ACADÉMIE HUMANITAIRE · HUMANITAIRES JOBS

Mini MBA Sécurité et gestion des risques : protéger les équipes et garder l'accès

Support de cours · Semaine 9 : Sécurité numérique et protection de l'information

Programme de 3 mois exactement (12 semaines, 144 heures) pour gérer la sécurité et les risques d'une organisation humanitaire : devoir de protection, analyse du contexte, évaluation des risques, plans et procédures, acceptation et négociation de l'accès, incidents, gestion de crise et enlèvement, santé et bien-être du personnel, sécurité numérique et protection des données, risques de l'organisation et conformité, partage du risque avec les partenaires, gouvernance et continuité d'activité. Exercices chiffrés corrigés, trois examens mensuels avec études de cas, et un diplôme vérifiable de l'Académie Humanitaire.

https://humanitairejobs.org/fr/academie/mini-mba-securite-risques/semaine-9/

Document gratuit de l'Académie Humanitaire. Il peut être imprimé et partagé librement à des fins de formation, sans modification.

Semaine 9 : Sécurité numérique et protection de l'information

Objectifs

- Identifier les menaces numériques propres aux organisations humanitaires : hameçonnage, fraude au virement, surveillance, fuite de données.
- Mettre en place des mesures de base proportionnées : authentification, sauvegardes, chiffrement, gestion des accès, appareils.
- Protéger les données des personnes aidées et du personnel, et réagir à un incident numérique.

Pourquoi le numérique est un risque de sécurité

Les organisations humanitaires détiennent des informations très sensibles : listes de bénéficiaires (parfois avec biométrie et localisation), témoignages de violations, données médicales, informations sur le personnel, analyses de sécurité, mouvements. Une fuite ou un piratage peut mettre des **vies** en danger, pas seulement des données.

Plusieurs cyberattaques connues ont visé des organisations humanitaires, y compris le vol de données de centaines de milliers de personnes vulnérables. Les organisations sont aussi visées par la fraude financière en ligne et par la **surveillance** des communications par des acteurs étatiques ou non étatiques.

Menaces principales :

- **Hameçonnage** (phishing) : faux courriels ou messages qui volent des identifiants ou installent des logiciels malveillants.
- **Fraude au virement** : faux fournisseur, faux directeur demandant un paiement urgent, changement frauduleux de coordonnées bancaires.
- **Rançongiciel** : chiffrement des données contre rançon.
- **Vol ou saisie d'appareils** (ordinateurs, téléphones) aux points de contrôle ou lors de braquages.
- **Surveillance** des communications et des réseaux sociaux.
- **Erreurs internes** : partage par erreur, fichier envoyé au mauvais destinataire, mot de passe affiché.

Les mesures de base

Quelques mesures simples bloquent la grande majorité des attaques courantes :

- **Authentification à plusieurs facteurs** (MFA) sur la messagerie, le stockage en ligne, la banque et le logiciel comptable.
- **Gestionnaire de mots de passe** et mots de passe longs et uniques.
- **Mises à jour** automatiques des systèmes et des applications.

- **Sauvegardes** régulières, dont une copie hors ligne ou isolée, et tests de restauration (règle 3-2-1 : trois copies, deux supports différents, une copie hors site).
- **Chiffrement** des disques des ordinateurs portables et des téléphones.
- **Gestion des accès** : chacun n'accède qu'à ce dont il a besoin ; retrait des accès le jour du départ d'un employé.
- **Formation** régulière, avec des exercices d'hameçonnage simulés.

Exemple d'exercice. Un faux courriel d'hameçonnage est envoyé à 120 employés : 38 cliquent sur le lien (31,7 %), 14 saisissent leurs identifiants (11,7 %), 9 signalent le courriel au service informatique (7,5 %). Après une formation ciblée, un second exercice donne 12 clics (10 %), 3 saisies (2,5 %) et 41 signalements (34,2 %). La hausse des signalements est aussi importante que la baisse des clics : elle transforme le personnel en système d'alerte.

