

CONFÉRENCE CYBERSÉCURITÉ

Comment se protéger
des arnaques en ligne, du piratage
et des escroqueries numériques ?



JEUDI 9 JUILLET 2026



19H00



Salle Multimodale de la Mairie
Saint-Martin-d'Auxigny

ENTRÉE GRATUITE

SOMMAIRE

Protégeons nos données, sécurisons nos usages

01 INTRODUCTION



08 LES RÉSEAUX SOCIAUX



02 LES ARNAQUES COURANTES



09 LES ACHATS EN LIGNE



03 LES SMS FRAUDULEUX (SMISHING)



10 QUE FAIRE SI VOUS ÊTES VICTIME ?



04 LE PHISHING (HAMEÇONNAGE)



11 CAS PRATIQUE N°1
Faux SMS CPF



05 LES MOTS DE PASSE



12 CAS PRATIQUE N°2
Faux message Messenger



06 LA DOUBLE AUTHENTIFICATION



13 RESSOURCES UTILES



07 LES SAUVEGARDES



14 QUESTIONS / ÉCHANGES



La meilleure protection reste **votre vigilance.**

Restons prudents, restons informés, restons protégés.

QUI SUIS-JE ?

Maxime Guillotin

MG Informatique 18

Dépannage & Assistance Informatique

- Gérant de MG Informatique 18
- Technicien Systèmes et Réseaux
- Assistance informatique auprès des particuliers
- Sensibilisation à la cybersécurité

Objectif de la conférence

Vous donner des **réflexes simples** pour éviter les arnaques numériques et **protéger vos données**.

POURQUOI CETTE CONFÉRENCE ?

Les arnaques numériques sont de plus en plus fréquentes et touchent toutes les générations.

Aujourd'hui, les fraudeurs utilisent :



| Les SMS frauduleux



| Les e-mails frauduleux



| Les appels téléphoniques



| Les sites internet frauduleux



| L'usurpation d'identité

Tout le monde peut être concerné

Quelques **réflexes simples** permettent d'éviter la majorité des arnaques.

LES ARNAQUES LES PLUS FRÉQUENTES



Faux SMS de livraison
“Votre colis ne peut être livré”



Faux conseiller bancaire
“Votre compte est bloqué”



Faux CPF
“Vous avez des droits à utiliser”



Faux support informatique
“Votre ordinateur est infecté”



Faux concours Facebook
“Gagnez un smartphone”



Les fraudeurs utilisent souvent **l'urgence**
pour pousser à agir rapidement.

COMMENT RECONNAÎTRE UNE ARNAQUE ?

Les fraudeurs utilisent souvent **les mêmes techniques** :



Créer un sentiment d'urgence



Faire peur à la victime



Inciter à cliquer sur un lien



Demander des informations personnelles



Récupérer des identifiants
ou coordonnées bancaires



Leur objectif : vous tromper et obtenir vos données
ou votre argent.

COMMENT RECONNAÎTRE UNE ARNAQUE ?

Les questions à se poser :

- ✓ | Est-ce que j'attendais vraiment ce message ?
- ✓ | L'expéditeur est-il légitime ?
- ✓ | Le lien semble-t-il normal ?
- ✓ | Pourquoi me demande-t-on d'agir immédiatement ?
- ✓ | Vais-je donner des informations personnelles ?



En cas de doute, **ne cliquez pas** et demandez conseil.

EXEMPLE D'UN SMS FRAUDULEUX

- ① Qui parmi vous a déjà reçu un SMS comme celui-ci ?
- ② Qu'est-ce qui vous paraît suspect dans ce message ?



EXEMPLE D'UN SMS FRAUDULEUX



QUE REMARQUEZ-VOUS ?

- ! Un message alarmant
- ! Une demande d'action immédiate
- ! Un lien internet suspect
- ! Une menace ou une conséquence annoncée
- ! Une adresse inhabituelle



EXEMPLE DE TEXTE :

*"Votre colis est bloqué. Merci de régler les frais de livraison via le lien suivant : **colis-livraison-suivi-24.com**"*



LES ORGANISMES OFFICIELS NE DEMANDENT
JAMAIS VOS INFORMATIONS BANCAIRES PAR SMS.

LES FAUX E-MAILS (PHISHING)



Les cybercriminels envoient des e-mails qui semblent provenir :



De votre banque



De La Poste



D'Amazon



Des impôts



De la CAF



De votre assurance



COMMENT LES RECONNAÎTRE ?



