CMP INVESTIGATION

ÉDITION 2026

Particuliers Collaborateurs

Guide des bons réflexes numériques

Comprendre, détecter et agir face aux risques numériques de la vie courante, au bureau comme à la maison.



Réalisé par CMP Investigation
Détective privé · Agrément CNAPS

cmp-investigation.com

Le premier rempart, c'est vous

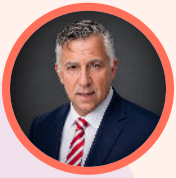
Messageries, banque en ligne, outils collaboratifs, démarches administratives : le numérique est devenu le prolongement naturel de notre vie privée comme de notre vie professionnelle. Il simplifie nos échanges, accélère notre travail et nous relie les uns aux autres.

Cette facilité a un revers. Les escrocs n'attaquent plus seulement les machines : ils s'adressent d'abord à nous. Un faux conseiller bancaire, un e-mail qui imite un fournisseur, un SMS de livraison… Un instant d'inattention suffit parfois à exposer une famille ou une entreprise.

En vingt ans de gendarmerie, puis comme enquêteur privé, j'ai constaté que la plupart des préjudices auraient pu être évités par un geste simple : s'arrêter quelques secondes, vérifier, et oser en parler.

Ce guide a été pensé pour cela. Nul besoin d'être expert : chaque page donne des repères concrets, applicables dès aujourd'hui, chez vous comme au travail.

> **La meilleure protection reste un utilisateur averti, qui prend le temps de vérifier avant d'agir.**



Philippe Priolon
Fondateur de CMP Investigation
Détective privé · Analyste en cybercriminalité

Un guide fait pour vous

Il s'adresse à chacun : salarié, dirigeant, agent public, retraité, parent… à toute personne qui utilise un ordinateur, un smartphone, une messagerie ou des services en ligne, au travail comme à la maison. Chaque page va droit au but pour vous aider à reconnaître une situation à risque, à prendre du recul et à choisir le bon geste.

Lisez-le d'une traite ou allez directement au thème qui vous concerne :

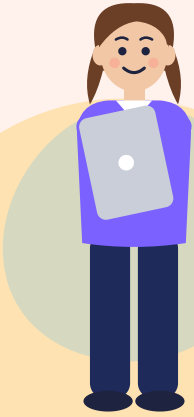
Manipulation · Signaux d'alerte · Attaques courantes · Bons réflexes · Mots de passe · Données · Intelligence artificielle · Sécurité physique · Déplacements · À la maison · Que faire en cas d'incident

En haut de chaque page, un repère indique l'étape abordée. Trois étapes structurent tout le guide :

1 · Comprendre
Comment fonctionnent les attaques, pourquoi la manipulation marche, et ce que vos habitudes changent.

2 · Détecter
Les indices qui doivent éveiller votre attention et les formes d'attaques les plus répandues.

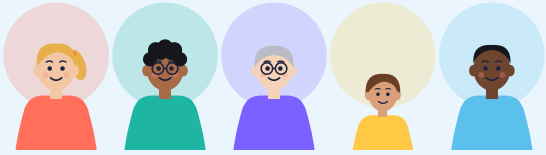
3 · Agir
Les gestes qui protègent vos comptes, vos données et vos appareils, et comment signaler un doute.



Pourquoi nous sommes tous concernés

La cybermalveillance ne vise pas que les informaticiens ou les grandes entreprises. Elle s'invite dans les gestes de tous les jours : consulter ses mails, payer en ligne, partager un fichier, répondre à un appel, valider une commande.

Concrètement, cela prend la forme d'un compte piraté, d'un faux message, d'une demande pressante, d'une information divulguée trop vite ou d'un accès détourné.



504 000+	victimes accompagnées en 2025 sur Cybermalveillance.gouv.fr, soit +20 % en un an.
+70 %	pour l'hameçonnage, première menace tous publics confondus.
+170 %	de fraudes au virement : faux RIB, faux fournisseurs, faux conseillers.
+45 %	pour le piratage de comptes et l'hameçonnage, en tête des menaces chez les professionnels.

