SIRIKITECH

IT Support you can trust — Support informatique de confiance

Protect Your Home & Small Business

A Simple, No-Jargon Security Guide

Protégez votre foyer et votre petite entreprise — Guide simple, sans jargon

Introduction

EN

Most cyber attacks on individuals and small businesses are not sophisticated. They succeed because of small, avoidable mistakes: a reused password, an unlocked router, an unpatched laptop. This short guide gives you the essential steps to protect yourself, in plain English, with no technical background required.

FR

La plupart des cyberattaques contre les particuliers et petites entreprises ne sont pas sophistiquées. Elles réussissent à cause de petites erreurs évitables : un mot de passe réutilisé, un routeur non sécurisé, un ordinateur non mis à jour. Ce guide vous donne les étapes essentielles pour vous protéger, en langage simple, sans connaissances techniques requises.

1. Passwords & Accounts / Mots de passe et comptes

EN — What to do

- Use a different password for every important account (email, banking, work).
- Aim for at least 12 characters — a short sentence is easier to remember and harder to crack than "P@ssw0rd1".
- Turn on two-factor authentication (2FA) wherever it's offered — this is the single most effective step you can take.
- Never share passwords over the phone, email, or text — legitimate companies will never ask you to.

> **Quick win:** Turn on 2FA for your email account today. If someone can't get into your email, they usually can't reset your other accounts either.

FR — Que faire

- Utilisez un mot de passe différent pour chaque compte important (email, banque, travail).
- Visez au moins 12 caractères — une courte phrase est plus facile à retenir et plus difficile à deviner que "P@ssw0rd1".
- Activez l'authentification à deux facteurs (2FA) partout où c'est possible — c'est l'action la plus efficace que vous puissiez faire.
- Ne partagez jamais vos mots de passe par téléphone, email ou SMS — une entreprise sérieuse ne vous le demandera jamais.

2. Your Home / Business Wi-Fi

EN — What to do

- Change the default router password (the one printed on the box) — this is one of the most common ways homes get compromised.
- Use WPA3 or WPA2 encryption (check your router settings) — never leave your network "open".
- Set up a separate guest Wi-Fi network for visitors and smart devices (TVs, cameras) so they're isolated from your main computers.

FR — Que faire

- Changez le mot de passe par défaut du routeur (celui imprimé sur la boîte) — c'est l'une des causes les plus fréquentes de piratage à domicile.
- Utilisez le chiffrement WPA3 ou WPA2 — ne laissez jamais votre réseau "ouvert".
- Créez un réseau Wi-Fi invité séparé pour les visiteurs et les objets connectés (TV, caméras), pour les isoler de vos ordinateurs principaux.

3. Recognising Phishing & Scams

EN — Warning signs

- Urgent language: "Act now or your account will be closed."
- Requests for payment via gift cards or bank transfer only.
- Slightly wrong email addresses (e.g. "@paypa1.com" instead of "@paypal.com").
- Links that don't match the company name when you hover over them.

> **Rule of thumb:** If a message creates panic or pressure, stop. Contact the company directly using a number or website you already trust — never the one in the message.

FR — Signes d'alerte

- Langage urgent : "Agissez maintenant ou votre compte sera fermé."
- Demande de paiement uniquement par carte cadeau ou virement bancaire.
- Adresses email légèrement incorrectes (ex : "@paypa1.com" au lieu de "@paypal.com").
- Liens qui ne correspondent pas au nom de l'entreprise une fois survolés.

4. Keeping Devices Updated

EN

Updates aren't just new features — they fix security holes that criminals actively exploit. Turn on automatic updates for your operating system (Windows, macOS), your browser, and your antivirus software. Old, unsupported devices (e.g. very old Windows 7 machines) are a serious risk — consider replacing or retiring them.

FR

Les mises à jour ne sont pas seulement de nouvelles fonctionnalités — elles corrigent des failles de sécurité activement exploitées par les criminels. Activez les mises à jour automatiques pour votre système d'exploitation (Windows, macOS), votre navigateur et votre antivirus. Les appareils anciens non pris en charge (ex : très vieux Windows 7) représentent un risque sérieux — envisagez de les remplacer.

5. Backups — Your Safety Net

EN

If ransomware locks your files, or your laptop is lost, stolen, or simply breaks, a backup is what saves you. Follow the simple "3-2-1" rule: 3 copies of your data, on 2 different types of storage, with 1 copy kept off-site (e.g. cloud storage like OneDrive or Google Drive).

FR

Si un rançongiciel bloque vos fichiers, ou si votre ordinateur est perdu, volé ou simplement en panne, une sauvegarde est ce qui vous sauve. Suivez la règle simple "3-2-1" : 3 copies de vos données, sur 2 types de stockage différents, dont 1 copie hors site (ex : stockage cloud comme OneDrive ou Google Drive).

Quick Checklist / Liste de vérification rapide

☐	2FA enabled on email & banking / 2FA activé sur email et banque
☐	Router default password changed / Mot de passe routeur changé
☐	Automatic updates turned on / Mises à jour automatiques activées
☐	Backup set up (cloud or external drive) / Sauvegarde en place
☐	Guest Wi-Fi network created / Réseau Wi-Fi invité créé
☐	Antivirus installed and up to date / Antivirus installé et à jour

Need help putting this into practice?

SirikiTech offers home & small business IT support, security check-ups, and device setup — in English and French.

🌐 sirikitech.com | 📘 Facebook: SirikiTech | 📍 London