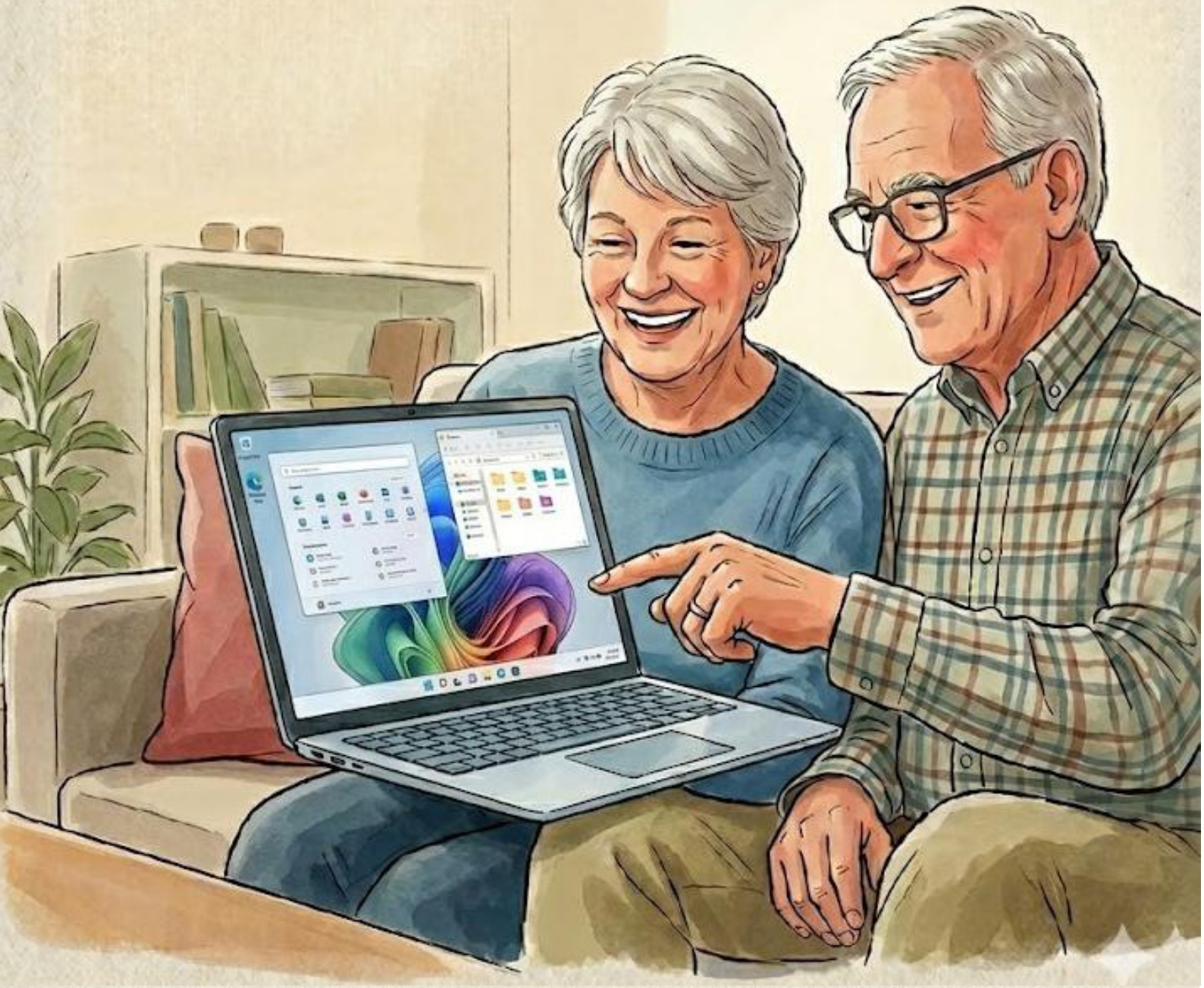
WINDOWS EN TOUTE SECURITE

GUIDE POUR LES SENIORS

Astuces concrètes, protection et sérénité pour une bonne maîtrise du système Windows

FEDERATION FRANÇAISE RETRAITE SPORTIVE
SPORT SENIOR SANTÉ
COMITE D'ILLE & VILAINE



Une publication du CODERS 35

COMPRENDRE LES RISQUES DE WINDOWS

LES MENACES LOGICIELLES (LOGICIELS MALVEILLANTS)

Les logiciels malveillants peuvent s'installer discrètement, voler des informations ou endommager des fichiers. Ils profitent souvent des failles de sécurité.