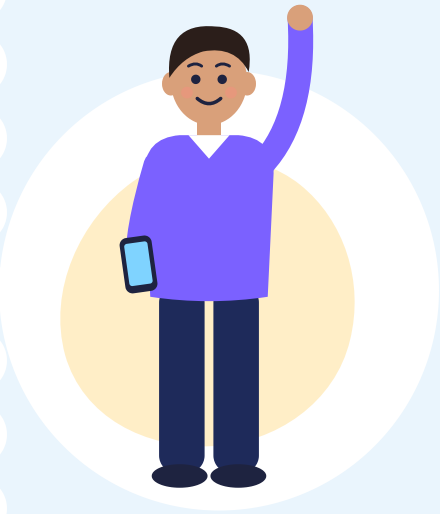
Source : Cybermalveillance.gouv.fr, bilan d'activité 2025 (publié en mars 2026).

Derrière chaque chiffre, il y a une famille, un salarié, une entreprise. La protection repose autant sur la technique que sur des usages maîtrisés et des alertes données à temps.

Des menaces réelles, des gestes simples

Une attaque se présente rarement comme telle. Elle ressemble à un moment banal de votre journée, ce qui la rend efficace. Elle commence souvent par :

1. un message reçu
2. un appel inattendu
3. un lien à ouvrir
4. un fichier à partager
5. un code à communiquer
6. un QR code à scanner
7. un paiement à valider
8. une discussion en public

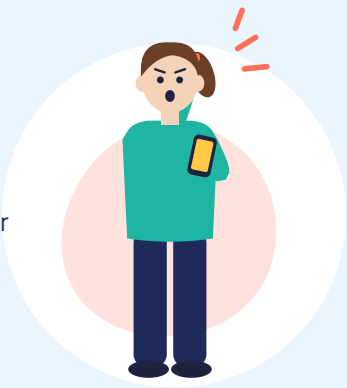


Les bonnes pratiques ne demandent aucune compétence technique. Elles demandent seulement de marquer une pause quand une situation paraît inhabituelle, pressante ou difficile à vérifier.

Un réflexe numérique n'est pas une contrainte de plus : c'est une vérification de quelques secondes, au bon moment. Avant de cliquer, de répondre, de payer, de transmettre ou de partager.

STOP je m'arrête → **VÉRIFIER** par un autre canal → **SIGNALER** en cas de doute

L'escroc vise d'abord vos émotions



Beaucoup d'attaques n'exploitent aucune faille informatique : elles exploitent nos réactions humaines. C'est l'**ingénierie sociale**. L'attaquant s'appuie parfois sur ce que vous publiez sur les réseaux sociaux pour paraître crédible. Son but : vous faire agir vite, cliquer, ouvrir, scanner, rappeler ou transmettre. Connaître ses leviers, c'est reprendre la main.

L'urgence

Un délai très court, une action « immédiate » exigée.

L'autorité

Un dirigeant, une banque, la police ou l'administration semble écrire.

La confiance

Un logo familier, un prénom connu, un contexte qui paraît vrai.

La curiosité

Une pièce jointe intrigante, une photo, un « document important ».

La peur

Menace d'amende, de blocage de compte, de poursuites ou de pénalité.

L'entraide

On sollicite votre aide, votre gentillesse ou votre réactivité.

LE RÉFLEXE Plus on vous presse d'agir, plus il faut ralentir.

Les indices qui doivent alerter

Avant de cliquer, de répondre ou de transmettre quoi que ce soit, certains détails méritent qu'on s'arrête.

- **Un expéditeur douteux.** Adresse ou numéro presque identique à un contact connu.
- **Une pression pour agir vite.** On vous pousse à réagir sans prendre le temps de contrôler.
- **Un lien ou un fichier imprévu.** Vous n'attendiez rien, ou le contexte de l'envoi reste flou.
- **Une demande de discrétion.** « Gardez ça pour vous », sortir de la procédure habituelle.
- **Une demande sensible.** Mot de passe, code SMS, coordonnées bancaires, fichier client.
- **Un ton qui sonne faux.** Trop pressant, trop vague, ou inhabituel chez cette personne.



AVANT D'AGIR, TROIS QUESTIONS

- Est-ce que je l'attendais ?
- Est-ce cohérent ?
- Puis-je vérifier autrement ?

08 · ENTRETIEN

« Le point d'entrée est presque toujours humain »



Philippe Priolon · Fondateur de CMP Investigation

Près de vingt ans en gendarmerie, enquêteur spécialisé dans le trafic d'œuvres d'art et la cybersécurité, aujourd'hui détective privé agréé CNAPS et analyste en cybercriminalité. Il livre son regard d'enquêteur sur les réflexes qui protègent.

Pourquoi la cybersécurité n'est-elle pas qu'une affaire d'informaticiens ?

