Table des matières

Compétence B3 : Utiliser les médias basés sur la technologie

> Le format distanciel permet une meilleure visibilité des pratiques individuelles, favorise les échanges et réduit le stress lié à la proximité physique. – Rogers, C. (1980)

Liens rapides :

Le mindmap collaboratif

Utiliser un mind map collaboratif en direct sur la cybersécurité est à la fois pédagogique et engageant, surtout pour des formateurs qui comprendront immédiatement l'intérêt de cet outil didactique.

Voici une liste de questions structurées pour guider votre brainstorming en 5 à 10 minutes, conçues pour faire émerger les branches logiques de votre carte mentale (Risques, Causes, Conséquences, Solutions)

Description : L'Expérience comme Ressource Centrale (Knowles) via la Cartographie Mentale Collective (Buzan). Ce concept opérationnalise le principe andragogique de Malcolm Knowles : l’adulte apprend en reliant le nouveau savoir à son expérience riche et diversifiée. Pour concrétiser cette co-construction, j’utilise un tableau blanc partagé supportant une cartographie mentale collective(méthode Tony Buzan). La structure rayonnante de la carte permet de visualiser et d’organiser les idées et vécus des apprenants autour d’un concept central. Ancrée dans la cognition située, chaque branche ancre la théorie dans un contexte pratique réel, transformant ainsi l’expérience individuelle en une intelligence collective visible.

Avantages : Valorisation : Rend visible et légitime l'expérience de chaque adulte, boostant la motivation et l'engagement (principe de Knowles). Ancrage mémoriel renforcé : La double codification (visuelle chez Buzan + sémantique par les pairs) favorise une rétention durable des concepts. Transfert immédiat : Les solutions co-construites sont directement issues de contextes réels, facilitant l'application en situation de travail. … Inconvénients : Risque de domination : Les participants les plus extravertis ou expérimentés peuvent monopoliser l'espace visuel au détriment des autres. Surcharge cognitive : La simultanéité des contributions peut créer un « chaos visuel » si la eModération n'est pas rigoureuse. Dépendance technique : Nécessite une maîtrise minimale de l'outil et une connexion stable ; peut exclure les apprenants en fracture numérique. …

Utilité : Groupes de praticiens : Idéal lorsque le formateur agit comme facilitateur pour structurer le savoir déjà présent dans le groupe (application directe de Knowles). Résolution de problèmes complexes : Pour cartographier les causes et effets basés sur le vécu terrain (cognition située), notamment lors de phases d'analyse de pratiques. Phases de synthèse : Pour co-construire un aide-mémoire opérationnel qui servira de support de transfert post-formation.

Liens avec d'autres concepts : L'Apprentissage Social (Social Learning - Bandura) : Concept clé où l'apprentissage se fait par l'observation et l'imitation des pairs. La Cognition Distribuée (Hutchins) : Théorie selon laquelle la connaissance n'est pas seulement dans la tête de l'individu, mais répartie entre les membres du groupe et leurs outils (ici, le tableau blanc). Le groupe "pense" mieux ensemble grâce à l'outil.

Vos remarques et questions : Le passage d'une prise de notes linéaire (individuelle) à une structure rayonnante (collective) représente-t-il une barrière cognitive pour certains adultes, et comment la lever rapidement ?

Phase 1 : Les Enjeux (Pourquoi ? - Quel est la motivation du hacker)

Objectif : Déclencher la première branche sur les "Gain/Motivation".

- À quoi ça sert concrètement à un cybercriminel d'avoir vos identifiants ?(Réponses attendues : argent, vol d'identité, accès aux données, espionnage)
- Si je vous donne mes mots de passe aujourd'hui, qu'est-ce qu'ils pourront 'acheter' ou 'faire' avec ?(Élargir vers les services financiers, réseaux sociaux, emails pro)
- Le but est-il toujours le gain financier immédiat, ou y a-t-il d'autres motivations ?(Faire apparaître : sabotage, fuite de données, usurpation)

Phase 2 : Les Vecteurs d'Attaque (Comment ? - Le risque)

Objectif : Créer la branche sur les "Méthodes/Pirater".

- "Concrètement, comment obtiennent-ils ces mots de passe sans force brute ?"(Phishing/hameçonnage, rejets de cookies, fuites de bases de données…)

- “Quelles sont nos petites habitudes de sécurité qui facilitent leur travail ?”(Mots de passe faibles, mêmes mots de passe partout, partage sur papier/post-it, pas de 2FA)
- “Où se passe souvent la faille humaine lors de la connexion ?”(Fausses pages de connexion, liens dans les emails, Wi-Fi public non sécurisé)

Phase 3 : Les Conséquences (L'impact)

Objectif : Une branche sur les “Effets/Risques” pour sensibiliser.

- “Une fois l'accès obtenu, quelle est la première chose qu'ils font généralement ?”(Changement de mot de passe pour verrouiller la victime, demande de rançon, envoi de mails aux contacts)
- “Au-delà de la perte financière, quels sont les risques réputationnels ou émotionnels ?”(Diffamation, chantage, perte de données privées/confidentielles)

Phase 4 : Les Parades (La résolution de problème)

Objectif : Terminer par la branche “Solutions/Protection”, positive et constructive.

- “Comment rendre cette 'porte numérique' beaucoup plus difficile à ouvrir pour eux ?”(Longueur du mot de passe, complexité, unicité)
- “Puisqu'on ne peut pas tout mémoriser parfaitement, quel outil centralisateur recommandons-nous ?”Gestionnaire de mots de passe / Coffre-fort numérique)
- “Et si le mot de passe est quand même trouvé, quelle sécurité supplémentaire bloque l'intrus ?”(Authentification à deux facteurs - 2FA/MFA)
- “En tant que formateurs, comment pouvons-nous changer les comportements plutôt que juste la technique ?”(Sensibilisation continue, simulation de phishing, culture de la vigilance)

Conseil pour le timing (5-10 min) :

- Min 0-2 : Posez les questions 1 et 2. Remplissez la branche “Motivations”.
- Min 2-4 : Questions 4, 5 et 6. Remplissez la branche “Vecteurs d'attaque”.
- Min 4-6 : Questions 7 et 8. Remplissez la branche “Conséquences”.
- Min 6-9 : Questions 9, 10 et 11. Remplissez la branche “Solutions”.
- Min 9-10 : Conclusion rapide et lien avec votre outil didactique (montrer comment ce Mind Map permet justement de visualiser ces interconnexions complexes).

Cette approche montre non seulement la pertinence du contenu (cybersécurité), mais valide aussi la puissance de l'outil (mind mapping) pour structurer la pensée collective. Bonne présentation !

Bibliographie & Ressources

- Knowles, M. S., Holton III, E. F., & Swanson, R. A. (2015). The Adult Learner: The definitive classic in adult education and human resource development (8e éd.). Routledge. (Ouvrage de référence sur l'andragogie et le rôle de l'expérience).
- Buzan, T., & Buzan, B. (2010). The Mind Map Book: How to Use Radiant Thinking to Maximize Your Brain's Untapped Potential. Penguin Books. (Fondements de la cartographie mentale et de la structure rayonnante).
- Hutchins, E. (1995). Cognition in the Wild. MIT Press. (Théorie de la cognition distribuée dans les systèmes collaboratifs).

Navigation de retour

Liens rapides :

- Compétence B Mener
- B3 Medias

---

competence, B3, médias-numériques, distanciel, SAMR, sobriété-numérique, Rogers, pédagogie-active, Teams

Page mise à jour le {{date | Auteur : Eugénie Decré | Version : 1.0 - Compétence B3}}