



Sécurité informatique

Les bons réflexes

Protégez vos données · Reconnaissez les arnaques · Sécurisez vos mots de passe

Ce guide s'adresse à tous. Pas de jargon — des faits concrets et des réflexes simples pour protéger vos données au quotidien.

01 Mots de passe — la première ligne de défense

La majorité des comptes piratés utilisaient un mot de passe réutilisé ou trop court. La règle est simple : **un compte = un mot de passe unique**. Un gestionnaire (Bitwarden, KeePass) vous évite de tout mémoriser.

Critère	À éviter	À adopter
Longueur	chat (4 car.)	ch@tBlueSky2024! (16 car.)
Unicité	Même partout	1 mot de passe par compte
Complexité	bonjour1	B0nj0ur!Landes40
Mémorisation	Post-it sur l'écran	Gestionnaire de mots de passe

Authentification à deux facteurs (2FA) — Même si votre mot de passe est volé, le 2FA bloque l'accès. Activez-le sur votre messagerie, votre banque, vos réseaux sociaux. Préférez une application (Google Authenticator, Authy) au SMS.

02 Reconnaître les arnaques courantes

Le phishing consiste à vous faire croire qu'un email provient d'un organisme de confiance pour vous soutirer des informations ou vous faire cliquer sur un lien malveillant.

CRITIQUE Faux email bancaire

Votre banque ne demande jamais vos codes par email. Signalez, supprimez sans cliquer.

CRITIQUE SMS frauduleux (smishing)

« Votre colis est bloqué » + lien suspect. Accédez directement au site officiel.

ATTENTION Faux support technique

Personne ne vous appellera spontanément pour accéder à distance à votre ordinateur.

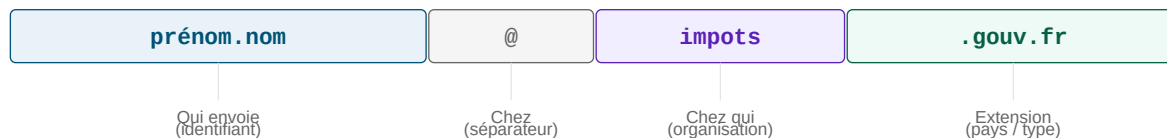
INFO Wi-Fi public

Évitez les opérations sensibles. Utilisez un VPN si nécessaire.

03 Lire un email comme un expert

Un email frauduleux imite souvent parfaitement le design d'un organisme officiel. La vigilance s'exerce sur **l'en-tête technique** — que les escrocs ne peuvent pas falsifier complètement.

Anatomie d'une adresse email



L'expéditeur affiché peut être un alias — vérifiez l'adresse réelle

Dans la plupart des clients mail (Outlook, Gmail, Apple Mail), cliquez sur le nom de l'expéditeur pour révéler l'adresse technique complète. L'alias affiché peut être « Service Clients BNP » alors que l'adresse réelle est `noreply@mailier99.ru`.

De : Service Clients <contact@boutique-promo.fr>

Expéditeur réel : `noreply@mailier99.ru` ← domaine .ru (Russie)

Heure d'envoi : `03h17` ← envoi nocturne, signal d'alerte

Reply-To : `collecte-donnees@form-secure.xyz` ← domaine inconnu

Objet : Votre commande est bloquée – action requise

Heure d'envoi — signal d'alerte



Note : certaines administrations ou services automatisés peuvent envoyer la nuit. Croisez toujours plusieurs indices avant de conclure.

Ressources officielles en cas de doute

Site	Usage	URL
Whois DomainTools	Vérifier le propriétaire d'un domaine	whois.domaintools.com
Signal-Spam	Signaler un email frauduleux	signal-spam.fr
Cybermalveillance.gouv.fr	Aide aux victimes	cybermalveillance.gouv.fr

04 Mises à jour — ne jamais reporter

Les mises à jour corrigent des failles de sécurité connues. Reporter une mise à jour, c'est laisser une porte ouverte. **Activez les mises à jour automatiques** sur votre ordinateur, téléphone, box internet et applications.

05 Sauvegardes — la règle 3-2-1

3 copies minimum

Au moins 3 exemplaires de vos données

2 supports différents

Disque externe + cloud ou NAS

1 exemplaire hors site

Une copie stockée hors de chez vous

Testez régulièrement vos sauvegardes : une sauvegarde non vérifiée n'est pas une sauvegarde.

06 Ma liste de contrôle

- ☐ J'utilise un mot de passe différent par site ou service
- ☐ J'ai activé l'authentification à deux facteurs (2FA) sur ma messagerie
- ☐ Mon téléphone et mon ordinateur se mettent à jour automatiquement
- ☐ Je sauvegarde mes données régulièrement (disque externe + cloud)
- ☐ Je vérifie l'adresse réelle de l'expéditeur avant d'ouvrir un email
- ☐ Je n'effectue pas d'opérations bancaires sur Wi-Fi public
- ☐ J'utilise un antivirus ou la protection intégrée de mon système
- ☐ Je sais comment signaler une arnaque (signal-spam.fr)



Assistance informatique et administrative à domicile

Envie d'aller plus loin ?

Ce guide couvre les fondamentaux. En formation ou lors d'une intervention sur site, nous analysons ensemble vos pratiques et mettons en place des règles concrètes.

Site : www.macwin.fr

Email : contact@macwin.fr

Tél : 06.18.49.09.10

Adresse : 4 Rue de l'Adour — 40480 Vieux-Boucau-les-Bains

R.C.S. Bordeaux 838 944 353 — MACWIN 2025