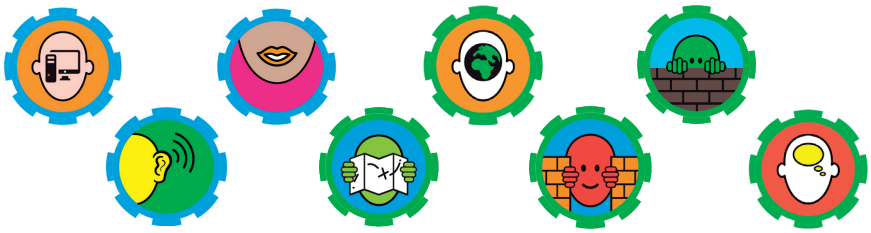
Scénario 6 : NAVIGUER EN LIGNE EN TOUTE SÉCURITÉ

Préambule



L'objet de cette démarche est de fournir des propositions de travail réfléchies et testées collectivement. Ce n'est pas un mode d'emploi strict.

Dans cette perspective, l'absence de prérequis est intentionnelle. La démarche vise à être à votre service en tant que formateur, offrant une flexibilité pour être adaptée aux groupes que vous animez, à leurs projets, ainsi qu'à leurs compétences en communication orale, écrite et en mathématiques. Il vous revient également d'organiser le temps en fonction des connaissances des participants, de leur rythme d'apprentissage et des questions qui peuvent surgir.

Certains objectifs liés aux langages fondamentaux ont été mentionnés.
Ils ne sont pas exhaustifs et dépendront de la manière dont chaque formateur conçoit et mène l'animation en fonction des objectifs de formation de son groupe. Vous les repérerez grâce aux pictogrammes correspondants et aux encadrés.

Ces démarches sont conçues en tenant compte de la vision de « Lire et Écrire » autour du numérique : face à une société hyper digitalisée, il est essentiel de nous outiller et de réfléchir à nos usages afin que cela ne devienne pas un obstacle à notre autonomie[1].

Matériel général

- Ordinateurs, téléphone portable (GSM)
- Rétroprojecteur
- Connexion Wifi

Objectifs

- Reconnaître et comprendre les menaces liées à la sécurité informatique ;
- Identifier et partager les bonnes pratiques pour assure une meilleure sécurité numérique, en mettant l'accent sur les mesures préventives et les habitudes sécurisées.

[1] Pour plus d'informations sur la vision de Lire et Écrire concernant le numérique, veuillez vous référer au Cadre de Référence des Compétences Numériques : (https://lire-et-ecrire.be/Cadre-de-reference-des-competences-numeriques-de-Lire-et-Ecrire)

Scénario 6 : DÉROULEMENT

ÉTAPE 1 : Emergence

Objectifs

- Echanger et comparer les différentes représentations du concept de sécurité ;
- Réfléchir collectivement ;
- Associer des exemples de la vie quotidienne à des questions sécuritaires.

Matériel (fourni) et (à se procurer)

- Photolangage « **Se protéger - 1. Sécurité** »

- Magazines, crayons, feutres, etc.

Le formateur affiche les images du photolangage pour que tous puissent les voir. *Qu'est-ce que c'est ?*

→ Ensuite, le formateur veille à faire émerger le concept de sécurité. *Qu'est ce qui est commun entre les photos ?*

Opportunité de travailler l'écriture des mots.

Après avoir identifié oralement les objets présentés dans le photolangage, chaque apprenant reçoit une feuille reprenant les photos et s'exerce à écrire chaque mot.

Cette activité peut aussi se faire avec une approche ludique. Par exemple, en sous-groupes, chaque groupe reçoit une feuille avec les photos et des cartes de lettres (chaque carte représentant une lettre de l'alphabet). Ensemble, ils discutent pour identifier chaque objet, puis utilisent les cartes de lettres pour épeler et écrire les mots dans les cases appropriées. Une fois tous les mots écrits, les résultats sont mis en commun et vérifiés de manière collective.

Ensuite, le formateur propose au groupe que chacun trouve une image représentant la sécurité. Par exemple :

- En utilisant des magazines ;
- En leur proposant de dessiner ;
- En fonction du travail effectué en amont avec le groupe, il est également envisageable de leur demander de réaliser une recherche d'image sur Internet.

→ Mise en commun des représentations de chacun.