LES ATTAQUES EN LIGNE (NAVIGATION INTERNET)

Les sites web malveillants tentent de tromper les utilisateurs pour obtenir des mots de passe ou installer des logiciels nuisibles via de fausses alertes.

LES RISQUES LIÉS AUX EMAILS ET MESSAGES (PHISHING)

Des courriels falsifiés peuvent imiter des institutions ou contacts connus pour voler des informations personnelles ou financières.

LA VULNÉRABILITÉ DU SYSTÈME (LOGICIELS OBSOLÈTES)

Les anciennes versions de Windows et des logiciels ont des vulnérabilités connues qui peuvent être exploitées si les mises à jour ne sont pas effectuées.

L'INGÉNIERIE SOCIALE (MANIPULATION HUMAINE)

Des escrocs utilisent la manipulation, par téléphone ou message, pour obtenir un accès à l'ordinateur ou des paiements sous de faux prétextes.

LA PERTE OU LE VOL DE DONNÉES (MATÉRIEL ET FICHIERS)

Les fichiers importants (photos, documents) peuvent être irrémédiablement perdus en raison de pannes matérielles, de suppression accidentelle ou de vol physique de l'ordinateur.

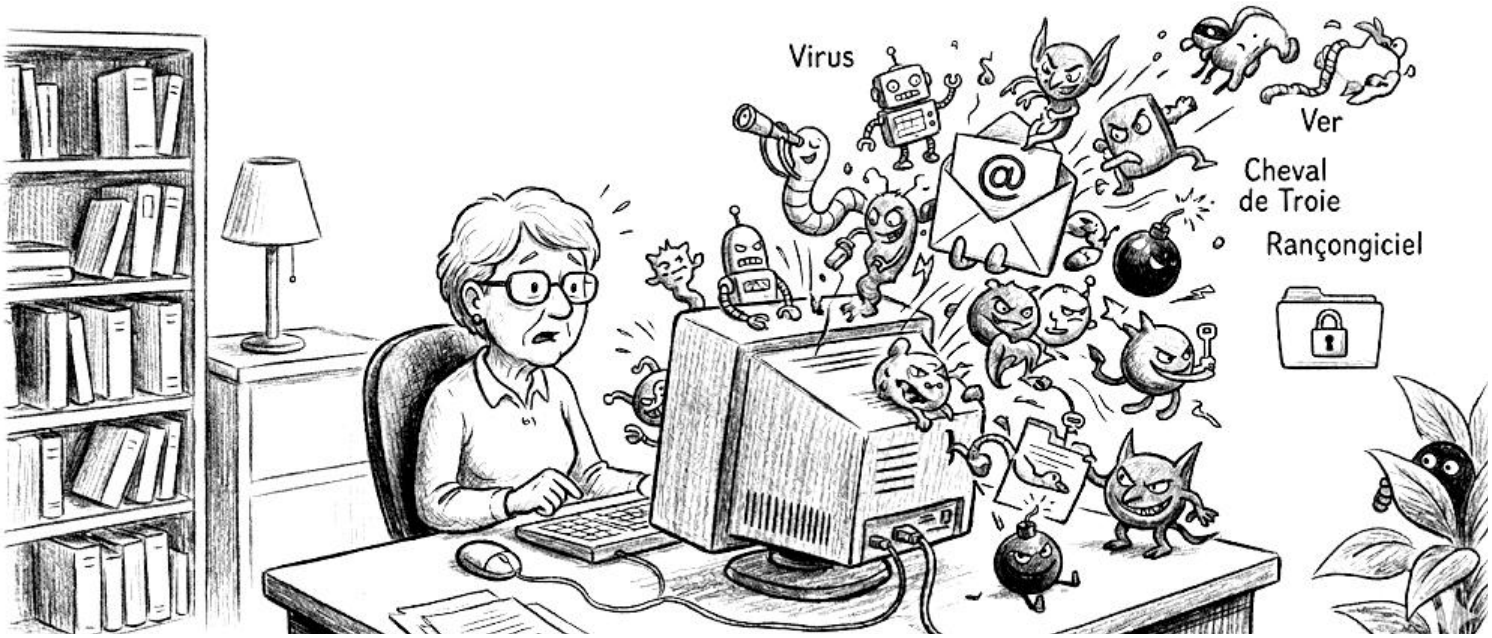
WINDOWS ET LA SÉCURITÉ INFORMATIQUE

Ce que tout senior devrait savoir pour naviguer en sécurité

Utiliser un ordinateur sous Windows est aujourd'hui aussi courant que de regarder la télévision. Mais comme dans la vie réelle, il existe des personnes malintentionnées qui cherchent à profiter des moins avertis. Ce guide vous explique, sans jargon, comment reconnaître les dangers et vous en protéger.

