



HELIOS

Service des Opérations · Bureau SSI

Guide des bons réflexes cyber du Combattant numérique

Comprendre · Repérer · Réagir face aux
risques cyber.



**Je suis HELIOS,
Soldat d'Elite du Digital**

Version à l'usage du personnel · Ne pas diffuser hors unité

Un mot de votre Bureau SSI

Un message crédible, un appel pressant ou une information partagée trop vite peuvent suffire à exposer HELIOS. La sécurité de nos systèmes ne repose pas seulement sur les outils et sur les spécialistes : elle dépend du geste de chacun, au bon moment.

Le Bureau SSI du Service des Opérations n'attend de vous ni expertise technique, ni méfiance permanente. Il attend un réflexe : faire une pause de quelques secondes avant de cliquer, de répondre ou de transmettre ; vérifier ; puis signaler en cas de doute.

Un doute signalé est un service rendu à toute l'unité, jamais un aveu de faute.



Chaque soldat du digital a un rôle utile, légitime et positif à jouer dans la sécurité collective.



Le Bureau SSI

Service des Opérations (SOPS) · HELIOS



Ce guide a été conçu pour vous

Il s'adresse à toutes celles et ceux qui utilisent chaque jour un ordinateur, un smartphone, une messagerie ou des services en ligne dans leur travail.

Chaque page va à l'essentiel pour vous aider à reconnaître une situation à risque, à prendre du recul et à adopter le bon réflexe au bon moment.

Lisez-le d'un bout à l'autre ou allez directement au thème qui vous concerne. Les repères en haut des pages vous guident :



Comprendre

Les mécanismes des attaques, le rôle de l'ingénierie sociale et l'importance des réflexes du quotidien.



Repérer

Les signaux d'alerte, les formes d'attaques courantes et les situations qui doivent attirer l'attention.



Réagir

Les bons réflexes à adopter pour protéger vos accès, vos données, vos outils, et signaler un doute.

Quand l'attaque vise d'abord votre réaction

Beaucoup d'attaques ne reposent pas sur une faille technique mais sur la manipulation. Elles jouent sur l'urgence, la confiance, la curiosité ou la peur, et peuvent s'appuyer sur des informations glanées sur les réseaux sociaux. Leur but : vous pousser à agir trop vite.



L'urgence

Un délai court ou une action immédiate est imposé : « votre accès sera coupé dans l'heure ».



L'autorité

La demande semble venir d'un chef ou d'un service interne.



La confiance

Le message reprend un logo, un prénom connu ou un contexte réel.



La curiosité

Une pièce jointe inattendue, ou un document présenté comme important.



La peur

Menace de sanction, de blocage, de retard ou de perte d'accès.



Le service rendu

Une personne semble demander de l'aide ou compter sur votre réactivité.



Le réflexe

Lorsqu'une demande vous pousse à agir vite, c'est justement le moment de ralentir.



Les signaux qui doivent vous alerter

Avant de cliquer, de répondre ou de transmettre une information, certains indices doivent vous inviter à faire une pause.



Un expéditeur inhabituel

L'adresse semble proche d'une adresse connue, mais comporte une différence ou un nom de domaine étranger.



Une demande urgente

Le message insiste pour que vous agissiez vite, sans prendre le temps de vérifier.



Un lien ou une pièce jointe inattendue

Vous ne vous attendiez pas à recevoir ce document ou ce lien, ou le contexte n'est pas clair.



Une demande discrète

On vous demande de ne pas en parler, de contourner une procédure ou d'utiliser un canal inhabituel.



Une demande sensible

Code, mot de passe, coordonnées bancaires, document interne, données personnelles.



Un ton inhabituel

Le message paraît étrange, trop pressant, trop vague ou différent des habitudes de l'expéditeur.



Avant d'agir, posez-vous 3 questions :



Est-ce attendu ?



Est-ce cohérent ?



Puis-je vérifier autrement ?



Reconnaître les formes d'attaques les plus courantes

Les cybercriminels changent de canal pour rendre leurs demandes crédibles. Leur objectif reste le même : vous amener à cliquer, répondre ou partager sans avoir vérifié le contexte.



E-mail frauduleux (Phishing)

Un message imite un service ou un collègue pour vous faire cliquer.



