MINISTÈRE
DE L'INTÉRIEUR
Liberté
Égalité
Fraternité

ALERTECYBERGEND80
Gendarmerie départementale de la Somme

6 octobre 2025

Dans le cadre du **CyberMois**, la **Gendarmerie de la Somme** se mobilise pour votre **sécurité numérique**. En suivant ces quelques conseils, vous serez mieux armé pour **détecter et éviter les tentatives de fraude** (hameçonnage et logiciels malveillants) qui passent couramment par des **liens frauduleux** et des **pièces jointes piégées**.

🔗 *LIENS INCONNUS : RÉFLEXES CLÉS* 🔗

Avant de cliquer sur un lien dans un e-mail, un SMS, ou sur un réseau social, ayez ces réflexes :

1. Vérifiez l'Expéditeur et le Contexte :

- ► **L'adresse de l'expéditeur est-elle légitime ?** Les fraudeurs utilisent des adresses très similaires à l'originale (comme par exemple : `@micros0ft.com` au lieu de `@microsoft.com`).
- ► **Est-ce que j'attendais ce message ?** Un e-mail non sollicité demandant une action urgente (mot de passe, données bancaires) est le principal signal d'alarme.

2. Inspectez l'URL sans Cliquer :

- ► **Passez votre souris** sur le lien sans cliquer (sur ordinateur) ou **appuyez longuement** (sur mobile) pour voir l'adresse de destination réelle s'afficher.
- ► **L'URL correspond-elle au site promis ?** Si l'URL affichée ne mène pas au domaine officiel (ex. un lien vers votre banque qui affiche une adresse IP ou un nom étranger), ne cliquez surtout pas.

3. Accédez au Site Directement : Si une alerte provient d'un service (banque, administration), **ne suivez pas le lien de l'e-mail**. Ouvrez plutôt votre navigateur, tapez l'adresse officielle vous-même, et connectez-vous comme d'habitude pour vérifier.

📎 *PIÈCES JOINTES : LA RÈGLE D'OR* 📎

L'ouverture d'une pièce jointe suspecte est le moyen le plus courant de s'infecter par un virus ou un rançongiciel (ransomware).

1. Méfiance Absolue : N'ouvrez jamais une pièce jointe si l'expéditeur est inconnu ou si le message est **inattendu**, même s'il semble provenir d'un collègue ou d'un contact (leur compte pourrait avoir été piraté).

2. Attention aux Formats Piégés : Soyez très vigilant avec les formats exécutables ou compressés, comme les fichiers **.exe, .zip**, ou les documents Office demandant d'activer des **macros**. Vérifiez toujours la double extension (par exemple : `facture.pdf.exe`).

3. Vérifiez le Contact : Si vous recevez un document important non sollicité (facture, bon de commande), **contactez l'expéditeur par un autre moyen que l'e-mail** (par exemple, en utilisant un **numéro de téléphone officiel** trouvé ailleurs que dans le mail suspect) pour confirmer l'authenticité de l'envoi avant de l'ouvrir.

Au moindre doute** sur un **lien** ou une **pièce jointe**, la meilleure pratique est de **supprimer l'e-mail** sans l'ouvrir : **VOTRE SÉCURITÉ VAUT PLUS QUE LA CURIOSITÉ.