FICHE MÉMO · SÉCURITÉ NUMÉRIQUE · PETIT RAPPEL (1/2)

Les expressions à connaître

En préambule : la sécurité numérique, un espace commun

Dans cette formation, la sécurité numérique est traitée comme **un espace commun**, et non appareil par appareil. Smartphone, tablette et ordinateur partagent **les mêmes comptes**, **les mêmes mots de passe** et attirent **les mêmes escrocs** : une faille sur l'un met en danger les autres. Quel que soit son matériel, chacun apprend donc **les mêmes bons réflexes**, ensemble.

Un lien	Un mot souligné ou une adresse (https://...) sur lequel on appuie pour **ouvrir une page Internet**. **Attention :** il peut mener vers un faux site qui ressemble au vrai.
Un SMS	Un **message écrit** reçu sur le téléphone, envoyé à mon numéro (appli Messages). **Attention :** n'importe qui peut envoyer un SMS au nom de ma banque ou d'un service public.
WhatsApp	Une **application gratuite** pour écrire, appeler et envoyer des photos par Internet. Mon compte est lié à mon numéro. **Attention :** un escroc qui obtient mon code de vérification prend mon compte.
Un mail	Un **courrier électronique**, reçu dans ma boîte (Gmail, Orange, Outlook...). **Attention :** le nom de l'expéditeur affiché peut être faux.
Une appli	Un **programme** installé sur le téléphone ou la tablette (banque, météo, WhatsApp...). **Attention :** je n'en installe que depuis le Play Store ou l'App Store.

FICHE MÉMO · SÉCURITÉ NUMÉRIQUE · PETIT RAPPEL (2/2)

Les expressions à connaître

Un code	Quelques chiffres reçus par SMS ou dans une appli (« code de vérification », « code de confirmation ») pour **prouver que c'est bien moi**. **Attention :** il ne se donne à personne, même à ma banque.
Une mise à jour	Une nouvelle version du téléphone, de l'ordinateur ou d'une appli, qui **corrige des failles de sécurité**. **Attention :** je n'accepte que celles proposées par l'appareil lui-même (Paramètres, Réglages, Windows Update, Play Store, App Store), jamais celles d'une fenêtre qui surgit sur un site.
Un spam	Un **message non sollicité** (publicité ou arnaque) envoyé en masse par mail, SMS ou appel. On dit aussi « pourriel ». **Attention :** je ne réponds pas et je ne clique pas ; je le signale (33700 pour un SMS, bouton « Spam » de ma messagerie).
L'hameçonnage	Une tentative pour me faire donner **mes mots de passe ou ma carte**, par un faux message aux couleurs d'un organisme connu. En anglais : « phishing ». **Attention :** aucune banque ni administration ne demande ces informations par message.
Un malware	Un **logiciel malveillant** (virus, espion, rançongiciel) qui s'installe à mon insu, par une pièce jointe, un lien ou une fausse appli. **Attention :** il touche aussi bien le téléphone que la tablette ou l'ordinateur. Je n'installe rien d'inconnu.

Un même escroc vise mon téléphone, ma tablette et mon ordinateur : je protège tout, partout.

FICHE MÉMO N°1 · SÉCURITÉ NUMÉRIQUE

Les 7 règles d'or du CIM.PP

1. **Ma banque ne me demande jamais** un code, ma carte ou un virement par téléphone.
2. Un **code reçu par SMS** ne se donne **à personne**, jamais.
3. Je **ne clique jamais sur un lien** reçu par SMS ou par mail : je vais moi-même sur le site ou l'appli officielle.
4. **Urgence + secret + argent = arnaque.** Je raccroche et je rappelle moi-même.
5. Un proche me demande de l'argent ? Je **le rappelle sur son numéro habituel** et je demande notre **mot de passe familial**.
6. J'accepte les **mises à jour proposées par mon appareil** (Paramètres ou Réglages, Windows Update, Play Store, App Store), **jamais** celles qui surgissent sur un site ou dans un message. Je **sauvegarde** mes photos.
7. En cas de doute, **j'en parle à un proche ou au club** avant d'agir.

VICTIME D'UNE ARNAQUE ?

1. J'appelle ma banque pour **faire opposition**. 2. J'appelle **Info Escroqueries : 0 805 805 817** (gratuit) ou je vais sur **17cyber.gouv.fr**. SMS frauduleux : je le transfère au **33700**.

FICHE MÉMO N°2 · SÉCURITÉ NUMÉRIQUE

Au téléphone

LE PIÈGE	MON BON RÉFLEXE
Le faux conseiller bancaire	
Le **vrai numéro de ma banque** s'affiche. Il veut un code, une validation dans l'appli ou ma carte.	**Je raccroche** et j'appelle le numéro au dos de ma carte. Je ne remets **jamais** ma carte.
Le faux proche en détresse (voix imitée)	
La **voix de mon petit-fils**, imitée par l'IA : un accident, de l'argent tout de suite, « n'en parle à personne ».	**Je le rappelle** sur son numéro habituel. Je demande notre **mot de passe familial**.
Le faux technicien	
« Ici Microsoft » : mon ordinateur aurait un virus. Il veut que j'installe un logiciel.	Microsoft et Apple **n'appellent jamais**. Je raccroche et je n'installe **rien** à la demande d'un inconnu.
L'appel d'une sonnerie et le démarchage	
Une seule sonnerie pour que je rappelle un numéro surtaxé. Des offres insistantes (isolation, panneaux solaires).	Je **ne rappelle pas** un numéro inconnu. Je ne signe rien le jour même. Je m'inscris sur **bloctel.gouv.fr**.