Fraude au virement et procédures financières

La **fraude au président** et la fraude aux coordonnées bancaires coûtent chaque année des sommes importantes aux organisations, y compris humanitaires. Les procédures financières sont la meilleure défense :

- Toute **modification de coordonnées bancaires** d'un fournisseur ou d'un employé est vérifiée par un appel à un numéro déjà connu, jamais à celui indiqué dans la demande.
- Aucun paiement urgent hors procédure, même à la demande apparente d'un directeur : la double validation reste obligatoire.
- Les accès à la banque en ligne utilisent des appareils et des comptes dédiés, avec double signature électronique.
- Le personnel sait qu'il sera **soutenu** s'il refuse un paiement suspect, même demandé par un supérieur.

> L'urgence et la confidentialité sont les deux leviers favoris des fraudeurs : « Je suis en réunion, fais ce virement tout de suite et n'en parle à personne. »

Appareils, points de contrôle et surveillance

Sur le terrain, les risques numériques sont aussi **physiques** :

- Aux points de contrôle, les téléphones peuvent être fouillés. Un téléphone qui contient des photos de positions militaires, des messages critiques envers une partie ou des listes de bénéficiaires peut entraîner une détention. Règle : ne transporter que le nécessaire, supprimer les données sensibles des appareils de terrain, utiliser des appareils dédiés au travail.
- Les **réseaux sociaux** du personnel révèlent des informations exploitables : localisation en temps réel, opinions politiques, photos de collègues, signes de richesse. Une politique sur l'usage des réseaux sociaux, expliquée et non punitive, réduit ces risques.
- Les **messageries** chiffrées de bout en bout protègent le contenu, mais pas le fait que l'on communique, ni le téléphone lui-même s'il est saisi déverrouillé.

- L'usage de certains outils (satellites, VPN, drones) peut être interdit ou suspect : vérifier la législation et l'acceptation.

Protéger les données des personnes

La **protection des données** des bénéficiaires et du personnel repose sur des principes reconnus (notamment le manuel du CICR et du Brussels Privacy Hub sur la protection des données dans l'action humanitaire) :

- **Licéité et finalité** : base légitime et finalité précise pour chaque collecte.
- **Minimisation** : ne collecter que ce qui est nécessaire.
- **Consentement éclairé** lorsque c'est la base retenue, en tenant compte des rapports de pouvoir (un ménage qui a besoin d'aide n'est pas libre de refuser).
- **Sécurité** : chiffrement, accès limités, journalisation.
- **Conservation limitée** et suppression à la fin de la finalité.
- **Partage encadré** par des accords de partage de données, avec une analyse des risques (y compris des demandes d'autorités ou de parties au conflit).
- **Analyse d'impact** avant tout nouveau système (biométrie, paiement mobile, plateforme partagée).

Exemple de minimisation. Pour une distribution de kits, il faut identifier le ménage et vérifier qu'il n'a pas déjà reçu le kit. L'appartenance ethnique ou religieuse n'est pas nécessaire et ne doit pas être collectée ; la photo et l'empreinte digitale ne le sont généralement pas non plus.

Réagir à un incident numérique

Un incident numérique (compte piraté, ordinateur volé, rançongiciel, fichier envoyé par erreur) se traite comme un incident de sécurité :

- **Contenir** : changer les mots de passe, révoquer les sessions, isoler l'appareil infecté, effacer à distance un appareil volé.
- **Évaluer** : quelles données, quelles personnes, quel risque pour elles ?
- **Informer** : direction, responsable de la protection des données, personnes concernées si elles sont exposées à un risque, autorités de contrôle selon le droit applicable, bailleurs selon les contrats.
- **Restaurer** à partir des sauvegardes ; ne pas payer une rançon sans décision de la direction et analyse juridique.
- **Apprendre** : analyse, corrections, formation.