Dans les dossiers que je traite, la brèche commence rarement par une machine. Elle commence par quelqu'un qui clique, qui répond ou qui fait confiance. Les techniciens protègent les systèmes ; chacun de nous protège ses accès, ses informations et ses échanges.

Qu'apportent vraiment les gestes du quotidien ?

Vérifier un expéditeur, verrouiller son écran, ne jamais dicter un code, passer par le bon canal : chaque geste ferme une porte. Pris isolément, ils paraissent modestes. Additionnés, ils compliquent sérieusement le travail d'un attaquant.

« Je ne suis pas une cible intéressante. » Vrai ou faux ?

Faux. L'escroc ne cherche pas forcément quelqu'un d'important : il cherche un accès. La boîte mail d'un salarié ou d'un grand-parent suffit pour piéger tout un carnet d'adresses, préparer une fraude au virement ou gagner la confiance d'autres victimes.



Comment cultiver le doute sans tomber dans la méfiance ?

Douter, ce n'est pas soupçonner tout le monde. C'est s'accorder le droit de poser une question quand quelque chose paraît pressé, bizarre ou incohérent. Un enquêteur ne croit rien sur parole : il vérifie. C'est la même posture, en version quotidienne.

Pourquoi signaler, même quand on n'est pas sûr ?

Signaler n'est pas avouer une faute, c'est un acte de responsabilité. Plus l'alerte est rapide, plus on limite les dégâts. Et une fausse alerte n'est jamais du temps perdu : elle entretient la vigilance de tous.

IA, faux appels, usurpations : quelle attitude adopter ?

Voix clonées, vidéos truquées, messages sans une faute : les arnaques gagnent en crédibilité. La parade, elle, ne change pas : ne pas céder à l'urgence, raccrocher puis rappeler sur un numéro connu, convenir en famille ou en équipe d'un mot de vérification.

Comment ancrer ces réflexes dans la durée ?

Par des consignes courtes, des cas concrets, des rappels réguliers et des mises en situation. Les managers, comme les parents, donnent le ton par l'exemple. La sécurité ne doit pas freiner l'activité : elle doit la rendre sereine.

À RETENIR

Au moindre doute : **je m'arrête, je prends du recul, je vérifie** par un autre canal. Vérifier ne ralentit pas : cela protège.

Les attaques les plus répandues



E-mail, téléphone, SMS, QR code, visio ou objet physique : le canal varie, l'objectif reste le même. Vous faire cliquer, répondre, payer ou divulguer sans avoir vérifié.

PHISHING
Hameçonnage
Un e-mail imite un service connu pour vous faire cliquer.

SPEAR PHISHING
Hameçonnage ciblé
Un message sur mesure, nourri de détails vrais sur vous.

VISHING
Faux appel
Faux conseiller, faux support : on vous met sous pression.

DEEPFAKE
Visio frauduleuse
Une identité usurpée, ou une demande de partage d'écran.

SMISHING
SMS piégé
Colis, amende, CPF : un lien vers un faux site.

QUISHING
QR code piégé
Un QR code collé ou envoyé redirige vers un leurre.

MESSAGERIES
Proche usurpé
« J'ai changé de numéro, peux-tu m'avancer de l'argent ? »

SUPPORT PHYSIQUE
Clé USB inconnue
Trouvée ou offerte, elle peut cacher un logiciel malveillant.

Faux profils sur les réseaux, faux PDF générés par l'IA… les techniques évoluent, **le piège reste le même : agir sans vérifier.**

7 réflexes à adopter



Avant de cliquer, interrogez le contexte. Ces gestes simples vous protègent au quotidien.

1 Contrôlez l'expéditeur

Adresse e-mail, numéro, identité réelle de la personne.

2 Examinez les liens

Survolez ou appuyez longuement pour lire la vraie adresse avant d'ouvrir.

3 Méfiez-vous des pièces jointes

Ouvrez-les seulement si elles sont attendues, d'un expéditeur vérifié, dans un contexte logique.

4 Gardez vos secrets

Mot de passe et codes ne se donnent jamais, même à votre « banque ».

5 Raccrochez et rappelez

Sous pression au téléphone, ne transmettez rien. Rappelez via un numéro que vous connaissez.

6 Utilisez les outils de protection

Bouton de signalement, antivirus, mises à jour, service informatique : ils sont là pour vous.

7 Au moindre doute, signalez

Prévenez votre service informatique, votre banque ou utilisez le canal de signalement prévu.

