Sécurité numérique

Mots de passe • Arnaques • Protection

Atelier inclusion numérique

Objectif : Sensibiliser aux bonnes pratiques de la sécurité numérique

Duree : 1h30 | **Public :** Débutants

Pourquoi se protéger en ligne ?

Arnaque financière

Piratage de compte, virement forcé

Vol d'identité

Usurpation de vos données personnelles

Accès à votre téléphone

Photos, contacts, comptes pirates

Phishing

Faux emails pour voler vos mots de passe

Faux appels

Imposteurs se faisant passer pour banque ou administration

Creer un mot de passe solide

✗ Mot de passe FAIBLE

- ✗ 1234
- ✗ azerty
- ✗ votrenom
- ✗ date de naissance
- ✗ motdepasse

☑ Mot de passe FORT

La méthode PHRASE-CODE

3 mots du quotidien + 1 chiffre + 1 symbole

Exemple : Chat!Velo92

- ✓ Au moins 8 caractères
- ✓ Majuscules + minuscules + chiffres
- ✓ Un symbole spécial (! @ # $ %)
- ✓ Jamais votre nom ou date de naissance
- ✓ Un mot de passe DIFFÉRENT par site important

Les 5 signes qui doivent vous alerter

1 

Urgence artificielle

On vous dit que vous devez agir TOUT DE SUITE

2 

Gain ou remboursement inattendu

Vous avez gagné un prix que vous n'avez pas demande

3 

Demande de mot de passe

Aucun organisme sérieux ne demande ça

4 

Lien ou adresse bizarre

L'adresse email ou le site contient des fautes ou caractères étranges

5 

Menace ou peur

Votre compte va être suspendu si... – c'est une manipulation

Phishing : exemples reels

Comment reperer un faux message ?

✗ FAUX SMS – Exemple

"Votre colis est bloque. Payez 1,80eur de frais de douane : http://livraison-24h.net/pay"

⚠ URL suspecte, paiement inattendu

✗ FAUX EMAIL – Exemple

"De : serviceclient@ameli-sante-fr.com
Objet : Remboursement de 87,60 eur en attente
Cliquez ici pour recevoir votre virement..."

⚠ Adresse email avec tirets suspects

EN CAS DE DOUTE : Ne cliquez pas – Contactez directement l'organisme par telephone

☑ **Les vrais organismes (banque, ameli, impots) ne demandent JAMAIS :**
vos mots de passe • votre code bancaire • un virement urgent par email ou SMS

Reconnaitre un site securise

Le cadenas HTTPS

Dans la barre d'adresse de votre navigateur, un cadenas ferme = la connexion est chiffrée.
Cliquez dessus pour voir les détails du certificat.

Adresse FIABLE

- https://www.ameli.fr
- https://www.impots.gouv.fr
- https://www.service-public.fr

Adresse SUSPECTE

- http://ameli-sante-fr.com
- https://impots-remboursement.net
- http://service--public.fr

Securiser son telephone

Code de verrouillage

Activez un code PIN ou schéma sur votre ecran d'accueil – empêche l’accès si perdu

Mises à jour

Acceptez les mises à jour : elles corrigent les failles de sécurité. Activez les mises à jour automatiques.

Wi-Fi public

Evitez de consulter votre banque ou vos mots de passe sur un Wi-Fi de cafe ou gare.

Applications : Telechargez uniquement depuis l'App Store (Apple) ou Google Play (Android).

Localisation : Désactivez la localisation pour les applications qui n'en ont pasbesoin.

Ce qu'on ne partage JAMAIS

Meme avec quelqu'un en qui vous avez confiance

Votre code bancaire (CB)

Votre banque ne vous le demandera jamais par telephone ou email

Votre numero de securite sociale

Ce numero suffit pour usurper votre identite

Vos mots de passe

Meme a un ami, un technicien ou un agent de support

Scan de votre carte d'identite ou passeport

Uniquement sur des sites officiels que vous avez vous-meme contactes

Votre IBAN ou RIB complet

Sauf pour recevoir un virement que VOUS avez demande

Votre adresse precise

Sur les reseaux sociaux ou a un inconnu en ligne

Mes 5 reflexes de securite

Un mot de passe long et unique pour chaque compte important

Je ne clique jamais sur un lien suspect, meme si c'est urgent

Je verifie le cadenas HTTPS avant de saisir mes informations

Mon telephone a un code de verrouillage active

Je ne communique jamais mon code ou mot de passe a personne