Le numéro affiché ne prouve rien : je raccroche et je rappelle moi-même.

FICHE MÉMO N°3 · SÉCURITÉ NUMÉRIQUE

SMS, mails et messageries

LE PIÈGE	MON BON RÉFLEXE
Le faux SMS (colis, Ameli, amende, impôts)	
« Votre colis est en attente, réglez 1,99 € » avec un lien vers un faux site qui vole ma carte.	**Je ne clique pas.** Je le transfère au **33700** (gratuit), puis je le supprime.
Le faux mail de la banque ou d'un organisme	
Aux couleurs de ma banque, d'EDF ou de la CAF : « mettez à jour vos informations », sinon suspension.	Je regarde **l'adresse de l'expéditeur**. Je vais **moi-même** sur le site ou l'appli officielle.
« Maman, j'ai changé de numéro »	
Un numéro inconnu se fait passer pour mon enfant et me demande de payer une facture urgente.	J'appelle **l'ancien numéro** de mon proche avant tout paiement.
Le code « envoyé par erreur »	
Un « ami » sur WhatsApp me demande de lui renvoyer un code reçu par SMS : son compte est piraté.	Un code ne se donne **jamais**. J'active la **double authentification**.

Un message pressant avec un lien ? Je ne clique pas : je vérifie moi-même.

FICHE MÉMO N°4 · SÉCURITÉ NUMÉRIQUE

Sur Internet et l'ordinateur

LE PIÈGE	MON BON RÉFLEXE
L'écran bloqué « Appelez Microsoft »	
Une alarme sonne, l'écran se bloque : « Virus détecté, appelez le 09… ».	**Je n'appelle pas.** Je ferme le navigateur ou je redémarre l'ordinateur.
Les vidéos truquées et les faux placements	
Une célébrité vante un placement « garanti » sur Facebook ou YouTube. La vidéo est fabriquée par IA.	Aucune célébrité ne conseille de placement. Un gros rendement **garanti n'existe pas**.
Les faux sites et les QR codes piégés	
Démarches payantes qui imitent l'État, boutiques à prix cassés, autocollant QR sur une borne.	Je vérifie **l'adresse du site** (l'État : « .gouv.fr »). Je préfère l'appli officielle.
Le faux amour et le faux emploi	
Un(e) inconnu(e) charmant(e) finit par demander de l'argent. Un travail à domicile qu'il faut payer.	Je n'envoie **jamais d'argent** à quelqu'un que je n'ai jamais vu. J'en parle à un proche.
La fausse mise à jour	
Sur un site, une fenêtre surgit : « Votre navigateur est obsolète » ou « Votre antivirus a expiré, installez la mise à jour ».	Je ferme la fenêtre. Je fais mes mises à jour **uniquement** depuis les Paramètres (ou Réglages), Windows Update, le Play Store ou l'App Store.

FICHE MÉMO N°5 · SÉCURITÉ NUMÉRIQUE

Victime ? Que faire

J'agis vite et sans honte : les escrocs sont des professionnels.

1. **Je bloque ma carte** : j'appelle ma banque (numéro au dos de la carte) ou j'utilise son appli.
2. **Je change mes mots de passe**, celui de ma messagerie en premier.
3. **Je garde les preuves** : SMS, mails, numéros, captures d'écran. Je n'efface rien.
4. **Je coupe le contact** et je me méfie des faux « services de récupération d'argent ».
5. **Je porte plainte** au commissariat, à la gendarmerie ou en ligne.

Info Escroqueries
0 805 805 817
Gratuit · lun.-ven. 9 h-18 h 30

Aide en ligne 17Cyber
17cyber.gouv.fr
Diagnostic et échange avec un policier

SMS ou appel indésirable
33700
Je transfère le SMS, gratuit

Soutien aux victimes
116 006
France Victimes · gratuit, 7 j/7

Fraude à ma carte
Perceval
sur service-public.gouv.fr

Stop au démarchage
bloctel.gouv.fr
Inscription gratuite

LE CLUB RESTE À VOTRE ÉCOUTE

Ces fiches **ne sont pas exhaustives** : de nouvelles arnaques apparaissent sans cesse. Malheureusement, **l'intelligence artificielle** les rend plus crédibles (voix imitées, vidéos truquées, messages sans fautes).

Le CIM.PP suit l'actualité et se fait un devoir de vous tenir informés. **Un doute ? Parlez-en au club.**

Mes numéros à moi (à remplir)

Opposition de ma banque : _____

Mon proche de confiance : _____

Mon animateur au club : _____