www.innovusconsulting.co

Animateurs de la séance : Catalina Valenzuela, Paula Quiñones et Camilo Forero

Créatrice du module : Carolina Botero