Livret d'animation du Cyber mystère

Par le GRADeS Inéa

Le Cyber Mystère est un module de sensibilisation à la cybersécurité vidéo conçu comme un plateau de jeu et visant à identifier la source d'une fuite de données en enquêtant au sein d'une entreprise fictive. **Pour y avoir accès et en faire bénéficier vos équipes, envoyez un mail à l'équipe cyber du GRADeS : equipecyber@esante-hdf.fr**

Ce module de sensibilisation et son animation dure en moyenne 45 minutes.

MISSION : ENQUETE SUR UNE FUITE DE DONNEES

- ➔ *Rôle* : Consultant(e) externe en cybersécurité
- ➔ *Lieu* : Entreprise **Chromelis**
- ➔ *Objectif* : Identifier, parmi **8 collaborateurs**, l'origine de la fuite de données sensibles

Vous commencez dans le **bureau de la Directrice Générale**, en présence du **RSSI** (Responsable de la Sécurité des Systèmes d'Information). Ils vous exposeront la situation. Ensuite, vous mènerez votre investigation dans les différents services de l'entreprise.

Conseils pour réussir

- ➔ Analysez chaque échange avec attention
- ➔ Croisez les informations récoltées
- ➔ **Prenez des notes** tout au long de l'enquête ! Elles vous seront précieuses pour identifier la personne responsable.

L'enquête n'est pas contextualisée santé, nous ne voulons pas stigmatiser un métier et les personnages hauts en couleurs sont là pour illustrer avec humour des attitudes clés… et rappeler des enjeux bien réels.

1. ROSA - ADMIN RESEAU

Mauvais réflexe observé

- Rosa n'a **pas signalé une activité suspecte nocturne** sur le réseau.
- Elle a considéré que « cela arrive parfois » mais n'a pas appliqué la procédure d'alerte.

Objectif pédagogique auprès des participants

- Les amener à repérer que **tout comportement anormal** sur le réseau doit être **signalé sans délai**, même si cela semble anodin.
- Débattre : *Qu'est-ce qu'une activité suspecte ? Qui doit être alerté ?*

Recommandations

- Toujours remonter les anomalies (activité inhabituelle, connexions hors horaires, tentatives de login répétées).
- Ne jamais banaliser un comportement réseau atypique.
- Connaître et appliquer les **processus d'escalade** (RSSI, DPO, support informatique…).
- Tenir un journal de bord des incidents.

2. RUBEN - COMPTABILITE

Mauvais réflexe observé

- Ruben utilise :
  - Une **clé USB personnelle** ;
  - Son **adresse mail personnelle**

…pour traiter des données comptables sensibles.

Objectif pédagogique

- Faire comprendre pourquoi l'usage d'outils personnels est dangereux :
  - Absence de protection antivirus/antimalware,
  - Risque de fuite non maîtrisée,
  - Absence de traçabilité.

Recommandations

- N'utiliser **que des supports USB professionnels chiffrés** et gérés par l'entreprise.
- Interdiction systématique des mails personnels pour des données métier.
- Utiliser les espaces sécurisés fournis par l'organisation (intranet, cloud pro, partage réseau).
- Chiffrer les documents sensibles si mobilité.

3. MALO - COMMERCIAL

Mauvais réflexe observé

- Malo s'est **connecté à la boîte mail de sa responsable** en son absence pour traiter un dossier.
- Cela implique qu'il a **accès ou connaissance de son mot de passe**.

Objectif pédagogique

- Débattre :
  - Des risques du **partage de mots de passe** ;
  - Du contournement des droits d'accès ;
  - Des alternatives sécurisées existantes.

Recommandations

- Ne **jamais partager un mot de passe**, même pour dépanner.
- Créer des espaces partagés sécurisés :
  - SharePoint,
  - Cloud professionnel,
  - Drive métier,
  - Dossiers réseau.
- Utiliser un **gestionnaire de mots de passe** pour les comptes *réellement* partagés (fonction, par personne).
- Configurer des **délégations d'accès** plutôt que partager un compte.

4. KYAN - CHARGE D'ACCUEIL

Mauvais réflexe observé

- Manque de rigueur dans le **contrôle des identités** des visiteurs ou intervenants.

Objectif pédagogique

- Amener les participants à discuter :
  - Des pratiques de contrôle dans leur établissement ;
  - De la gestion des accès physiques ;
  - Des risques liés à l'ingénierie sociale (personne se faisant passer pour un technicien, par ex.).

Recommandations

- Vérifier systématiquement l'identité des visiteurs.
- Ne jamais laisser entrer quelqu'un « parce qu'il a l'air de connaître ».
- Mettre en place un registre ou badge visiteur.
- Accompagner toute personne extérieure dans les zones sensibles.
- Sensibiliser à l'ingénierie sociale : toujours valider une intervention auprès du service concerné.

5. PRUNE – RESPONSABLE COMMERCIALE

Mauvais réflexe observé

- Prune a **partagé son mot de passe** avec un ou plusieurs collaborateurs.

Objectif pédagogique

- Faire prendre conscience :
  - Des problèmes de **traçabilité** ;
  - Des risques en cas de fraude ou erreur ;
  - De la responsabilité engagée.

Recommandations

- Un mot de passe = une personne = une responsabilité.
- Utiliser les **délégations d'accès**.
- Mettre en place une **politique de mots de passe forte**.
- Activer la **double authentification** pour les accès sensibles.

6. AMBRE - SECRETARIAT

Mauvais réflexe observé

- Ambre ne vérifie pas correctement l'identité de ses interlocuteurs **au téléphone**.

