FICHE ATELIER

Sécurité numérique

Mots de passe • Arnaques • Vie privée

Semaine 6

Durée : 1h30 à 2 heures	**Participants :** 4 à 8 personnes
Matériel : Smartphones, tablettes ou PC	**Niveau :** Débutant – échanges clés

OBJECTIFS DE L'ATELIER

A la fin de cet atelier, les participants seront capables de :

- Créer et gérer un mot de passe solide
- Reconnaitre les arnaques en ligne (phishing, faux appels)
- Protéger leur téléphone avec un code de verrouillage
- Comprendre ce qu'est une connexion sécurisée (cadenas, https)
- Identifier les informations à ne jamais partager en ligne

DEROULEMENT DE L'ATELIER

1. **Introduction – 'Avez-vous déjà été piège ?' (15 min)**
   Tour de table ouvert. Recueillir les expériences : SMS suspects, faux appels, email bizarre...
2. **Les mots de passe : pourquoi et comment ? (25 min)**
   Expliquer les risques d'un mot de passe simple. Méthode de la phrase-code. Exercice : créer un mot de passe fort.
3. **Reconnaitre une arnaque (20 min)**
   Montrer des exemples réels (email phishing, SMS frauduleux, faux appel). Checklist pour ne pas se faire piéger.
4. **La connexion sécurisée (15 min)**
   Expliquer le cadenas HTTPS dans le navigateur. Reconnaitre un vrai site officiel vs un faux.
5. **Protéger son téléphone (20 min)**
   Code de verrouillage, double authentification, mises à jour. Exercice : activer le verrouillage si absent.
6. **Ce qu'on ne partage jamais en ligne (15 min)**
   Liste concrètes : code bancaire, numéro sécu, mot de passe, photos de documents...
7. **Questions et remise fiche usager (10 min)**

Synthèse collective. Temps libre pour questions. Distribution fiche récapitulative.

CONSEILS POUR L'ANIMATEUR

⚠ POSTURE RECOMMANDEE

Partir des expériences vécues des participants – beaucoup auront déjà eu peur ou été victimes

Ne pas dramatiser : l'objectif est de donner confiance, pas de générer de la peur

Être concret : montrer de vrais exemples d'arnaques (captures d'écran imprimées ou projetées)

Rappeler que même les experts se font parfois piéger – c'est la vigilance qui protège

Respecter la confidentialité : certains participants peuvent avoir été victimes d'arnaques financières

ERREURS FREQUENTES A ANTICIPER

Confondre le code PIN de la carte bancaire avec le mot de passe du téléphone

Croire qu'un site avec le cadenas est forcément fiable (expliquer nuance)

Penser que seuls les gens 'crédules' se font arnaquer

Utiliser le même mot de passe partout – aborder sans culpabiliser

RESSOURCES ET PREPARATION

Avant l'atelier	• Préparer 3 exemples imprime ou projetés d'arnaques réelles (phishing, SMS) • Prévoir des feuilles pour l'exercice 'créer un mot de passe' • Tester la démonstration du cadenas HTTPS sur le navigateur • Identifier les participants qui n'ont pas de code de verrouillage
Supports à distribuer	• Fiche usager 'Sécurité numerique' (1 par participant) • Exercice pratique imprime (reconnaissance arnaques + quiz)