

Le numérique, en clair.

18 cartes pour comprendre.
18 réflexes pour agir.

CHOISISSEZ VOTRE THÈME

01 LES BASES

02 VOS COMPTES

03 LES ARNAQUES

04 VOS DONNÉES

05 L'IA AU QUOTIDIEN

06 LES BONS RÉFLEXES

À LA MAISON • AU TRAVAIL • SANS JARGON

Protéger votre vie numérique.

EN UNE PHRASE

La cybersécurité sert à protéger vos appareils, vos comptes et vos informations contre le vol, les arnaques et les blocages.

PAR EXEMPLE

Un faux message peut voler votre mot de passe et donner accès à vos e-mails.



LE RÉFLEXE SUIV-IT

Protégez d'abord votre boîte mail : un mot de passe différent des autres comptes et une confirmation sur votre téléphone.

Une mise à jour, c'est aussi une réparation.

EN UNE PHRASE

Une mise à jour remplace une ancienne version d'un logiciel pour corriger des problèmes, notamment des faiblesses de sécurité.

PAR EXEMPLE

Votre téléphone demande un redémarrage : cela peut terminer l'installation de nouvelles protections.



LE RÉFLEXE SUIV-IT

Dans les réglages de vos appareils, activez les mises à jour automatiques et redémarrez quand c'est demandé.

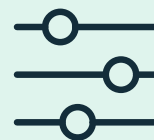
Votre micro. Vos photos. Votre permission.

EN UNE PHRASE

Une autorisation, c'est votre accord pour laisser une application utiliser le micro, la caméra, vos photos ou vos contacts.

PAR EXEMPLE

Une application de photo a besoin de la caméra ; une calculatrice n'a normalement pas besoin de vos contacts.



LE RÉFLEXE SUIV-IT

N'accordez que les accès utiles à l'application. Pour le micro ou la caméra, choisissez « pendant l'utilisation » si possible.

Un mot de passe par compte. Un seul coffre-fort.

EN UNE PHRASE

Un mot de passe protège l'accès à un compte ; un gestionnaire est un coffre-fort numérique qui crée et garde vos mots de passe pour vous.

PAR EXEMPLE

Si vous utilisez le même mot de passe partout, un seul vol peut donner accès à plusieurs comptes.



LE RÉFLEXE SUIV-IT

Laissez le gestionnaire créer un mot de passe différent pour chaque compte. Protégez ce coffre-fort avec un long mot de passe.

Un mot de passe volé ne doit pas ouvrir la porte.

EN UNE PHRASE

Le MFA combine deux preuves ou plus pour vous reconnaître : par exemple, votre mot de passe et une confirmation sur votre téléphone.

PAR EXEMPLE

Quelqu'un connaît votre mot de passe ? Il lui manque encore cette seconde preuve pour se connecter.



LE RÉFLEXE SUIV-IT

Activez la double vérification dans les réglages de sécurité de votre boîte mail. Ne confirmez que vos propres connexions.

Votre appareil peut devenir votre clé.

EN UNE PHRASE

Une clé d'accès, ou passkey, remplace le mot de passe par une clé numérique que vous utilisez en déverrouillant votre appareil.

PAR EXEMPLE

Sur un site compatible, vous confirmez avec votre empreinte ou le code de votre appareil, sans taper de mot de passe.



LE RÉFLEXE SUIV-IT

Activez-la sur un compte compatible et vérifiez comment retrouver l'accès si vous perdez votre appareil.

Un logo connu. Une demande à vérifier.

EN UNE PHRASE

Le phishing est une arnaque qui imite une personne ou un organisme connu pour vous faire donner vos informations ou votre argent.

PAR EXEMPLE

« Votre colis est bloqué. Payez 1,99 €. » Le logo peut être copié et le texte parfaitement écrit.



LE RÉFLEXE SUIV-IT

N'utilisez pas le lien reçu. Ouvrez vous-même l'application ou le site habituel pour vérifier la demande.

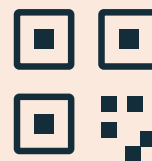
Scanner, ce n'est pas faire confiance.