Adresse de l'expéditeur inhabituelle



Fautes d'orthographe ou de grammaire



Message alarmant ou urgent



Pièce jointe suspecte



Lien internet étrange



Vérifiez toujours **l'adresse de l'expéditeur** avant de cliquer sur un lien ou d'ouvrir une pièce jointe.

LES FAUX E-MAILS (PHISHING)

Qu'est-ce qui vous paraît suspect dans cet e-mail?

De : Crédit Agricole <service-client@credit-agricole-securite.com>
À : moi
Objet : **URGENT** - Votre compte sera suspendu
Date : Mer. 4 juin 2025 à 09:17



Cher client,

Nous avons détecté une activité suspecte sur votre compte en ligne.

Pour des raisons de sécurité, votre accès peut être suspendu si vous ne confirmez pas vos informations.

Merci de confirmer vos informations sous 24h pour éviter la suspension de votre compte.

Sécuriser mon compte

Ce lien est valide pendant 24h.

Cordialement,
Le service sécurité du Crédit Agricole

© Crédit Agricole 2025 – Tous droits réservés
Ne répondez pas à cet e-mail. Contactez-nous via notre site officiel.

LES FAUX E-MAILS (PHISHING)

De : Crédit Agricole <service-client@credit-agricole-securite.com>
À : moi
Objet : **URGENT** - Votre compte sera suspendu
Date : Mer. 4 juin 2025 à 09:17



Cher client,

Nous avons détecté une activité suspecte sur votre compte en ligne.

Pour des raisons de sécurité, votre accès peut être suspendu si vous ne confirmez pas vos informations.

Merci de confirmer vos informations sous 24h pour éviter la suspension de votre compte.

Sécuriser mon compte

Ce lien est valide pendant 24h.

Cordialement,
Le service sécurité du Crédit Agricole

© Crédit Agricole 2025 – Tous droits réservés
Ne répondez pas à cet e-mail. Contactez-nous via notre site officiel.

QUE REMARQUEZ-VOUS ?



Adresse d'expéditeur inhabituel
(non officielle)



Demande urgente
(sous 24h)



Création d'un sentiment
de peur



Lien potentiellement
frauduleux



Demande d'informations
personnelles



Votre banque ne vous demandera jamais vos identifiants, mots de passe ou codes de validation par e-mail.

LES MOTS DE PASSE

Pourquoi sont-ils importants ?



Ils protègent vos comptes



Messagerie



Banque



Réseaux sociaux



Sites marchands

Les erreurs les plus fréquentes

✗ 123456

✗ azerty

✗ password

✗ prénom + date de naissance

✗ même mot de passe partout

Exemple :

Mot de passe faible :

✗ Maxime1998

Mot de passe plus robuste :

✓ JaimeLesPommes!2026

CRÉER UN BON MOT DE PASSE

Les règles à respecter

- ✓ Au moins 12 caractères
 - ✓ Mélanger lettres, chiffres et caractères spéciaux
 - ✓ Éviter les informations personnelles
 - ✓ Utiliser un mot de passe différent pour chaque compte
-

La méthode la plus simple

Utiliser une phrase de passe

Exemples :

- ✓ MonChienMange3CroquettesParJour!
- ✓ J'AimeLeCafeDepuis2005!
- ✓ JeParsEnVacancesChaqueEte!

LA DOUBLE AUTHENTIFICATION

Qu'est-ce que c'est ?



Une sécurité supplémentaire qui protège vos comptes.



Même si quelqu'un connaît votre mot de passe, il ne pourra pas se connecter sans un second code.

Comment ça fonctionne ?

1



Vous saisissez votre mot de passe

2



Vous recevez un code de vérification

3



Vous confirmez votre identité



Connexion autorisée

Exemples de services compatibles



Gmail



Facebook



Instagram



Amazon



Applications bancaires



Activez la **double authentification** sur
vos comptes importants :
messagerie, banque et réseaux sociaux.

SAUVEGARDER SES DONNÉES

Pourquoi sauvegarder ?



Pour conserver ses photos de famille



Pour protéger ses documents importants



En cas de panne ou de perte du téléphone



En cas de virus ou de piratage



En cas de casse ou de vol de l'appareil

Ce qu'il faut sauvegarder



Photos et vidéos



Documents administratifs



Factures importantes



Contacts



Documents professionnels



Une sauvegarde n'est utile que si elle existe **avant le problème.**

LES SOLUTIONS DE SAUVEGARDE

Sauvegarde dans le Cloud



- Google Photos



- iCloud



- OneDrive

Avantages

- ✓ Automatique
- ✓ Accessible partout
- ✓ Protection en cas de perte du téléphone