Exemple. Un ordinateur portable non chiffré contenant la liste de 3 200 ménages avec leurs numéros de téléphone et leur localisation est volé lors d'un braquage. Le risque pour les personnes dépend du contexte : si certains ménages appartiennent à un groupe ciblé, il est élevé. Actions : évaluation immédiate, information des communautés concernées par des canaux sûrs si elles sont exposées, changement des modalités de contact, chiffrement obligatoire de tous les ordinateurs portables.

Exercice d'application : un courriel urgent du directeur

Situation. Un vendredi à 17 h, la comptable reçoit un courriel apparemment du directeur pays, en déplacement : « Confidentiel. Nous devons payer aujourd'hui l'acompte de 48 000 USD au nouveau fournisseur de carburant, sinon nous perdons le contrat. Coordonnées bancaires ci-jointes. Je ne suis pas joignable, réunion avec le ministre. » L'adresse d'envoi diffère d'une lettre de l'adresse habituelle. Le même jour, un fournisseur habituel a demandé par courriel de changer ses coordonnées bancaires. La messagerie de l'organisation n'a pas d'authentification à deux facteurs.

Travail demandé. 1) Signaux d'alerte. 2) Conduite immédiate. 3) Mesures durables.

Corrigé. 1) Urgence, confidentialité, indisponibilité du demandeur, nouveau fournisseur sans dossier d'achat, adresse d'envoi légèrement différente, demande parallèle de changement de coordonnées bancaires. 2) Ne pas payer ; appeler le directeur sur son numéro connu (ou son adjoint) ; ne pas modifier les coordonnées du fournisseur habituel sans appel de vérification à un numéro déjà connu ; signaler au responsable informatique et à la finance ; conserver les courriels comme preuves. 3) Authentification à deux facteurs sur toute la messagerie ; règle écrite : aucun paiement hors procédure, double validation, vérification téléphonique de toute modification bancaire ; formation et exercices d'hameçonnage ; filtrage des domaines ressemblants ; message clair de la direction : refuser un paiement suspect sera toujours soutenu.

À retenir

- Les données humanitaires sont sensibles : une fuite peut mettre des vies en danger.
- MFA, mots de passe uniques, mises à jour, sauvegardes 3-2-1, chiffrement, accès minimaux, formation.
- Fraude au virement : vérification par un numéro connu, double validation, soutien à qui refuse.
- Terrain : appareils allégés aux points de contrôle, politique sur les réseaux sociaux.
- Protection des données : finalité, minimisation, sécurité, conservation limitée, analyse d'impact.

Quiz

1. 150 employés reçoivent un faux courriel ; 24 cliquent. Taux de clic :
   A. 24 %
   B. 16 %
   C. 6,25 %
   D. 15 %

2. La règle de sauvegarde 3-2-1 signifie :
   A. 3 copies, 2 supports différents, 1 copie hors site
   B. 3 mots de passe, 2 facteurs, 1 compte
   C. 3 jours, 2 semaines, 1 mois
   D. 3 serveurs, 2 pays, 1 cloud

3. Un fournisseur demande par courriel de changer ses coordonnées bancaires. Vous :
   A. Changez immédiatement
   B. Payez en espèces
   C. Répondez au courriel
   D. Vérifiez par un appel au numéro déjà connu

4. Pour une distribution de kits, collecter l'appartenance ethnique des ménages est :
   A. Obligatoire
   B. Recommandé
   C. Contraire au principe de minimisation si ce n'est pas nécessaire
   D. Sans risque

5. Un ordinateur non chiffré contenant des listes de bénéficiaires est volé. Première étape :
   A. Racheter un ordinateur
   B. Évaluer les données exposées et le risque pour les personnes, puis informer
   C. Ne rien dire
   D. Publier un communiqué

Corrigé du quiz : 1. B · 2. A · 3. D · 4. C · 5. B