Chaque réflexe compte. Ensemble, on se protège mieux.

Attendu ? · Cohérent ? · Urgence justifiée ?

Vos identifiants sont des clés



Un compte ouvre bien plus qu'une messagerie : documents, outils métiers, espaces partagés, contacts, banque, photos de famille. C'est pourquoi les identifiants sont si convoités : ils permettent à un attaquant de circuler dans vos systèmes ou de se faire passer pour vous.

Un mot de passe par compte

Si un service est piraté, les autres restent à l'abri.

Une phrase de passe

Longue et imprévisible, elle résiste mieux qu'un mot court.

Un coffre-fort numérique

Ni post-it ni fichier ouvert : un gestionnaire de mots de passe reconnu.

La double authentification

Activez-la partout où c'est possible : elle bloque l'intrus même s'il a votre mot de passe.

Un code reste secret

Jamais communiqué, même à quelqu'un qui paraît légitime ou pressé.

Un écran verrouillé

Même pour deux minutes : Windows + L, ou verrouillage automatique du téléphone.

Vos accès sont personnels. Les protéger, c'est protéger **votre identité numérique, vos proches, vos collègues** et votre organisation.

Tout ne se partage pas



Certaines informations concernent des personnes, des clients, des finances ou le fonctionnement interne d'une structure. Elles ne portent pas toujours la mention « confidentiel », mais deviennent sensibles dès qu'elles circulent trop largement ou par le mauvais canal.

Données personnelles	Identité, adresse, téléphone, justificatifs, informations RH ou de santé : à ne transmettre que si c'est réellement nécessaire.
Informations internes	Organigramme, procédures, plannings, comptes rendus, captures d'écran : elles révèlent comment fonctionne votre organisation.
Clients et partenaires	Contrats, devis, factures, historiques d'échanges : ils engagent la confiance de tiers et ne circulent qu'entre personnes concernées.
Éléments financiers	RIB, bons de commande, budgets, demandes de virement : tout changement inhabituel se vérifie par un canal connu avant d'agir.

AVANT DE TRANSMETTRE, QUATRE QUESTIONS

- **Qui en a besoin ?**
- **Pour quoi faire ?**
- **Par quel canal ?**
- **Y a-t-elle droit ?**

L'IA générative : utile, avec un cadre

Reformuler, résumer, structurer, expliquer : bien encadrée, l'IA est un vrai assistant. Deux précautions : surveiller ce qu'on lui confie, prendre du recul sur ce qu'elle répond. Elle aide, elle ne décide pas.



DEUX QUESTIONS À SE POSER

- **Ai-je le droit de partager cette information ?**
- **Ai-je vérifié la réponse obtenue ?**

Avant de lui confier une information

Données personnelles, RH ou clients, contrats, code, identifiants : jamais dans un outil non validé. À la maison, gardez pour vous papiers d'identité et relevés bancaires.

Avant de réutiliser une réponse

Claire et assurée ne veut pas dire juste. Vérifiez les faits importants, relisez les formulations, respectez les règles internes.

À retenir

L'IA fait gagner du temps, pas du jugement. Votre regard critique reste le dernier filtre.

Numérique ou physique : mêmes réflexes



Une information peut fuir sans jamais être envoyée : sur un écran visible, une feuille oubliée, un appel passé en public ou un ordinateur laissé seul.

Un écran à la vue de tous

Open space, train, salle d'attente : quelqu'un peut lire par-dessus votre épaule.

Un document papier

Contrat, facture, liste de contacts oubliés sur l'imprimante ou jetés sans être détruits.

Une conversation entendue

Un nom de client, un projet, une date clé, une difficulté interne lâchés en public.

Un équipement laissé seul

Ordinateur, téléphone, badge, clé USB, carnet : autant d'accès à vos données et à vos locaux.

Un Wi-Fi inconnu

Un réseau public peut être piégé et capter vos échanges ou vos identifiants.

À RETENIR

Les bons réflexes numériques **valent aussi pour le monde physique** : écran, papier, voix, matériel, connexion.

Hors du bureau, on garde le cap

Train, hôtel, café, domicile : en déplacement ou en télétravail, les repères changent. Pas besoin de s'inquiéter en permanence, seulement d'adapter ses habitudes pour protéger ce que l'on consulte, transporte ou partage.



LE CONSEIL DE L'ENQUÊTEUR

Un ordinateur volé, c'est parfois un dossier entier qui disparaît. Chiffrez vos disques et sauvegardez régulièrement.

