Formation en sécurité informatique - GUIDE DU FORMATEUR

Notes:

- L'ordre et contenu peut changer selon l'audience et à la discrétion du formateur
- L'information en référence sera remise aux participants

Séance 1 (3h)

- **Présentation, remise de matériel** (15m)
  - Tour de table rapide pour évaluer les besoins et adapter la formation-atelier
    - Présentation du formateur/formatrice
  - Contexte des participants (OSBL? Commercial? Humanitaire? Commercial? Individu? Système d'exploitation/logiciels connus)
  - Buts recherchés, demandes spécifiques
  - Ressources utiles (liens, support) → document à produire
- **“Checklist” - les bonnes pratiques, sécuriser son environnement**: confidentialité, intégrité, accès (45m)
  - Je suis responsable, alerte: je reconnais les tentatives d'ingéniérie sociale
  - Je choisis de bons mots de passe je les protèges (XKCD, générateurs, Keepass)
  - J'utilise les outils et l'environnement indiqués selon le travail à faire
  - Je connais les risques associés aux communications en personne, ex: courriel (virus/maliciels, vol d'identité)
  - Quand je vais sur “le web” je prends des précautions: (TOR, https://, VPN, environnement et connection connus/fiables)
  - Je sécurise mon appareil/poste de travail (desktop, laptop, tablette, téléphone..) - “Clean disk policy”, tableaux, impression, notes, poubelles, filtre d'ecran, sécuriser son poste (Super-L, écran de veille)
  - Je sécurise mes accès à distance (SSH/RDP, chiffrement par tunnel, 2FA,..)
  - Je connais le classement des informations auxquelles j'ai accès et j'agis en conséquence (confidentiel, interne, public: “logout”, verrouillage de station, PIN, accès réseaux, clés USB, etc.)
    - Refuser un accès non-sécurisé, partager (ou pas) ses accès
  - Je protège les informations en transit (chiffrement sur clé, transport de stockage, bris physique, déni possible)
  - Quand je me débarasse de stockage brisé/inutilisé je prends les précautions d'usage (destruction, “wipe”, etc.)
- **Sécuriser ses données** (15m)
- Définitions:

Le secret, le transit, le stockage, la confidentialité, la protection de renseignements (accès), l'intégrité

Pause (10m)

- Chiffrement - définitions/discussion (15m)
  - [1] Protection de renseignements et accès anonyme (“Need to know”, accès réseaux/local, mots de passe)
  - [2] Chiffrement de fichiers (par mot de passe, par conteneur, disque complet)
  - [3] Chiffrement d'information en transit (messagerie instantanée, courriel, web)

Exercices pratiques - ateliers (1h)

- Installation et utilisation de logiciels
  - [1] KeepassX pour protéger ses mots de passe, Syspass.org pour accès web partagé (10m)
  - [2] GnuPG pour chiffrer les fichiers; mots de passe sur .ZIP, .DOC, etc. (10m)
    - Chiffrement, signature, confiance

Fin de séance

- Questions/difficultés, points à améliorer/suivis

Séance 2 (3h)

- Installation et utilisation de logiciels - ateliers
  - [2] OTR (pour Pidgin/Jabber), Silence (pour SMS/Android) (~20m)
  - [3] TOR (pour le web “anonyme), mode privé des navigateurs, CD amorçable Tails/autre
  - [3] Enigmail pour Thunderbird, Mailvelope pour le web (~45m+)

Pause (10m)

- [2] VeraCrypt pour conteneurs et chiffrement complet (sur USB/partitions), LUKS pour Gnu/Linux, Mac OS et son chiffrement intégré (45m+)
- Défis et difficultés

Tour de table et discussion sur les difficultés, améliorations possibles et suivi futur.