E-mail ciblé (Spear phishing)

Un message personnalisé utilise des éléments crédibles vous concernant.



Appel frauduleux (Vishing)

Un appel vous met sous pression pour vous faire agir : faux conseiller, faux chef.



Appel vidéo frauduleux

Une visio sert à usurper une identité ou à obtenir un partage d'écran.



QR code piégé (Quishing)

Un QR code peut rediriger vers un faux site.



SMS frauduleux (Smishing)

Un SMS vous pousse à ouvrir un lien piégé : faux gain, faux compte Mobile Money bloqué.



Support inconnu

Une clé USB ou un disque trouvé ou reçu peut contenir un logiciel malveillant.



Les techniques évoluent (faux liens WhatsApp, PDF générés par l'IA...), mais l'objectif reste le même : vous pousser à agir sans vérifier.



Appliquer les bons réflexes

7 réflexes simples pour vous protéger au quotidien.

**Une seconde
de recul**

**Avant
de cliquer,
interrogez
le contexte.**



Posez-vous 3 questions :

- ☑ **Est-ce que j'attendais ce message ?**
- ☑ **La demande est-elle cohérente ?**
- ☑ **L'urgence est-elle justifiée ?**



Vérifiez l'expéditeur

Contrôlez l'adresse e-mail, le numéro ou l'identité de la personne.



Inspectez les liens

Vérifiez la véritable adresse du lien avant de l'ouvrir, surtout si le message est inattendu.



Soyez prudent avec les pièces jointes

N'ouvrez une pièce jointe que si vous l'attendiez, si l'expéditeur est vérifié et si le contexte est cohérent.



Ne communiquez pas d'informations sensibles

Un mot de passe ou un code ne doit jamais être communiqué par e-mail, SMS ou téléphone.



Restez vigilant au téléphone

Sous pression, ne transmettez rien de sensible. Raccrochez et rappelez via un numéro validé.



Utilisez les outils de sécurité

Canal de signalement, alertes internes, Bureau SSI : ils sont là pour vous aider.



En cas de doute, signalez

Contactez le Bureau SSI ou utilisez le canal de signalement prévu.

Chaque bon réflexe compte.

Ensemble, nous renforçons notre sécurité.



Vos accès sont des clés



Un compte professionnel donne souvent accès à bien plus qu'une messagerie : documents internes, outils métiers, espaces collaboratifs, informations sensibles. C'est pourquoi les identifiants sont très recherchés : l'attaquant s'en sert pour se déplacer dans les systèmes.



Un mot de passe unique

Réutiliser le même mot de passe augmente le risque : si un service est compromis, les autres peuvent l'être aussi.



Un mot de passe robuste

Une phrase de passe longue, difficile à deviner, est bien plus efficace qu'un mot court et réutilisé.



Un stockage sécurisé

Jamais de mots de passe sur papier ou dans un fichier non protégé. Utilisez le gestionnaire validé par HELIOS.



L'authentification multifacteur

Activez-la lorsqu'elle est disponible : elle protège même si votre mot de passe est compromis.



Un code jamais transmis

Un mot de passe ou un code ne doit jamais être communiqué, même à une personne qui semble légitime ou pressée.



Le verrouillage des appareils

Même pour une courte absence, verrouillez votre écran : il protège vos messages, vos fichiers et vos outils.



Vos accès sont personnels. Les protéger, c'est protéger votre identité numérique, vos camarades et les informations de HELIOS.

Sécurité numérique, sécurité physique : mêmes réflexes

Une donnée sensible peut aussi être exposée sur un écran visible, dans un document imprimé, lors d'un appel passé en public ou sur un poste laissé sans surveillance.



Un écran visible

Dans un espace partagé, quelqu'un peut lire une information confidentielle sans que vous ne le remarquiez.



Un document imprimé

Une note, un ordre, une liste de contacts peuvent contenir des informations sensibles.



Une conversation entendue

Un appel peut révéler un nom, un projet, une date ou une difficulté interne.



Un matériel sans surveillance

Ordinateur, smartphone, badge, clé USB ou carnet donnent accès à des informations ou à des locaux.



Une connexion non maîtrisée

Un Wi-Fi public ou inconnu peut être frauduleux et exposer vos identifiants.

