Ma boîte à outils anti-arnaque

Les bons outils, installés une fois, vous protègent tous les jours — sans être expert.

Cette fiche est à conserver chez vous. Voici les outils et réflexes qui vous protègent contre le phishing et les arnaques en ligne, sur téléphone comme sur ordinateur. Commencez par un gestionnaire de mots de passe et la double authentification : ce sont vos meilleures défenses anti-hameçonnage.

1. Sur votre smartphone

	Outil	À quoi ça sert	Coût	Où le trouver / l'activer
	Bitwarden	Gestionnaire de mots de passe : ne remplit vos identifiants que sur le vrai site (un faux site = pas de remplissage = signal d'alerte).	**Gratuit**	App Store / Google Play
	Google Authenticator	Double authentification : génère un code unique. Votre compte tient même si le mot de passe est hameçonné.	**Gratuit**	App Store / Google Play
	Microsoft Authenticator	Autre appli de double authentification, pratique pour les comptes Microsoft et Outlook.	**Gratuit**	App Store / Google Play
	Google Chrome / Safari	Navigateur avec protection anti-hameçonnage : alerte rouge sur les sites de phishing connus.	**Gratuit**	Déjà installé — gardez-le à jour
	Malwarebytes Mobile	Analyse les SMS et liens douteux et bloque les sites frauduleux (surtout sur Android).	**Gratuit**	malwarebytes.com/fr

2. Sur votre ordinateur (PC)

	Outil	À quoi ça sert	Coût	Où le trouver / l'activer
	Microsoft Defender	Antivirus intégré à Windows : bloque les sites piégés et les pièces jointes malveillantes.	**Gratuit**	Déjà dans Windows — vérifiez qu'il est activé
	Malwarebytes	Détecte et supprime les logiciels malveillants ; complète bien l'antivirus.	**Gratuit**	malwarebytes.com/fr
	Bitwarden / KeePass	Gestionnaire de mots de passe : n'auto-remplit que sur le vrai site → repère les faux sites.	**Gratuit**	bitwarden.com/fr
	Mozilla Firefox	Navigateur à jour avec filtre anti-hameçonnage intégré (comme Chrome et Edge SmartScreen).	**Gratuit**	mozilla.org/firefox
	VirusTotal	Site où coller un lien ou déposer un fichier douteux : analysé par des dizaines d'antivirus.	**Gratuit**	virustotal.com

3. Les bons réflexes (en plus des outils)

Le bon réflexe	Pourquoi c'est important
Ne donnez jamais un code reçu	Aucune banque, aucun service public ne vous demandera un code reçu par SMS ou par téléphone. C'est toujours une arnaque.
Tapez l'adresse vous-même	N'utilisez pas le lien d'un message. Ouvrez le site en tapant son adresse. Un service public se termine toujours par .gouv.fr.
Méfiez-vous de l'urgence et de la peur	« Compte bloqué », « dernier rappel », « amende à payer » : la pression et la menace sont la signature des arnaques.
Vérifiez le vrai expéditeur	Le nom affiché peut être faux. Regardez l'adresse e-mail ou le numéro complet : une faute ou un domaine bizarre = piège.
Applis : magasin officiel seulement	N'installez jamais une appli via un lien reçu par SMS ou mail. Passez toujours par l'App Store ou Google Play.
QR codes : prudence (quishing)	Ne scannez pas un QR code reçu par message ou collé dans la rue sans vérifier l'adresse affichée avant d'ouvrir.
Dans le doute, demandez de l'aide	Prenez le temps de vérifier, appelez l'organisme via son vrai numéro, ou demandez à un proche. Personne ne vous reprochera d'être prudent.

Cédric WALTENER · Médiateur Numérique · waltenercedric@proton.me