LES LOGICIELS MALVEILLANTS

Un logiciel malveillant (ou « malware » en anglais) est un programme conçu pour nuire à votre ordinateur ou à vous-même. Il en existe plusieurs variétés, chacune ayant un mode d'action différent.



Le virus classique

Comme un vrai virus biologique, il se propage d'un fichier à l'autre et peut ralentir, bloquer ou corrompre votre ordinateur. Il arrive souvent via une pièce jointe ou un fichier téléchargé sur Internet.

Le cheval de Troie

Caché dans un programme apparemment inoffensif (un jeu gratuit, un utilitaire), il s'installe discrètement et ouvre une "porte dérobée" sur votre ordinateur pour permettre aux pirates d'y accéder à distance.

Le rançongiciel (ransomware)

Le plus redoutable aujourd'hui : il chiffre tous vos fichiers (photos, documents, vidéos) et réclame une rançon pour les récupérer. Même payer ne garantit pas la restitution de vos données.

L'espion (spyware)

Silencieux et invisible, il observe ce que vous tapez sur votre clavier - mots de passe, numéros de carte bancaire - et envoie ces informations à des pirates sans que vous vous en aperceviez.

Analogie pour mieux comprendre

Imaginez que quelqu'un glisse un colis piégé dans votre boîte aux lettres. Le virus, c'est le colis qui abîme la boîte. Le cheval de Troie, c'est un livreur qui vous remet une belle bouteille de vin… et qui en profite pour copier vos clés. Le rançongiciel, lui, barricade votre maison et vous demande de payer pour rentrer chez vous.

⚠ Signe d'alerte

Votre ordinateur est soudainement très lent, des publicités apparaissent partout, ou un message inhabituel vous demande de l'argent ? Ne payez pas. Éteignez l'ordinateur et appelez un proche ou un technicien de confiance.

LE PHISHING : L'ARNAQUE PAR E-MAIL

Le mot "phishing" vient de l'anglais fishing - la pêche. Les pirates "lancent leur hameçon" en vous envoyant de faux e-mails qui ressemblent à des messages officiels (banque, La Poste, impôts, Ameli…) pour vous soutirer des informations personnelles.

Comment reconnaître un e-mail piégé ?

L'expéditeur a une adresse bizarre : impots-gouv@gmail.com n'est PAS l'administration fiscale

Le message crée une urgence anxiété : "Votre compte sera bloqué dans 24h"

Il vous demande de cliquer sur un lien et d'entrer votre mot de passe ou numéro de carte

L'e-mail contient des fautes d'orthographe ou un français maladroit

En cas de doute, appelez directement l'organisme via le numéro de son site officiel

Analogie

C'est comme recevoir une lettre qui ressemble parfaitement à un courrier de votre banque, mais fabriquée par des escrocs. L'enveloppe et le logo sont identiques, mais l'adresse de retour ne correspond pas.

✓ Règle d'or

Votre banque, La Poste ou les impôts ne vous demanderont JAMAIS vos identifiants ou votre numéro de carte par e-mail. Si un message vous le demande, c'est une arnaque.

LES FAILLES "ZERO-DAY"

Un logiciel, aussi bien conçu soit-il, peut contenir des défauts cachés. Quand des pirates découvrent l'un de ces défauts avant que les éditeurs (comme Microsoft) ne le sachent, ils peuvent s'en servir pour attaquer des millions d'ordinateurs. C'est ce qu'on appelle une faille "zero-day" : les victimes ont eu zéro jour pour se préparer.

Analogie

Imaginez qu'un cambrioleur découvre que votre immeuble a une entrée secrète que même le gardien ignore. Il peut entrer chez tous les résidents avant que quiconque soit averti. La seule protection est que le gardien soit informé rapidement et condamne cette entrée - c'est exactement ce que fait une mise à jour Windows.

✓ Bonne nouvelle

Vous ne pouvez pas empêcher l'existence de ces failles, mais vous pouvez installer les correctifs dès qu'ils sont disponibles. C'est précisément le rôle des mises à jour Windows : colmater ces brèches au plus vite.