Hors du bureau : trois moments clés



Avant de partir

Emportez le strict nécessaire ; vérifiez vos accès.



Pendant le déplacement

Verrouillez dès que vous vous éloignez ; gardez vos affaires.



Au retour

Rangez sous clé documents et supports sensibles ; détruisez au broyeur brouillons et impressions inutiles ; signalez toute perte.

IA générative : utile, mais pas sans cadre

Les outils d'IA peuvent faire gagner du temps : reformuler un texte, résumer un contenu, structurer des idées. Mais ils demandent deux précautions : faire attention aux informations qu'on leur transmet, et garder du recul sur leurs réponses. Une IA peut aider, elle ne décide pas à votre place.



Deux réflexes dans l'usage de l'IA

- ✓ Ai-je le droit de partager cette information ?
- ✓ Ai-je vérifié la réponse produite ?



Avant de partager une information

Données personnelles, informations RH, noms et fonctions, ordres, plans, codes source, captures d'écran internes, identifiants : si l'outil n'est pas validé par HELIOS, ces informations ne doivent pas y être déposées.



Avant de réutiliser une réponse

Une réponse peut sembler claire et convaincante tout en étant incomplète, imprécise ou inadaptée au contexte réel. Vérifiez les faits importants, relisez, et assurez-vous qu'elle respecte les règles internes.



À retenir

L'IA peut vous aider à gagner du temps, mais elle ne remplace pas votre jugement.



En cas de doute, signalez

Signaler n'est pas reconnaître une faute : c'est participer activement à la protection collective. Un signalement rapide permet de bloquer un lien, de sécuriser un compte et d'alerter d'autres camarades. Même une fausse alerte reste utile.



1. Je m'arrête

Je ne clique pas, je ne réponds pas, je ne transmets rien.



2. Je vérifie

Par un autre canal : contact connu, numéro officiel, messagerie interne.



3. Je signale

Au Bureau SSI, tout de suite, avec le message, l'adresse, le lien ou la capture d'écran.

À détacher et garder près de soi

Fiche réflexe

Une seconde de recul. Avant de cliquer, interrogez le contexte.



Est-ce attendu ?



Est-ce cohérent ?



L'urgence est-elle justifiée ?



Puis-je vérifier autrement ?

1. Je m'arrête

2. Je vérifie

3. Je signale

Chaque bon réflexe compte.

Ensemble, nous renforçons la sécurité de HELIOS.



Ressources utiles et diffusion du guide

Pour aller plus loin, s'informer ou savoir vers qui se tourner en cas de doute, plusieurs ressources peuvent vous accompagner.

Se former gratuitement

- SecNumacadémie de l'ANSSI : un parcours de formation en ligne ouvert à tous.
- ANTIC, Agence Nationale des TIC du Cameroun : alertes et conseils nationaux.
- Atelier RGPD de la CNIL : protéger les données personnelles.



Signaler un incident

Contactez le Bureau SSI via le canal de signalement HELIOS. Joignez le message, le lien ou la capture d'écran, et ne tentez pas de corriger seul.

Un signalement rapide protège toute l'unité, même en cas de fausse alerte.

Diffuser ce guide dans votre organisation ?

Téléchargez la version numérique du guide ou recevez des exemplaires imprimés pour vos actions de sensibilisation, vos parcours d'intégration, vos campagnes de prévention ou une diffusion directe auprès de vos camarades.



**Version imprimée
ou numérique : à vous de choisir !**

Pour obtenir ou imprimer le guide

Scannez le QR code ci-contre ou rendez-vous sur le site officiel HELIOS :

<https://heliosc4i.cm/>



heliosc4i.cm



**Ensemble, contribuons chaque jour
à protéger HELIOS.**



**Je suis HELIOS,
Soldat d'Elite du Digital**

Source et mentions

Contenus adaptés du « Guide des bons réflexes cyber du collaborateur », réalisé par Hucency (human centered cybersecurity). © Hucency, tous droits réservés.

Adaptation et mise en forme : HELIOS, Service des Opérations, Bureau SSI. Illustrations originales HELIOS.

Reproduction, diffusion ou modification interdites sans autorisation préalable des titulaires des droits. Usage interne HELIOS.