

■ ■ Sécurité & Vie Privée

Protégez-vous des arnaques, virus et phishing

Les bons réflexes numériques pour naviguer en sécurité

Ce guide a été préparé par l'association DoctoNET pour vous aider à utiliser internet en toute sérénité. Pas de jargon technique : seulement des conseils simples, concrets et immédiatement applicables.

1. Reconnaître les arnaques en ligne

Les escrocs sur internet sont de plus en plus habiles. Voici comment les repérer avant qu'il ne soit trop tard.

■ ■ Signes d'alerte à ne jamais ignorer

- Un email ou SMS vous demande votre mot de passe, numéro de carte bleue ou code secret.
- Un message vous annonce un gain (loterie, héritage) alors que vous n'avez rien demandé.
- On vous presse d'agir "immédiatement" ou "avant ce soir" — c'est pour vous empêcher de réfléchir.
- L'adresse email de l'expéditeur ne correspond pas au nom affiché (ex : "Banque Postale" mais @gmail.com).
- Il y a des fautes d'orthographe ou un français approximatif dans le message.

■ La règle d'or

Aucune banque, administration (Impôts, CAF, Sécurité Sociale) ou entreprise sérieuse ne vous demandera jamais votre mot de passe ou votre code PIN par email ou téléphone. En cas de doute, raccrochez et appelez le numéro officiel.

2. Le phishing : l'hameçon numérique

Le **phishing** (ou hameçonnage) consiste à vous envoyer un faux email ou SMS qui imite parfaitement un organisme officiel (La Poste, EDF, Ameli, votre banque...) pour vous voler vos identifiants ou votre argent.

1	Vérifiez l'adresse email Cliquez sur le nom de l'expéditeur pour voir la vraie adresse. "Ameli" qui écrit depuis @free.fr, c'est une arnaque.
2	Passez la souris sur le lien Avant de cliquer, posez votre souris sur le lien (sans cliquer). L'adresse réelle apparaît en bas de votre écran. Si elle semble bizarre, ne cliquez pas.
3	Allez directement sur le site Plutôt que de cliquer sur le lien reçu, tapez vous-même l'adresse du site dans votre navigateur (ex : www.ameli.fr).
4	Vérifiez le cadenas Un site sécurisé affiche un cadenas ■ à gauche de l'adresse. Sans cadenas, ne saisissez jamais vos données personnelles.

3. Se protéger des virus

Un virus informatique peut ralentir votre ordinateur, espionner ce que vous faites, chiffrer vos fichiers et vous réclamer une rançon. La bonne nouvelle : quelques précautions simples suffisent à s'en protéger.

Comment attrape-t-on un virus ? • En cliquant sur une pièce jointe suspecte • En téléchargeant un logiciel sur un site douteux • En branchant une clé USB inconnue • En cliquant sur une fausse publicité • En utilisant un Wi-Fi public non sécurisé	Comment s'en protéger ? • Installer un antivirus (Windows Defender est gratuit et efficace) • Mettre à jour Windows régulièrement • Ne jamais ouvrir une pièce jointe inattendue • Télécharger uniquement depuis des sites officiels • Éviter les Wi-Fi publics pour vos opérations bancaires
--	--

4. Les mots de passe : votre première ligne de défense

Un mot de passe robuste, c'est comme une bonne serrure sur votre porte. Voici comment en créer un facilement.

■ Les règles d'un bon mot de passe

- **Au moins 12 caractères** : plus c'est long, plus c'est solide.
- **Mélangez** : majuscules, minuscules, chiffres et symboles (ex : !, @, #).
- **Un mot de passe différent par site** : si un site est piraté, les autres restent protégés.
- **Astuce simple** : prenez une phrase facile à retenir et transformez-la. Ex : "Mon chat Félix a 3 ans !" → **McF3l1x@3!**
- **Utilisez un gestionnaire de mots de passe** comme Bitwarden (gratuit) pour retenir tous vos mots de passe à votre place.
- **Ne jamais** utiliser : votre date de naissance, "123456", "motdepasse" ou votre prénom.

5. Protéger votre vie privée en ligne

Sur internet, vos données personnelles ont de la valeur. Voici comment limiter ce que vous partagez.

Réseaux sociaux

- Réglez vos comptes en "privé". Ne partagez pas votre adresse, numéro de téléphone ou photos de documents officiels.

Cookies & traceurs

- Cliquez sur "Refuser tout" ou "Personnaliser" quand un site vous demande d'accepter les cookies — vous pouvez refuser les cookies publicitaires.

Email jetable

- Pour vous inscrire sur un site qui vous inspire peu confiance, utilisez une adresse temporaire (ex : tempmail.com) plutôt que votre vraie adresse.

Applications mobiles

- Vérifiez les autorisations demandées par les applis. Une lampe torche n'a pas besoin d'accéder à vos contacts ou votre position GPS.

Mises à jour

- Faites régulièrement les mises à jour de votre téléphone et ordinateur. Elles corrigent des failles de sécurité importantes.

■ Ma checklist sécurité — à vérifier dès aujourd'hui !

☐	J'ai un antivirus actif sur mon ordinateur (Windows Defender suffit)
☐	Mon système Windows est à jour
☐	Mes mots de passe font au moins 12 caractères
☐	Je n'utilise pas le même mot de passe partout
☐	Je vérifie l'adresse email de l'expéditeur avant d'ouvrir une pièce jointe
☐	Je ne communique jamais mon mot de passe ou code PIN par téléphone ou email
☐	Mes comptes sur les réseaux sociaux sont en mode "privé"
☐	J'ai activé la double authentification sur ma messagerie et ma banque

Besoin d'aide ? DoctoNET est là pour vous !

Nos bénévoles vous accompagnent gratuitement pour sécuriser votre ordinateur, vérifier si vous avez été victime d'une arnaque, ou installer un antivirus.

■ 01 80 06 46 49 ■ www.doctonet.org ■ Paris 17e