L'ATTAQUE DE L'"HOMME DU MILIEU"

Cette attaque se produit lorsqu'un pirate s'intercale discrètement entre vous et le site que vous consultez. Il peut ainsi lire, modifier ou voler les informations que vous échangez, sans que vous vous en rendiez compte.

Ce risque est particulièrement élevé lorsque vous vous connectez à un réseau Wi-Fi public : café, gare, bibliothèque, hôtel… Ces réseaux sont souvent peu ou pas sécurisés.

Analogie

Imaginez que vous envoyez une lettre à votre banque, mais qu'un employé malveillant de La Poste ouvre l'enveloppe, note vos informations, la referme et la renvoie comme si de rien n'était. Ni vous ni votre banque ne vous doutez de rien.

Ce qu'il faut faire

- Ne jamais effectuer d'opérations bancaires sur un Wi-Fi public
- Méfiez-vous des sites dont l'adresse commence par http:// sans le "s" final
- Un petit cadenas dans la barre d'adresse de votre navigateur signifie que la connexion est chiffrée
- Préférez votre connexion mobile (4G/5G) pour les opérations sensibles

LE DANGER DES ANCIENNES VERSIONS DE WINDOWS

Windows est un logiciel qui évolue. Quand une version devient trop ancienne, Microsoft cesse de lui fournir des correctifs de sécurité - c'est la "fin de support". Un ordinateur sous une version non maintenue est comme une maison dont on aurait cessé de réparer les serrures : toutes les nouvelles techniques de cambriolage deviennent efficaces.

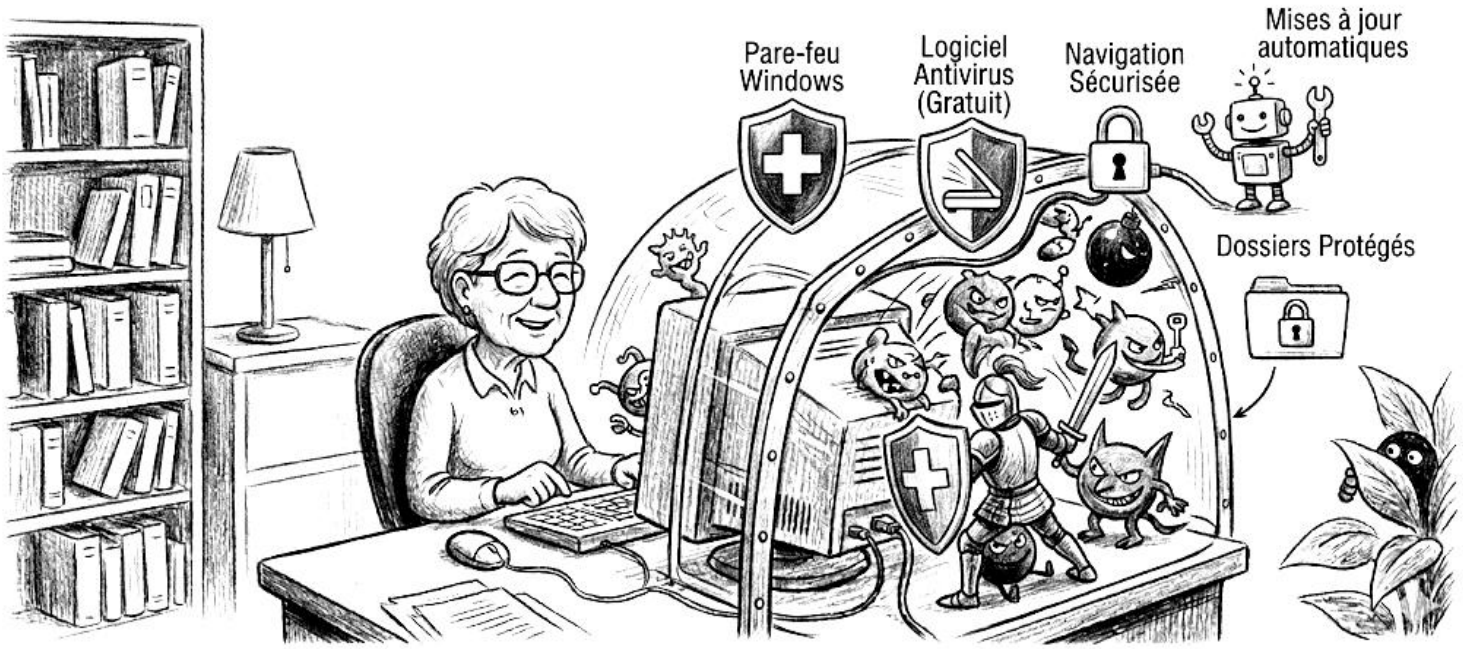
Version Windows	Fin de support	Situation
Windows XP	Avril 2014	Très dangereux ⚠ ⚠
Windows Vista	Avril 2017	Très dangereux ⚠ ⚠
Windows 7	Janvier 2020	Très dangereux ⚠ ⚠
Windows 8/8.1	Janvier 2023	Dangereux ⚠
Windows 10	Octobre 2025	Mettre à jour bientôt
Windows 11	2028 et au-delà	Recommandé ☑

