CYBER WARDEN

PRACTICAL CYBER RISK MANAGEMENT

# Cyber Survival Guide

## Chapter 1: The Basics

Small & medium sized businesses (and surprisingly, some large businesses) don't usually have a huge budget for anything that doesn't directly benefit the business.
At the same time, especially when you have just yourself or a handful of employees, you don't usually have an IT or CyberSecurity specialist on staff. It's usually just a case of get it working and that'll be enough.
With that in mind, Here's some tips to avoid having to live in your car with your dog because someone stole all your money or destroyed your business, and now you can't afford rent or mortgage payments, and your employees and creditors are hunting you down because they want to be paid.
No-one is too poor, and no business is too small for the scammers to target. They actually perfer to target small & medium businesses because they're usually easier.

### Authentication

This is how you prove that you are who you say you are and is required for the remaining steps.

- Use Passkeys where you can, but be aware of their limitations and make sure that you register two separate passkeys for every service that you use them on in case you lose access to one of them.
- Utilize a trusted password manager – (NEVER use the built-in password manager in your browser or operating system). This software stores your passwords (and other authentication methods) securely, and a good one will be available on all your devices.
    - We recommend Bitwarden Professional for individuals, and BitWarden Teams if you have staff.
    - Ensure that your password manager supports MFA, and use a separate app to manage the OTP or a physical authentication token such as a YubiKey.
- Authenticator App. This is the app that provides one-time passwords and authentication prompts.

    - We recommend Microsoft Authenticator if you are using Microsoft cloud services, and it works very well with the vast majority of other services that use one time passwords.
    - We recommend not to use SMS OTP if you can avoid it (they aren't as secure, and sometimes they just don't come through).
    - The Bitwarden app can also provide the OTP codes and store passkeys for sites that support passkeys.
    - The Authenticator app should support MFA
- Create unique, complex passwords on EVERY account (your password manager will help you with this, also meaning you don't need to type those passwords)
- Enable MFA on EVERY account that you use.
- Enable biometric authentication for your physical devices. It's convenient, and it's relatively secure.
- On moble devices, set the pin code required to first login to the device after a reboot to a minimum of 6 digits.

## Email

Email is the lifeblood of your business, so take a little bit of time to protect it.

- Enforce MultiFactor Authentication on all mail accounts.
- If you have a custom domain (e.g. you@yourcompany.com) ensure that you configure DMARC to prevent people impersonating you, and to improve your mail deliverability. This is really easy (and cheap!) with a service like CyberWarden Mail Aegis.
- Utilize a 3rd party email security service like CyberWarden Mail Aegis to scan your email for phishing attempts and malware, even if your mail provider claims that they do this – two sets of eyes is always better than one.
- NEVER scan QR codes in emails.
- NEVER click links in emails.
- If you get an email from anyone saying that their account has changed and you need to send payments to a different account, Pick up the phone and verify the change with them directly. Don't use any contact information in the email.
- If you get an email from anyone telling you that you need to reset your password, NEVER click on the link, and DON'T copy/pase the link from the email. Go to the service directly, login and change it yourself if the service prompts you to change your password.
- Banks NEVER include links in their emails.
- The police, customs, or the central bank will NEVER contact you by email, SMS, WhatsApp, etc. If they're after you, you'll know. Usually at 3am.
- NEVER share card numbers over email.
- Remember – you're not paranoid if they're really out to get you (and they are).

## Data

Once you have created unique, complex passwords on your accounts, and enabled MFA, the safest place for all your data is in the cloud. Microsoft OneDrive, Apple iCloud, Google Drive, and Box.com are examples of cloud storage that can replicate to your laptop for seamless offline use if necessary.

- Our recommendation is to use the cloud storage that comes with your Microsoft 365 or Google Workspace account. It works seamlessly with those services.
- Backup your data. The cloud providers don't provide this service, but does provide some limited protection against accidental deletion or even ransomware. We can help you with this (Included in Cyber Warden Mail Aegis Gold)
- Data that only exists on your computer is lost if something happens to your computer.
- There are several options for backing up your data, including manual backups, automatic backups on premises, and automatic cloud based backups.

## Malware

Malware refers to any software that you really don't want on your systems. It includes Virus, Worms, Stealers, encryptors, adware, etc.

- Use good Anti-Malware software on ALL your devices
    - Yes, Mac and Linux computers do get malware all the time
    - You get what you pay for, and some "free" anti-malware providers have been caught selling your data, and some is fake.
    - We recommend a managed XDR service like Crowdstrike, or the commercial version of Microsoft Defender, as they will protect all your devices. These services are typically billed on a per-seat basis.
- In conjuction with your anti-malware software, use a DNS filtering service
    - Can help protect against malicious websites (including phishing)
    - Can help disrupt the Command & Control component of malware on your system
    - We recommend NextDNS as an easy, effective, and inexpensive option, but there are plenty of other good, paid alternatives, including Cloudflare.
- NEVER install cracked software.
    - Nothing ever comes for free
    - No security updates
    - Often comes pre-loaded with malware
- Keep your systems up to date
    - Enable the auto update feature on all your devices for both applications and the operating system.
    - Don't forget about things like your internet router, your wireless access points, and NAS boxes. Even smart TVs need regular updates.

## Stay Invisible

Don't expose anything directly to the internet.

- NAS (Network Attached Storage)
- PBX Systems
- If you can see it from the internet, so can the bad guys. There's smarter ways of doing these things.

Don't leave your stuff lying around in plain view/unsecured, even in the office.

- Keys
- USB drives
- Laptops/Phones/Tablets
- Notebooks/note pads
- Documents

## Don't Over-Share

Social media can be fun, and are great for sharing business (and personal) updates.

- Don't announce that you're traveling anywhere – Wait until after you get back before you share that news.
- Be aware of what is in pictures that you share, especially in the office.
    - Computer screens
    - Phone screens
    - Security cameras
    - Whiteboards & flipcharts
    - Documents lying around
    - Credit cards etc.
    - Post-it notes

Be discrete. Remember that the walls have ears (and eyes).

- Don't discuss anything that you don't want a competitor or a bad guy to hear in public, including on the phone.
    - You're not a Kardashian. NEVER have your phone on loudspeaker in public. Do whatever you like at home.
- Don't view/edit anything that you wouldn't post on facebook in public. Yes, that includes airline lounges, coffee shops, planes, etc.
- Screen privacy filters are security theatre. Don't believe me? Have a look next time you're in a plane or a coffee shop and someone is tapping away on their laptop or phone. If you're behind them, their screen is visible. This is called shoulder surfing.
- Beware of cameras. Phones and security cameras can get a really detailed view of what's on your screen, your keyboard, and record your voice.