CYBER WARDEN

PRACTICAL CYBER RISK MANAGEMENT

Cyber Survival Guide: Basics

PROTECT YOURSELF AND YOUR ORGANIZATION

Andrew MacLachlan

December 2024

CYBER WARDEN
PRACTICAL CYBER RISK MANAGEMENT

Perception

- Security is expensive, with no tangible benefit
- My IT guy knows what he's doing
- Security is inconvenient
- Security slows down business
- I have nothing to hide and no secrets
- We're just a small business, no-one is going to attack us
- The UAE is safe
- Our developers look after all the security stuff

CYBER WARDEN
PRACTICAL CYBER RISK MANAGEMENT

Reality

- Scammers actively target small businesses
  - Lack of controls = easy target
  - Less chance of being hunted down by the authorities
- Your money is just as desirable as from a large business
- Small business losses are proportionally larger than for large businesses
  - 60% of small businesses that pay a ransom or are defrauded fail within 6 months
- It's orders of magnitude cheaper to prevent issues than to recover from them
- Your IT guy is a generalist, not a specialist
- Developers have a narrow field of specialism. You wouldn't ask a cardiologist to do brain surgery.

CYBER WARDEN
PRACTICAL CYBER RISK MANAGEMENT

Strong Authentication on everything

- Passkeys. Considered to be phishing resistant
  - Stored in physical hardware
    - Yubikey
    - OS based
- Time based One Time Password (TOTP)
  - Microsoft Authenticator, Google Authenticator
  - Code changes every 30-60 seconds
- Long complex passwords
  - Use a trusted password manager
    - Bitwarden, Lastpass, 1Password…
    - NOT the password manager built into your OS or browser
- Avoid SMS based OTPs where possible

CYBER WARDEN
PRACTICAL CYBER RISK MANAGEMENT

Secure your email

- Email is involved in over 90% of all cyber attacks
- DMARC with a reject policy helps stop impersonation attacks (spoofing)
- Strong Authentication makes password guessing & leaked credential attacks far less likely to succeed
- Utilize a 3rd party email scanning service to block many phishing and malware attacks
- Phishing Awareness

CYBER WARDEN
PRACTICAL CYBER RISK MANAGEMENT

Phishing Awareness

- Messages require you to follow a link to sign in to something
- Unexpected invoices
- “Our bank account has changed”
- Links in emails from banks
  - Banks NEVER include a link to their service
- Something is held in customs / needs payment for delivery…
- Central Bank, Police, etc.
- Urgency, Authority, and Fear are common themes
  - Problem & pressure
  - Central Bank, Police, etc
  - The boss requesting that you buy something like vouchers etc and send the codes
- QR codes in emails

CYBER WARDEN
PRACTICAL CYBER RISK MANAGEMENT

Messaging Safety

- NEVER send credit card details over email
- NEVER share OTPs
- If in doubt, Call the supposed sender using a number that you KNOW is correct and verify with them.
  - NEVER use the contact details in a suspect message
  - Couriers are always happy to accept payment for any customs, delivery charges on delivery.

CYBER WARDEN
PRACTICAL CYBER RISK MANAGEMENT

Data Safety

- Don't store or share data on USB drives etc
  - The cloud is safer and more convenient when protected with strong authentication
  - Use the cloud storage that is bundled with M365 / GWS.
- Check your shared data permissions regularly
- Backup your data
  - Protects against accidents and malicious actions
  - Use trusted automatic backup solutions
  - Cloud data is NOT backed up by the provider

CYBER WARDEN
PRACTICAL CYBER RISK MANAGEMENT

Malware

- ALWAYS use good anti-malware (anti-virus) software
  - Free Microsoft Defender is good. The commercial version is better, and may be included in your M365 subscription.
  - Crowdstrike Falcon and other commercial managed XDR services.
  - Don't use free 3rd party anti-malware software
- Macs are also affected by malware
- Use a DNS filtering service such as NextDNS
- Your email filter service must include with a malware and URL filter
- NEVER install cracked software – It usually includes malware or vulnerabilities.
- Enable auto-update on everything
- Don't use public WiFi – use mobile data

CYBER WARDEN
PRACTICAL CYBER RISK MANAGEMENT

Mobile Devices

- Use biometrics
- Use at least a 6 digit PIN
- Restart them at least every week
- Enable automatic updates for the OS and for apps
- ONLY install apps from the official app store
  - Don't sideload apps
  - Don't install unecessary/novelty apps
  - Check the app permissions before installing
  - Delete unneeded apps
- DO use Google/Apple/Samsung pay instead of credit cards
- Never hand the phone to someone else for payment

CYBER WARDEN
PRACTICAL CYBER RISK MANAGEMENT

Stay invisible

- Don't expose internal systems to the internet
  - NAS (Network Attached Storage)
  - PBX Systems
  - Remote control software
- If you can access it from the internet, so can the bad guys.