EN UNE PHRASE

Un QR code est un carré à scanner qui peut ouvrir un site : comme un lien reçu par message, il peut être piégé.

PAR EXEMPLE

Sur un parking, un autocollant peut recouvrir le vrai code et vous envoyer vers un faux paiement.



LE RÉFLEXE SUIV-IT

Avant de payer, vérifiez le site affiché. En cas de doute, ouvrez l'application officielle du service.

Une alerte qui fait peur ? Gardez la main.

EN UNE PHRASE

Un faux dépanneur vous fait croire que votre ordinateur a un problème pour vous soutirer de l'argent ou le contrôler à distance.

PAR EXEMPLE

Une fenêtre annonce « PC infecté ! » et affiche un numéro à appeler immédiatement.



LE RÉFLEXE SUIV-IT

N'appellez pas ce numéro et ne donnez pas accès à votre ordinateur. Contactez votre informaticien habituel.

Vos fichiers en ligne, ça veut dire quoi ?

EN UNE PHRASE

Le cloud est un espace de rangement sur Internet ; la synchronisation recopie automatiquement vos changements entre cet espace et vos appareils.

PAR EXEMPLE

Une photo supprimée sur votre téléphone peut aussi disparaître de votre espace en ligne et de vos autres appareils.



LE RÉFLEXE SUIV-IT

Avant de supprimer, vérifiez où le fichier disparaîtra. Gardez une copie séparée de vos fichiers importants.

Votre ordinateur lâche. Vos photos restent-elles ?

EN UNE PHRASE

Une sauvegarde est une copie de secours de vos fichiers, conservée à part pour les retrouver si les originaux sont perdus ou abîmés.

PAR EXEMPLE

Si votre ordinateur tombe en panne, une copie sur un disque externe peut vous rendre vos photos et documents.



LE RÉFLEXE SUIV-IT

Faites des copies régulières sur un disque externe, débranchez-le ensuite et vérifiez qu'un fichier peut être récupéré.

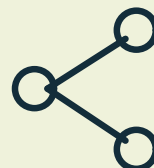
Qui peut lire ? Qui peut modifier ?

EN UNE PHRASE

Partager un document, c'est choisir qui peut le consulter et qui peut le modifier.

PAR EXEMPLE

Un lien ouvert à « toute personne disposant du lien » peut aussi être utilisé par quelqu'un à qui il a été transféré.



LE RÉFLEXE SUIV-IT

Choisissez des personnes précises et « lecture seule » si elles doivent juste consulter le document.

L'IA rédige. Vous gardez le dernier mot.

EN UNE PHRASE

Une intelligence artificielle générative est un outil qui crée du texte ou des images à partir de votre demande, mais peut inventer une réponse.

PAR EXEMPLE

Elle peut rédiger un résumé convaincant et y citer un article qui n'existe pas.



LE RÉFLEXE SUIV-IT

Avant d'utiliser une réponse importante, vérifiez les faits sur un site de référence ou auprès d'un professionnel.

Avant de coller, pensez à ce que vous confiez.

EN UNE PHRASE

Coller un texte dans une intelligence artificielle, c'est le confier à un service : ce qu'il en fait dépend de ses règles et réglages.

PAR EXEMPLE

Une fiche de paie contient un nom, une adresse et un salaire : ces informations ne sont pas anodines.



LE RÉFLEXE SUIV-IT

Évitez les informations privées ou confidentielles ; au travail, vérifiez d'abord les règles d'utilisation de l'outil.

Sa voix. Son visage. Pas forcément lui.

EN UNE PHRASE

Un deepfake est une voix, une image ou une vidéo fabriquée ou modifiée par intelligence artificielle pour faire croire qu'elle est vraie.

PAR EXEMPLE

Vous reconnaissez la voix d'un proche qui réclame de l'argent en urgence ; elle peut pourtant avoir été imitée.



LE RÉFLEXE SUIV-IT

Raccrochez et rappelez la personne sur son numéro habituel avant d'envoyer de l'argent ou des informations.

« C'est bien vous ? » Si c'est non, refusez.