⚠ **Urgent si vous utilisez Windows 7 ou XP**

Ces versions ne reçoivent plus aucun correctif depuis plusieurs années. N'importe quel pirate peut s'introduire sur votre ordinateur via des failles connues de tous. Nous vous conseillons vivement de mettre à jour votre système ou d'acquérir un nouvel ordinateur.

LES SOLUTIONS DE PROTECTION

La bonne nouvelle, c'est qu'il existe de nombreux outils pour vous protéger - et certains sont même inclus gratuitement dans Windows.



Windows Defender - l'antivirus intégré

Gratuit, automatique et déjà présent sur votre ordinateur. Il surveille en permanence les menaces. Vérifiez simplement qu'il est bien activé (cherchez "Sécurité Windows" dans le menu Démarrer).

Les mises à jour Windows

Installez-les dès qu'elles sont proposées. Elles corrigent les failles avant que les pirates ne puissent en profiter. Vous pouvez les autoriser à s'installer automatiquement la nuit.

La sauvegarde régulière

Copiez vos photos et documents importants sur un disque dur externe. En cas de rançongiciel, vous récupérez tout sans payer. Débranchez le disque après la sauvegarde.

Le gestionnaire de mots de passe

Un outil comme Bitwarden (gratuit) retient à votre place des mots de passe forts et uniques pour chaque site. Vous n'avez besoin de retenir qu'un seul mot de passe principal.

Le navigateur à jour

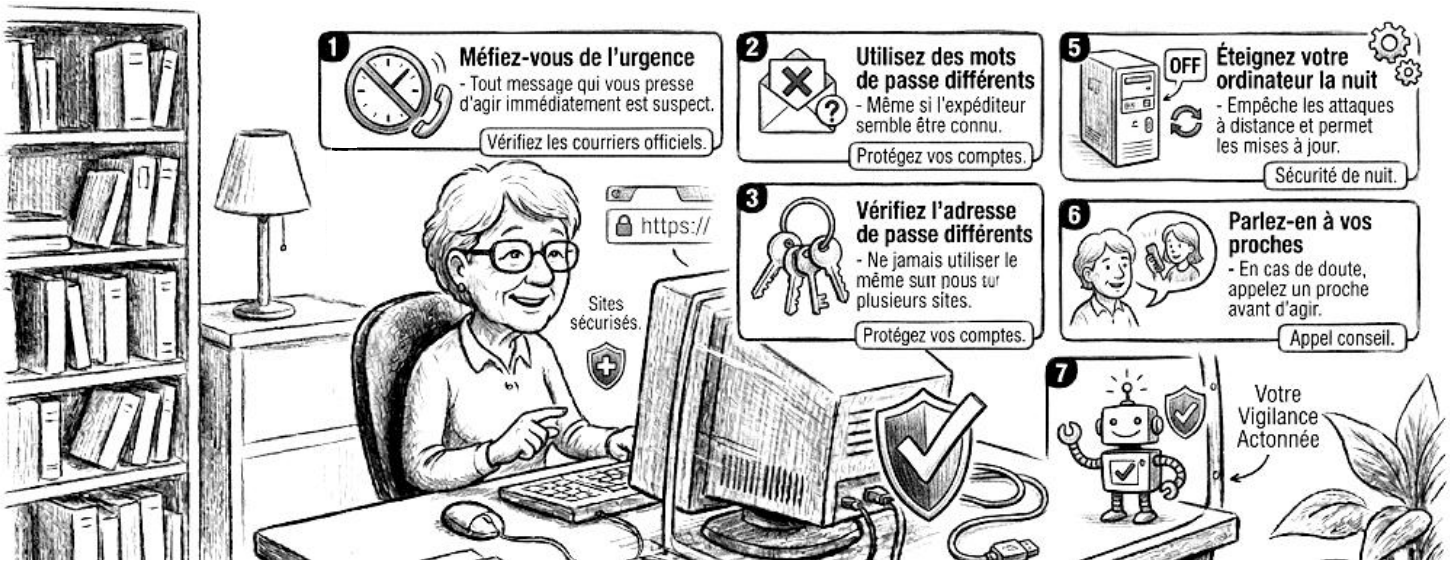
Utilisez Firefox, Chrome ou Edge dans leur dernière version. Ils bloquent de nombreux sites dangereux automatiquement et signalent les tentatives de phishing.