ÉTAPE 2 : Introduction à la sécurité numérique

Objectifs

- Distinguer la sécurité dans le contexte physique et la sécurité dans le domaine numérique ;
- Identifier les méthodes de protection physique et de protection numérique d'un GSM ;
- Comprendre l'importance de sécuriser l'accès à son téléphone ;
- Nourrir le lexique du groupe autour de la sécurité numérique.

Matériel (fourni)

Photolangage « **Se protéger - 2. Sécurité numérique - GSM** ».

Le formateur montre une photo de l'écran d'un téléphone portable demandant le mot de passe. Il pose la question suivante :

La sécurité dans le contexte physique et la sécurité dans le contexte numérique, est-ce la même chose ?

Pour rendre la question plus concrète, le formateur demande :

Comment protéger son GSM ?

→ Ensemble, on veille à identifier les manières de protéger son GSM en différenciant la protection physique de la protection numérique.
Le formateur peut utiliser le photolangage pour animer cette activité.

À travers le travail collectif, le groupe identifie les méthodes de protection physique de leur GSM (coque de téléphone, étui de protection, verre trempé, etc.), ainsi que les méthodes de protection numérique (code de déverrouillage, empreinte digitale, reconnaissance faciale, etc).

Le formateur poursuit l'animation en demandant :

Pourquoi est-il important de protéger l'accès à son téléphone ?
Qu'y a-t-il à l'intérieur ?

Avez-vous un code pour accéder à votre téléphone ?
Quel type de code utilisez-vous ?

→ Ensemble, identifier les types de codes de déverrouillage utilisés dans le groupe (digicode, empreinte digitale, reconnaissance faciale, schéma ou absence de code).

Proposition de prolongement :

C'est l'occasion de pratiquer le vocabulaire appris sur les différents types de déverrouillage. Un tableau à double entrée est utilisé (les noms des apprenants sur une entrée et les différents types de déverrouillage sur l'autre). Des croix sont placées pour indiquer les types de déverrouillage utilisés par chaque apprenant.
Les apprenants posent ensuite des questions :

« Est-ce que tu utilises ton doigt pour déverrouiller ton téléphone ? »

« Est-ce que tu utilises ton visage pour déverrouiller ton téléphone ? »

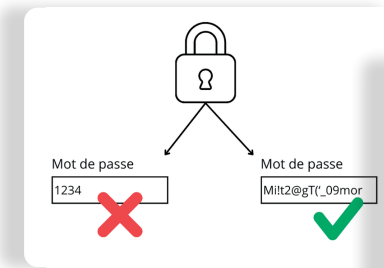
ÉTAPE 3 : Situer ses connaissances en matière de sécurité numérique

Objectifs

- Construire un état des lieux autour des connaissances du groupe des menaces liées à la sécurité informatique ;
- Partager les expériences vécues et les stratégies activées ;
- Se questionner sur les conséquences des menaces de sécurité ;
- Classer les menaces selon leur fréquence d'occurrence ;
- Analyser les scénarios de menace à partir de vidéos illustratives (cfr page 6) ;
- Utiliser un lexique progressif pour faciliter la compréhension des concepts de sécurité numérique.

Matériel (fourni)

Photolangage « **Se protéger - 2. Sécurité numérique - Bonnes pratiques** »



Réflexion adressée au formateur :

Les menaces « hors ligne » et « en ligne » ont des points communs. Si l'idée de risquer de se faire arnaquer ou de cliquer sur le mauvais lien peut être inquiétante, rappelez-vous que le vol de données ou d'argent et les arnaques existaient avant l'ère numérique.

Par exemple :

Tromperie : utiliser une histoire crédible en apparence pour arnaquer	*Je me trouve dans un magasin, le vendeur me promet que le téléphone portable qu'il essaie de me vendre est neuf et de bonne qualité. Je dépense beaucoup d'argent, mais une semaine plus tard, il se casse et je n'ai aucune garantie pour le retour.*	*Je navigue sur un site web proposant des prix très bas pour des téléphones portables. Je décide d'en acheter un, mais le colis ne me parvient jamais, il s'agissait d'une fausse entreprise.*
Distraction	*Je suis distrait, quelqu'un me vole mon téléphone sans que je m'en rende compte.*	*Je suis distrait, je clique sur un lien malveillant sans faire attention.*

Le formateur demande au groupe :

Avez-vous déjà rencontré des problèmes de virus sur vos appareils ?

Vous êtes-vous déjà fait « arnaquer » sur Internet ?

Comment pensez-vous pouvoir protéger votre vie privée lorsque vous utilisez des réseaux sociaux ou des applications mobiles ?...