Sauvegarde sur support physique



- Disque dur externe



- Clé USB



- Ordinateur

Avantages

- ✓ Pas besoin d'Internet
- ✓ Contrôle total des données
- ✓ Grande capacité de stockage



Une sauvegarde n'est utile que si elle existe **avant le problème.**

RÉSEAUX SOCIAUX ET USURPATION D'IDENTITÉ

Les risques les plus fréquents



Faux profils Facebook



Vol de photos



Piratage de compte Messenger



Demandes d'argent frauduleuses



Arnaques Marketplace

Ce qui peut arriver



Messages envoyés à vos proches



Demandes d'argent



Tentatives d'escroquerie



Atteinte à votre réputation



Ne prêtez **jamais d'argent** à un proche sans vérifier son identité par téléphone.

Comment se protéger ?



Vérifier les **paramètres de confidentialité**



Limiter les **informations publiques**



Utiliser un **mot de passe fort**



Activer la **double authentification**



Se méfier des **demandes inhabituelles**



Avant d'envoyer de l'argent à un proche,
vérifiez toujours son identité par téléphone.

ACHATS EN LIGNE EN TOUTE SÉCURITÉ

Avant d'acheter :



Vérifier l'adresse du site



Rechercher le cadenas de sécurité



Consulter les avis



Vérifier les coordonnées de l'entreprise

Les signes d'un site frauduleux :



Prix anormalement bas



Nombreuses fautes d'orthographe



Aucune mention légale



Paiement uniquement par virement



Adresse de contact inexistante

LES BONNES PRATIQUES



Utiliser une **carte bancaire**



Vérifier l'**adresse du site**



Ne jamais communiquer un **code** reçu par **SMS**



Se méfier des **offres trop belles** pour être vraies



Si une offre paraît trop belle pour être vraie,
elle est **probablement frauduleuse.**

QUE FAIRE SI JE SUIS VICTIME D'UNE ARNAQUE ?



Ne pas paniquer

Même si vous avez cliqué sur un lien ou communiqué une information, il est important d'agir rapidement.

Les bons réflexes :



Changer immédiatement
ses **mots de passe**



Contacteur sa banque si des
informations bancaires ont été
transmises



Déconnecter les appareils
suspects



Vérifier sa messagerie
électronique

Si votre compte a été piraté :