Astuce

Si vous n'êtes pas à l'aise pour configurer tout cela seul, demandez à un proche ou contactez une association locale d'aide informatique aux seniors. Certaines mairies proposent des ateliers numériques gratuits.

LES BONS RÉFLEXES AU QUOTIDIEN

La meilleure protection reste votre vigilance. Voici les sept habitudes les plus importantes à adopter :



1. **Méfiez-vous de l'urgence** - Tout message qui vous presse d'agir immédiatement est suspect. Les vraies institutions prennent le temps d'envoyer des courriers officiels.
2. **N'ouvrez pas les pièces jointes inattendues** - Même si l'expéditeur semble être votre banque ou un ami. Vérifiez par téléphone avant d'ouvrir quoi que ce soit.
3. **Utilisez des mots de passe différents** - Ne jamais utiliser le même mot de passe sur plusieurs sites. Si l'un est volé, les autres restent protégés.
4. **Vérifiez l'adresse des sites web** - Un cadenas et "https://" dans la barre d'adresse indiquent un site sécurisé. Sans cela, ne saisissez aucune information personnelle.
5. **Éteignez votre ordinateur la nuit** - Un ordinateur éteint ne peut pas être attaqué à distance. Cela permet aussi aux mises à jour de s'installer correctement.
6. **Parlez-en à vos proches** - En cas de doute, appelez un proche avant de faire quoi que ce soit. Mieux vaut une question de plus qu'une erreur irréversible.

En France, en cas d'arnaque

Signalez toute tentative sur cybermalveillance.gouv.fr ou appelez le 3018 (numéro national). Votre signalement aide à protéger d'autres personnes.

SOLUTIONS POUR UTILISER WINDOWS SANS RISQUE

PROTÉGER LE SYSTÈME AVEC UN ANTIVIRUS

Installer un logiciel antivirus réputé. Planifier des analyses régulières et le maintenir à jour.

NAVIGUER SANS RISQUE SUR INTERNET

Éviter les sites douteux. Installer un bloqueur de pop-ups. Ne jamais saisir d'informations sur des sites non sécurisés.

IDENTIFIER ET ÉVITER LE PHISHING (HAMEÇONNAGE)

Vérifier l'expéditeur et les liens. Se méfier des offres trop belles ou urgentes. Signaler les spams.

MAINTENIR VOTRE WINDOWS ET LOGICIELS À JOUR

Activer les mises à jour automatiques pour le système et les navigateurs. Ne pas utiliser de versions obsolètes.

ADOPTER DE BONNES PRATIQUES DE SÉCURITÉ

Utiliser des mots de passe complexes et uniques. Activer la double authentification (2FA). Se méfier des appels non sollicités.

SAUVEGARDER VOS DONNÉES PRÉCIEUSES

Sauvegarder régulièrement vos photos et documents sur un disque dur externe et/ou le cloud (sauvegarde régulière).

FEDERATION FRANÇAISE RETRAITE SPORTIVE
SPORT SENIOR SANTÉ

La Licence Unique :
Votre Passeport Sport, Santé et Convivialité

Le Concept de la Licence Unique

Un seul paiement pour tout pratiquer

Accédez librement à l'ensemble des activités proposées sans surcoût d'adhésion par discipline

Un réseau national sans frontières

Votre licence vous donne accès à l'ensemble des 460 clubs du réseau national

Ce qui est inclus dans votre adhésion

Plus de 60 activités sportives et cognitives

Du tai-chi à la randonnée, incluant des programmes exclusifs comme Activ'mémoire

Une assurance complète et sécurisante

Couverture individuelle accident, responsabilité civile et garanties spécifiques pour les séjours

L'information au cœur de votre pratique

Réception régulière des publications de la fédération et de votre comité départemental

Un Engagement Bénévole et Solidaire

6 000 animateurs bénévoles certifiés

Un encadrement de qualité assuré par des passionnés formés par la fédération

Un coût très modeste

Des tarifs accessibles grâce au dévouement et au fonctionnement bénévole de la structure