Quelles mesures avez-vous mises en place ? À quoi il faut faire attention ?

→ La discussion offre l'opportunité de dresser un état des lieux des stratégies mises en place, que le groupe répertorie sur une affiche.

L'occasion de travailler sur la notion de fréquence se présente. *Selon vous, est-ce que ces menaces sont fréquemment rencontrées ou non ?* Le groupe classe les menaces en fonction de ce critère.

Le formateur projette une vidéo qui illustre une menace de sécurité numérique. Regarder la vidéo autant de fois que nécessaire et progressivement, analyser le contenu de la vidéo.

Commencer par :

Qui sont les personnages principaux ? Où se trouvent-ils ?

→ Lors des visionnages suivants, avancer vers :

Qu'est-ce qui s'est passé ? Pourquoi cela est-il arrivé ?
Quelles ont été les conséquences de cela ?
Comment aurait-on pu éviter cela ?

Voici quelques vidéos qui expliquent de manière illustrée, avec peu de texte, le fonctionnement de certaines menaces à la sécurité numérique.

Scénario d'attaque de ransomware :
https://www.youtube.com/watch?v=bSp6gSp5KT4

Scénario d'attaque de phishing :
https://www.youtube.com/watch?v=dych1UN8WX0

C'est quoi le piratage informatique ? :
https://youtu.be/Lnpn-AZ9Qzo?si=dRCCTuFi59e30cgz

Penser à élaborer un lexique progressivement afin de faciliter la compréhension et l'assimilation des concepts.

Voici un exemple : avec les apprenants, choisir des images associées aux mots abordés lors de la séance. Imprimer deux cartes par mot.

Jouer à un jeu de mémoire : toutes les cartes sont placées face cachée, et l'objectif est de les retourner une à une pour former des paires en associant les images. Si deux images identiques sont retournées, dire le mot correspondant.
S'il n'est pas dit, cela ne compte pas comme une paire réussie.

Ressources en soutien au formateur pour alimenter ses connaissances :

Webinaire : Sécurité en ligne - Replay. 123 Digit :
https://www.youtube.com/watch?v=kTzvRZm5XIw&list=PL7GY6JIsmrdRJIf_434PqLQo9P6usOyB5&index=8

Capsule 2 : Les indices d'une arnaque en ligne (123 Digit) :
https://www.youtube.com/watch?v=yrZUlUQJXJM

Box Numérique : 9.1. Les essentiels de la sécurité en ligne :
https://www.interface3namur.be/documentation/box-numerique/fiches-outils/securite/les-essentiels-de-la-securite-en-ligne/

Box Numérique : 9.2. Les différents types de menaces :
https://www.interface3namur.be/documentation/box-numerique/fiches-outils/securite/les-differents-types-de-menaces/

ÉTAPE 4 : Explorer les bonnes pratiques du numérique

Objectifs

- Identifier des stratégies de protection ;
- Analyser les bonnes pratiques proposées dans le photolangage ;
- Effectuer des recherches et collecter des données sur les pratiques de protection ;
- Créer une liste des astuces de sécurité numérique identifiées.

Matériel (fourni)

Photolangage « **Etape 3 et 4 se protéger (bonnes pratiques)** ».

Le formateur montre des images sur les bonnes pratiques :

Quel message transmet chaque image ? Avons-nous déjà parlé de l'un d'eux dans les étapes précédentes ?

→ Après avoir passé en revue les images qui restent sur la table, proposer de jouer à un jeu de rôle. Deux volontaires sont sollicités, ils choisissent une photo et sortent de la salle avec le formateur.

→ Il leur explique ce que représente cette image et les apprenants doivent ensuite faire une représentation pour expliquer aux autres ce que montre l'image.

Proposition de prolongement :

C'est une opportunité de mener des recherches et de travailler sur la collecte et l'analyse des données. Chaque apprenant s'engage à interroger deux personnes de leur entourage sur une pratique qu'ils ont mise en place pour se protéger.

Avec le soutien du photolangage, les apprenants sont invités à placer un autocollant sur les pratiques qui ont été mentionnées. En cas de nouvelles pratiques, réfléchir à la manière de les représenter en image. Une autre possibilité est de leur demander à l'avance d'apporter une trace visuelle de la pratique que chaque personne interrogée raconte.

Le formateur propose de poursuivre l'enrichissement de l'affiche sur les pratiques de sécurité en ligne commencée à l'**Étape 3**. Le groupe ajoute les nouvelles astuces qui ont émergé lors de cette étape.