EN UNE PHRASE

Une demande de validation sur votre téléphone sert à autoriser une connexion à votre compte : accepter peut laisser entrer quelqu'un.

PAR EXEMPLE

Votre téléphone vous demande de confirmer une connexion alors que vous ne faites rien.



LE RÉFLEXE SUIV-IT

Si vous n'êtes pas à l'origine de la connexion, refusez et prévenez votre conseiller informatique.

Même facture. Autre compte. Attention au piège.

EN UNE PHRASE

L'IBAN est le numéro qui identifie un compte bancaire ; un fraudeur peut remplacer celui d'une facture pour recevoir votre paiement.

PAR EXEMPLE

Votre fournisseur annonce un nouveau compte par e-mail : la demande peut venir d'un escroc.



LE RÉFLEXE SUIV-IT

Avant de payer, confirmez ce changement par un appel au numéro habituel du fournisseur, jamais seulement à celui du message.

Vous avez cliqué ? Parlez-en. Sans attendre.

EN UNE PHRASE

Un clic sur un lien suspect ne signifie pas forcément que vous êtes piraté, mais donner un mot de passe ou installer un programme augmente le risque.

PAR EXEMPLE

Mot de passe donné ? Changez-le depuis un appareil sûr. Paiement ou données bancaires ? Appelez immédiatement votre banque.



LE RÉFLEXE SUIV-IT

Fermez la page et prévenez votre conseiller informatique. Signalez le message à suspect@safeonweb.be.

POUR ALLER PLUS LOIN

Les sources. Les bons repères.

RESSOURCES CONSULTÉES LE 25 SEPTEMBRE 2026

01 Les bases de la sécurité numérique

Cybermalveillance.gouv.fr • Cartes 01-03 • [Ouvrir la source](#)

02 Protégez vos comptes

Safeonweb / CCB • Cartes 04 • [Ouvrir la source](#)

03 Authentification à deux facteurs

Safeonweb / CCB • Cartes 05, 16 • [Ouvrir la source](#)

04 Passkeys : principe et protection

FIDO Alliance • Cartes 06 • [Ouvrir la source](#)

05 Protect yourself from phishing

Microsoft Support • Cartes 07, 17 • [Ouvrir la source](#)

06 Phishing, IA et deepfakes (02/01/2026)

Safeonweb / CCB • Cartes 07, 15 • [Ouvrir la source](#)

07 Attention au quishing

Safeonweb / CCB • Cartes 08 • [Ouvrir la source](#)

08 Utiliser l'IA : conseils (maj 14/09/2026)

Cybermalveillance.gouv.fr • Cartes 03, 13-14 • [Ouvrir la source](#)

Une sélection pédagogique SUIV-IT. Les exemples sont illustratifs ; les conseils sont à adapter à votre environnement.

POUR ALLER PLUS LOIN

Les sources. Les bons repères.

RESSOURCES CONSULTÉES LE 25 SEPTEMBRE 2026

09 L'arnaque au faux support technique

Cybermalveillance.gouv.fr • Cartes 09 • [Ouvrir la source](#)

10 Utiliser des fichiers synchronisés

Microsoft Support • Cartes 10 • [Ouvrir la source](#)

11 Bien gérer ses sauvegardes (maj 14/09/2026)

Cybermalveillance.gouv.fr • Cartes 10-11 • [Ouvrir la source](#)

12 Partager des fichiers et dossiers OneDrive

Microsoft Support • Cartes 12 • [Ouvrir la source](#)

13 Notifications d'authentification inattendues

Microsoft Learn • Cartes 16 • [Ouvrir la source](#)

14 Fraude à la facture : vérifier avant de payer

Spuerkeess • Cartes 17 • [Ouvrir la source](#)

15 Lien suspect : que faire après un clic ?

Safeonweb / CCB • Cartes 18 • [Ouvrir la source](#)

16 Signaler les messages suspects

Safeonweb / CCB • Cartes 18 • [Ouvrir la source](#)

Une sélection pédagogique SUIV-IT. Les exemples sont illustratifs ; les conseils sont à adapter à votre environnement.