Objectif pédagogique

- Faire réfléchir :
  - Au risque de divulgation d'informations à des personnes non autorisées ;
  - Aux techniques d'hameçonnage vocal (vishing).

Recommandations

- Valider l'identité de l'appelant (questions de contrôle, numéro interne connu).
- Ne jamais transmettre :
  - Des mots de passe,
  - Des données personnelles,
  - Des documents sensibles par simple appel.
- Proposer un rappel via un **numéro officiel de l'entreprise**.
- Former le personnel à détecter les appels suspects.

7. JADE - STAGIAIRE

Mauvais réflexe observé

- Jade imprime des **documents sensibles** et les laisse traîner / ne connaît pas la règle.

Objectif pédagogique

- Sensibiliser à l'enjeu :
  - De l'impression maîtrisée,
  - De la confidentialité des documents papier,
  - Du clean desk.

Recommandations

- Utiliser l'option **impression sécurisée** (badge ou code).
- Ne jamais laisser un document sensible dans le bac d'impression.
- Éviter d'imprimer si cela n'est pas indispensable.
- Détruire immédiatement les documents obsolètes (broyeur ou poubelle sécurisée).

8. RESPONSABLE RH – CLEMENT

Mauvais réflexe observé

- Le bureau de Clément est **mal rangé** : dossiers ouverts, documents sensibles accessibles.

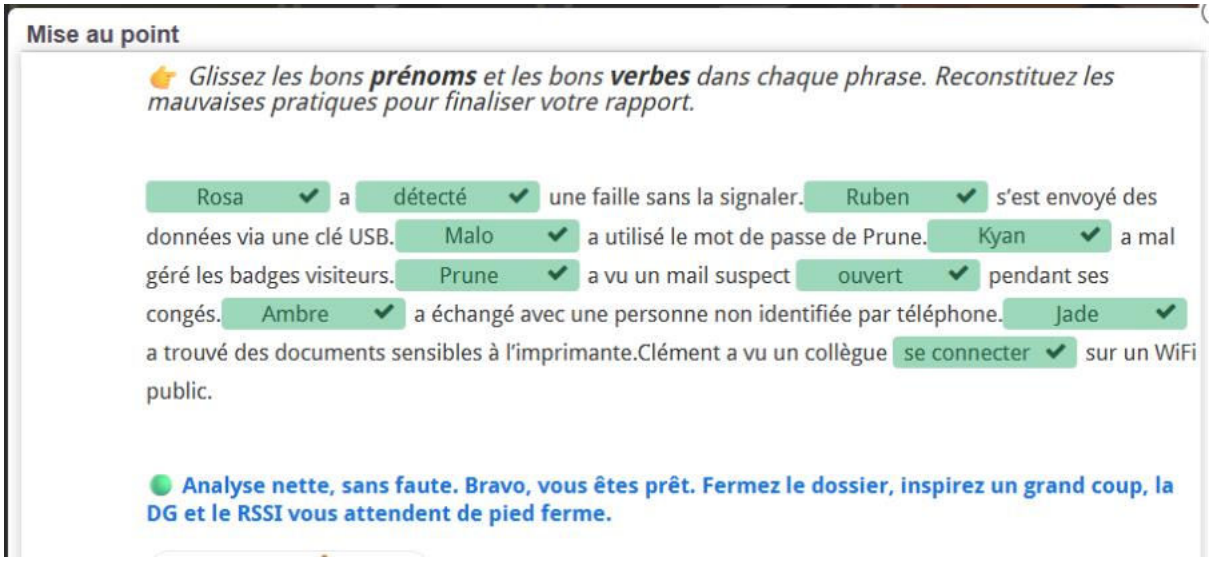
Objectif pédagogique

- Montrer les risques :
  - De fuite involontaire,
  - D'accès non autorisé,
  - De violation RGPD.

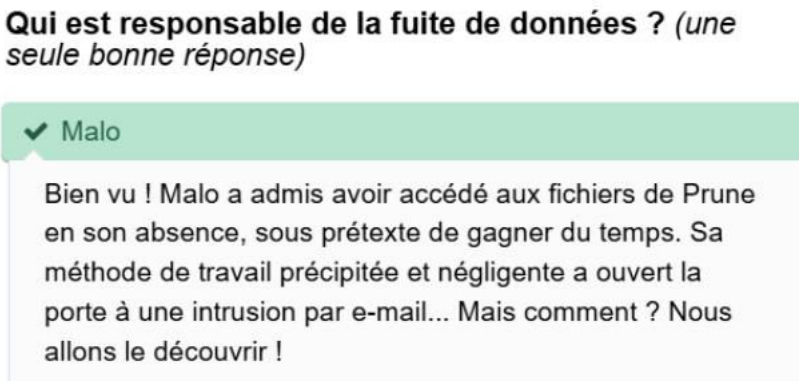
Recommandations

- Appliquer systématiquement la règle du **clean desk** :
  - Rien de sensible ne doit rester visible en absence.
  - Ranger les dossiers dans des armoires fermées à clé.
  - Éloigner les documents sensibles des zones de passage.
  - Verrouiller son poste à chaque absence, même courte.

Mise au point



MISSION ACCOMPLIE



Vous avez identifié l'origine de la fuite de données chez Chromelis.

Votre vigilance en cybersécurité a fait la différence.

⚠ *Une simple mauvaise pratique peut avoir de graves conséquences pour toute l'organisation.*

CE QU'IL FAUT RETENIR

- ➔ **La cybersécurité repose sur la vigilance humaine autant que sur la technologie**
- ➔ **Chaque collaborateur** joue un **rôle clé** dans la protection des données
- ➔ Les **bonnes pratiques** appliquées au quotidien font toute la différence