Quelles informations souhaitons-nous y inclure ?

→ Ensuite, le groupe réfléchit pour déterminer quelles actions sont pertinentes pour le groupe et lesquelles ne le sont pas.
Une méthode consiste à voter à main levée ou à placer des autocollants à côté des suggestions.

Ressources en soutien au formateur pour alimenter ses connaissances :

7 façons de se protéger contre la cybercriminalité :
https://www.youtube.com/watch?v=C84hkYrLdpI

Safe on Web : Comment mieux protéger notre compte :
https://campagne.safeonweb.be/fr/authentification-a-2-facteurs

Cybersimple.be : nombreux conseils pour se protéger en ligne :
https://www.cybersimple.be/fr/homepage

AlphaNumérique.ca : Vidéo Sécurité en ligne :
https://alphanumerique.ca/espace-public/ressources/securite-en-ligne-trucs-et-astuces/

Vidéos de sensibilisation et de prévention du risque numérique :
https://cybermalveillance.gouv.fr/cybermenaces

Box Numérique : Thématique 9 Sécurité. (9.7. Localiser son smartphone ; 9.8. Sécuriser son PC ; 9.9. Sécuriser ses données sur PC) :
https://www.interface3namur.be/documentation/box-numerique/fiches-outils/securite/31569/

ÉTAPE 5 : Appliquer les bonnes pratiques du numérique

Objectifs

- Réfléchir, valoriser et partager ses connaissances ;
- Mettre ses connaissances au service du groupe ;
- S'approprier les pratiques identifiées.

Une fois que l'affiche a été complétée, il est temps de travailler sur l'appropriation des pratiques. Elaborer une ligne du temps sous forme de calendrier.

→ Le groupe organise des moments dédiés à travailler sur chaque pratique, en se fixant des objectifs et des échéances.

Le formateur utilise des exercices déjà existants pour travailler sur ce sujet (voir **« Pour s'entraîner »**).

→ En sous-groupes, les exercices sont réalisés, ce qui crée des moments d'échange et d'analyse.

Pour s'entraîner :

Thématique Sécurité en Ligne (123Digit!) :
Comment créer un mot de passe sécurisé ? / Découvrir la sécurité sur internet / Comment protéger ses données personnelles ?

123Digit : Jeu « traque l'arnaque » : pour apprendre à reconnaître les indices de phishing : https://www.123digit.be/fr/ressources-pedagogiques/traque-larnaque

Safe on Web
(proposition pour des groupes plus avancés en lecture et en écriture)

Testez votre santé digitale :
https://campagne.safeonweb.be/fr/testez-votre-sante-digitale

Faites le test du mot de passe :
https://safeonweb.be/fr/test-du-mot-de-passe

Ressources en soutien au formateur pour alimenter ses connaissances :

→ Cf. Etape 3

ÉTAPE 6 : Élaboration d'une charte sur les « Conseils généraux de sécurité numérique »

Objectifs

- Construire une trace commune qui rassemble les bonnes pratiques que les apprenants voudraient implémenter dans leur vie ;
- Créer un outil adapté aux besoins du groupe ;
- Communiquer, collaborer et coopérer avec les membres du groupe.

Matériel (à se procurer)

Tout autre matériel que le formateur juge nécessaire pour réaliser l'animation : magazine, colle, ciseaux, etc.

En s'appuyant sur l'affiche construite au long de cette démarche, le groupe réfléchit à la manière de compiler les bonnes pratiques pour assurer une utilisation sécurisée du numérique.

Quel format choisir pour notre charte ?
Comment présenter visuellement notre charte ?
(exemples : photos, collages, écritures, enregistrements audio, etc.)

→ *Quelles tâches sont nécessaires pour réaliser la charte ?*
De quoi avons-nous besoin ?

Il est également possible de restreindre le contenu de la charte et de se concentrer sur un axe spécifique, par exemple les mots de passe.

ÉTAPE 7 : Évaluation formative

Objectif

Réfléchir à ses propres apprentissages.

Chaque apprenant est encouragé à choisir :

- 2 choses / sujets / pratiques qu'il connaissait déjà ;
- 2 choses / sujets / pratiques qu'il a mieux compris, consolidés après cette démarche ;
- 2 découvertes.

Projet réalisé avec
le soutien du Fonds ING pour une société plus digitale, géré par la Fondation Roi Baudouin,
et le soutien de la Fédération Wallonie-Bruxelles