Changer le **mot de passe**



Activer la **double authentification**



Prévenir ses **proches**



Vérifier les **connexions récentes**



**Agir vite peut limiter les dégâts
et protéger vos données et votre argent.**

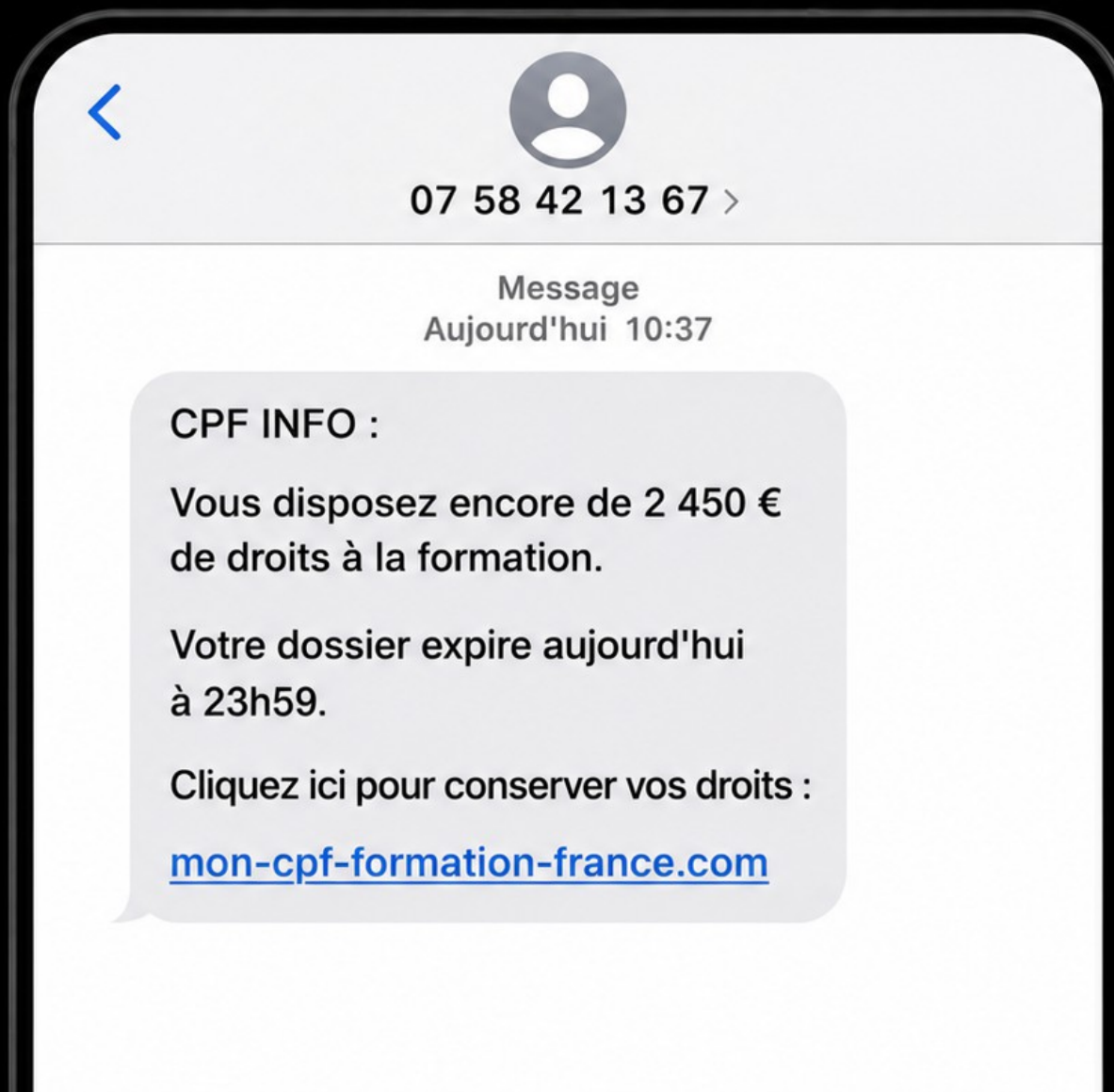
CAS PRATIQUE N°1

FAUX SMS CPF



QUESTION AU PUBLIC

Que remarquez-vous de suspect dans ce message ?



CAS PRATIQUE N°1

FAUX SMS CPF



QUESTION AU PUBLIC

Que remarquez-vous de suspect dans ce message ?



07 58 42 13 67 >

Message
Aujourd'hui 10:37

CPF INFO :

Vous disposez encore de **2 450 €** de droits à la formation.

Votre dossier expire **aujourd'hui** à **23h59**.

Cliquez ici pour conserver vos droits :
mon-cpf-formation-france.com



APRÈS DISCUSSION, LES ÉLÉMENTS SUSPECTS



Sentiment d'urgence
"expire aujourd'hui"



Lien internet suspect
(adresse non officielle)



Demande d'action immédiate
("cliquez ici", "conserver vos droits")



Adresse non officielle
(mon-cpf-formation-france.com)



Les organismes officiels
ne contactent pas ainsi par SMS



Le CPF, les impôts, la CAF ou votre banque ne vous demandent **jamais** de cliquer en urgence sur un lien reçu par SMS.

