immervox

2025

# ESSENTIAL CYBER SECURITY GUIDE

Practical, jargon-free advice your team can follow to stay secure and protect your business.

www.immervox.com

# About Us.

## Introduction

At Immervox we curate bespoke telecoms, cyber security and IT solutions to ensure businesses stay connected, secure, and compliant, enabling uninterrupted operations.

Our ex-military Board and engineer-led approach is backed by 25 years of experience, delivering reliable, vendor-agnostic/independent solutions.

With 24/7 UK-based support and a commitment to UK data compliance, we protect business critical information, prioritise genuine value and build long-term partnerships.

# Passwords & Authentication.

- Use unique passwords for every system or account.
- Never reuse passwords — especially for work and personal accounts.
- Always enable Multi-Factor Authentication (MFA) where available.
- Don’t write passwords down — use a secure password manager.
- Make passwords long (12+ characters) and include symbols.
- Avoid using birthdays, pet names, or obvious personal details.
- Change default passwords on all devices and software.
- Never share your passwords — even with colleagues.
- Use passphrases instead of passwords (e.g. “PurpleHorsesDance@9”).
- Watch out for fake MFA prompts — attackers may try to trick you into approving a login.

# Phishing & Email Awareness.

- Always check the sender address — not just the display name.
- Don’t click on links from unknown or unexpected sources.
- Hover over links to preview the URL before clicking.
- If an email feels urgent or emotional — pause and verify it.
- Be suspicious of grammar and spelling mistakes.
- Never open unexpected attachments — even from known contacts.
- Report phishing attempts to your IT or Security team immediately.
- Look for subtle domain name spoofing (e.g. “rnicrosoft.com”).
- Use Outlook’s “Report Phishing” button if available.
- Beware of fake invoice or payment requests, especially near month-end.

# Device & Endpoint Security.

- Lock your computer when stepping away — even for a moment.
- Don’t plug in unknown USB devices — they could be infected.
- Keep your operating system and apps fully up to date.
- Install only approved software — avoid freeware or unknown tools.
- Use antivirus/EDR software — and make sure it’s active and updating.
- Avoid public Wi-Fi — or use a VPN when working remotely.
- Don’t let others use your work devices — even family members.
- Back up your files regularly — and know where they’re stored.
- Use screen privacy filters when working in public spaces.
- Restart your machine weekly to apply security updates.

# Browsing & Internet Use.

- Only visit trusted websites — look for HTTPS and padlock icons.
- Avoid clicking on ads or popups.
- Don’t download from torrent or piracy sites.
- Never enter sensitive information on unfamiliar websites.
- Be careful with browser extensions — install only verified ones.
- Clear your browser cache and cookies regularly.
- Log out of web apps after use — especially on shared devices.
- Disable auto-fill for sensitive fields in your browser.
- Don’t use “Sign in with Facebook/Google” for work systems.

# Remote Work Security.

- Use company-approved VPN when working from home.
- Ensure your home Wi-Fi has a strong password and WPA2/WPA3 encryption.
- Don’t let Alexa, Siri, or smart devices eavesdrop in your home office.
- Store work devices securely when not in use.
- Avoid working in cafés or shared spaces with sensitive data.
- Don’t take photos of your workstation or screen — watch the background!

www.immervox.com

# Immervox Limited

If you still have some questions, or would like some support making sure your business is secure, reach out to our experienced advisors.

☎ 0333 014 6220

✉ sales@immervox.com