CYBER WARDEN
PRACTICAL CYBER RISK MANAGEMENT

Keep a clear desk

- Don't leave stuff lying around on desks etc.
  - Keys
  - USB drives
  - Laptops, phones, tablets…
  - Notebooks
  - Documents

CYBER WARDEN
PRACTICAL CYBER RISK MANAGEMENT

Don't over-share

- Don't share travel details on social media. Wait until you get back.
- Don't share photos from inside the office.
  - A lot can be gained from an innocent office photo
    - Screens
    - Documents
    - Security cameras
    - Whiteboards/flipcharts
    - Post-it notes

CYBER WARDEN
PRACTICAL CYBER RISK MANAGEMENT

Loose Lips Sink Ships

- Don't have confidential discussions in public, including on the phone
  - You're not a Kardashian. NEVER use the speaker on the phone in public.
- Don't view/edit anything confidential in public
  - Planes, Airports, Coffee shops…
  - Privacy filters are security theatre and are susceptible to shoulder surfing
- Beware of cameras
  - Phones, CCTV…

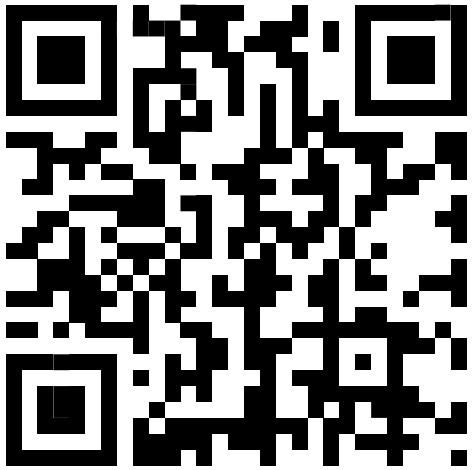
CYBER WARDEN
PRACTICAL CYBER RISK MANAGEMENT

Summary

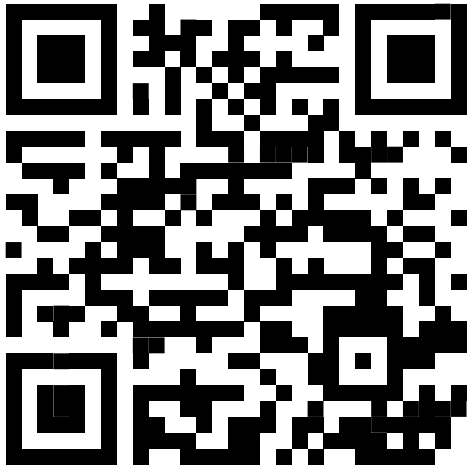
You're not paranoid if they're really out to get you

CYBER WARDEN
PRACTICAL CYBER RISK MANAGEMENT

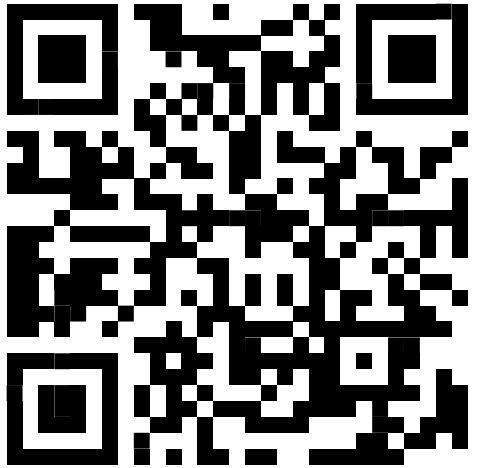
Contact Details



Andrew's LinkedIn



Cyber Warden LinkedIn



Andrew's Contact

CYBER WARDEN
PRACTICAL CYBER RISK MANAGEMENT

Download a copy of these slides