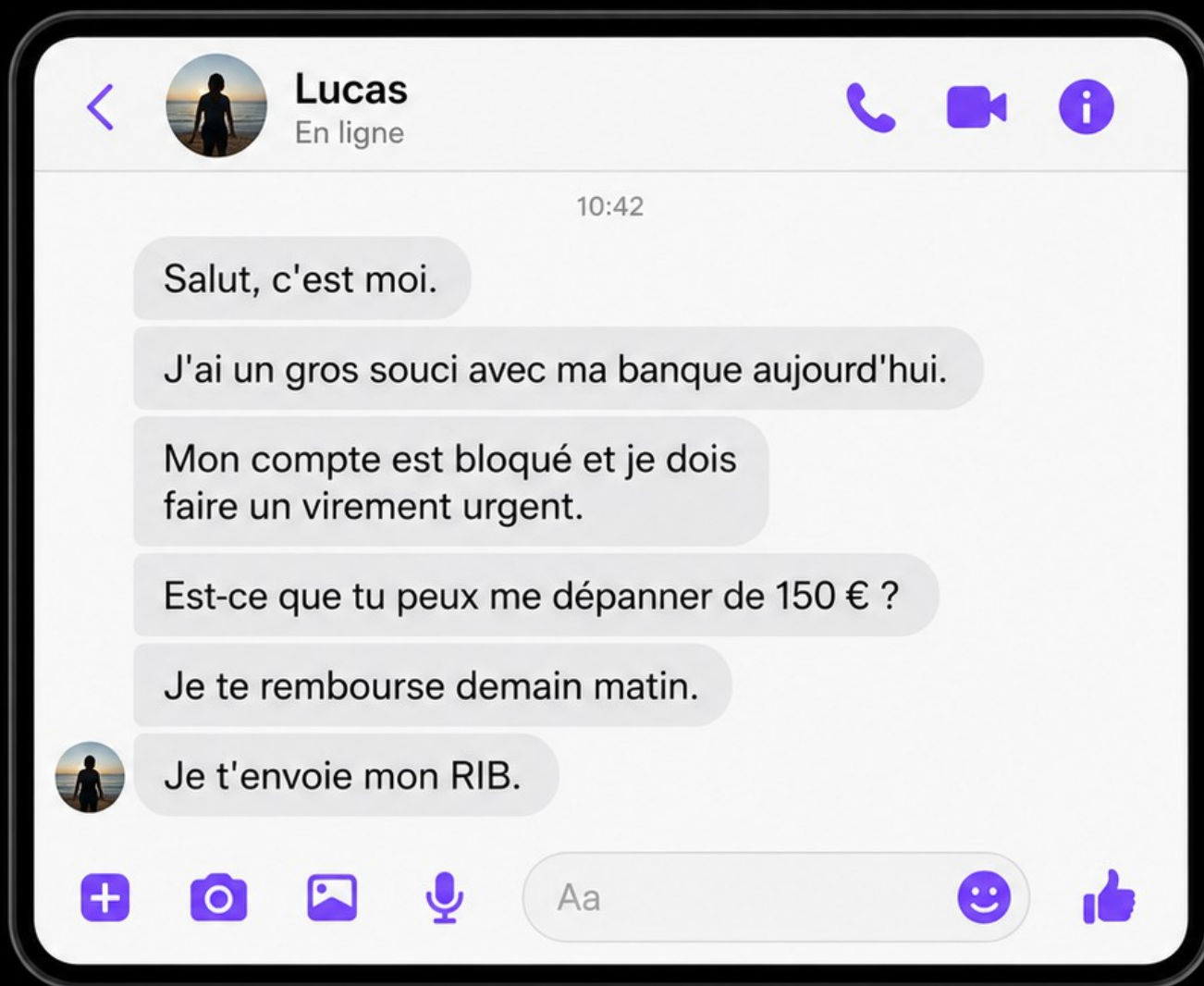
CAS PRATIQUE N°2

FAUX MESSAGE D'UN PROCHE



QUESTION AU PUBLIC

Que feriez-vous à sa place ?



RESSOURCES UTILES

Que faire et vers qui se tourner ?



SIGNALER UNE ARNAQUE



PHAROS

Plateforme officielle pour signaler tout contenu ou comportement illicite sur Internet.

www.internet-signalement.gouv.fr



CYBERMALVEILLANCE.GOUV.FR

Assistance et prévention en cas d'arnaque, de virus ou de piratage.

www.cybermalveillance.gouv.fr



SIGNAL SPAM

Signalez les emails ou SMS indésirables et frauduleux.

www.signal-spam.fr

33700

33700 (SMS FRAUDULEUX)

Numéro gratuit pour signaler les SMS et appels frauduleux.



À RETENIR

En cas de doute, ne cliquez pas, ne répondez pas, et demandez conseil.
La vigilance est votre meilleure protection !



EN CAS DE PROBLÈME BANCAIRE



Contactez immédiatement votre banque

via le numéro officiel (au dos de votre carte bancaire ou sur le site de votre banque).



Faites opposition si nécessaire

sur votre carte bancaire ou vos moyens de paiement.



Conservez toutes les preuves

(SMS, emails, captures d'écran, relevés...).



BESOIN D'AIDE ?



FRANCE SERVICES

Un accompagnement gratuit et personnalisé près de chez vous.



MAIRIE

Vos services municipaux peuvent vous orienter et vous accompagner.



MG INFORMATIQUE 18

Dépannage, assistance et conseils informatiques.
Nous sommes à votre écoute !



PLUS VOUS RÉAGISSEZ VITE, PLUS VOUS LIMITEZ LES DÉGÂTS.

MERCI DE VOTRE ATTENTION

Avez-vous des questions ?



QUELQUES RÉFLEXES À RETENIR :

- ✓ Ne jamais agir dans l'urgence
- ✓ Vérifier avant de cliquer
- ✓ Utiliser des mots de passe forts
- ✓ Activer la double authentification
- ✓ Faire des sauvegardes régulières



MG INFORMATIQUE 18

Dépannage & Assistance Informatique



Saint-Martin-d'Auxigny



Assistance
particuliers et professionnels



**LA MEILLEURE PROTECTION RESTE
VOTRE VIGILANCE.**