01 Avant de partir

N'emportez que l'indispensable. Appareils à jour et protégés, accès testés, outils autorisés par votre organisation.

02 Pendant le trajet

Écran verrouillé dès que vous vous levez, filtre de confidentialité, affaires jamais laissées seules.

03 En télétravail

Un espace à l'écart, des appels discrets, un poste verrouillé, une box sécurisée et les outils prévus.

04 Au retour

Rangez ou détruisez les papiers inutiles, vérifiez votre matériel, signalez vite toute perte.

Partout, l'information reste sensible : **protégez vos appareils, limitez ce que vous emportez, évitez les regards** et signalez sans tarder toute perte.

Chez soi aussi, les bons réflexes



Les escrocs ne font pas de différence entre vie privée et vie professionnelle. Un compte personnel piraté peut ouvrir la porte à l'entreprise, et inversement.

Faux conseiller bancaire

Votre banque ne vous fera jamais valider ou déplacer de l'argent par téléphone.

Achats en ligne

Sites reconnus, paiement sécurisé, méfiance face aux prix trop beaux.

Mises à jour et sauvegardes

Mises à jour automatiques, copie régulière de vos photos et papiers.

Réseaux sociaux

Profil restreint, pas de vacances en direct, aucune photo de documents.

Enfants et aînés

Parlez des arnaques et convenez d'un mot secret pour démasquer un faux proche.

Démarches officielles

Sites en .gouv.fr uniquement. Une amende ne se paie jamais via un SMS.

Un doute sur un appel ou un message ? **Raccrochez, puis appelez vous-même** le numéro officiel figurant sur votre carte, votre contrat ou le site de l'organisme.

Vous avez cliqué ? Réagissez vite.



Personne n'est infaillible. Ce qui compte, c'est la rapidité de la réaction.

1. **Isolez** l'appareil : coupez le Wi-Fi ou le câble réseau, sans l'éteindre ni rien effacer.
2. **Prévenez** votre service informatique ; pour un paiement, faites opposition auprès de votre banque.
3. **Changez vos mots de passe** depuis un autre appareil sain.
4. **Conservez les preuves** : captures d'écran, messages, numéros, références de virement.
5. **Signalez et portez plainte** : police, gendarmerie ou en ligne.

CONTACTS UTILES

17Cyber
Assistance et urgence cyber · 17cyber.gouv.fr

Cybermalveillance
Diagnostic et conseils · cybermalveillance.gouv.fr

0 805 805 817
Info Escroqueries, appel gratuit

33700
Signaler un SMS ou un appel frauduleux

Perceval
Fraude à la carte bancaire · service-public.fr

Pharos
Contenus illicites · internet-signalement.gouv.fr

Besoin d'une enquête ou d'une expertise numérique ? **06 40 95 40 59**

Mon contrôle en 10 points



À cocher, à afficher près de l'écran ou sur le frigo.

- [ ] Mes mots de passe sont **différents** pour chaque compte.
- [ ] J'utilise un **gestionnaire** de mots de passe.
- [ ] La **double authentification** est activée sur mes comptes clés.
- [ ] Mes appareils se **mettent à jour** automatiquement.
- [ ] Je **sauvegarde** régulièrement mes fichiers importants.
- [ ] Je **verrouille** mon écran dès que je m'éloigne.
- [ ] Je ne communique **jamais un code** reçu par SMS.
- [ ] Je **vérifie par un autre canal** toute demande urgente.
- [ ] Je ne confie **aucune donnée sensible** à une IA non validée.
- [ ] Je sais **qui prévenir** en cas de doute ou d'incident.

MON CONTACT EN CAS DE DOUTE

Nom / service : _____

Téléphone : _____

CMP INVESTIGATION

La vérité par la preuve et l'enquête

ENQUÊTER · ANALYSER · CONFIRMER · SÉCURISER · INFORMER

Enquêtes

Investigations privées pour particuliers, entreprises et professionnels du droit.

Cybercriminalité

Analyse d'escroqueries, preuves numériques, accompagnement des victimes.

Formations

Sensibilisation et formation cybersécurité pour particuliers, TPE et PME.

NOUS CONTACTER

06 40 95 40 59

contact@cmp-investigation.com

www.cmp-investigation.com

Facebook · LinkedIn · Instagram · YouTube · TikTok

CMP Investigation · Détective privé · Agrément CNAPS N° AUT-095-2122-06-17-20230376901

Guide des bons réflexes numériques · Édition 2026