Cybersecurity Maintenance Checklist

Whittier Trust

In today's interconnected world, protecting your digital information is vital. Cyber threats are constantly evolving, so staying informed and proactive is the best defense. Whittier Trust takes cybersecurity seriously, and we aim to help you maintain your online security and safeguard your sensitive information. Here is a detailed checklist to help keep you protected from digital and online threats.

One-Time Setup

☐ **Password Security Foundation**

- Install and configure a reputable password manager
- Enable Multi-Factor Authentication (MFA/2FA) on all accounts that support it
- Create strong, unique passwords (12-16+ characters with uppercase, lowercase, numbers, symbols) for all existing accounts using your password manager

☐ **Device Security Setup**

- Enable automatic updates for your operating system (Windows, macOS, Linux)
- Enable automatic updates for all software applications (browsers, office suites, antivirus)
- Install reputable antivirus/anti-malware software
- Enable your operating system's firewall (or install dedicated firewall solution)
- Set up a VPN service for secure public Wi-Fi use

☐ **Router Security (Initial Setup)**

- Change default router administrator username and password
- Enable WPA2 or WPA3 Wi-Fi encryption (avoid WEP)
- Set up a guest Wi-Fi network for visitors
- Change default Wi-Fi network name and password

Monthly Tasks

☐ **Software Maintenance**

- Check for and install any pending software updates (if not set to automatic)
- Run full antivirus/anti-malware scan on all devices
- Review and update passwords for any accounts you use frequently

☐ **Device Firmware Updates**

- Check manufacturer websites for firmware updates for:
  - Printers
  - Smart TVs
  - Network-attached storage (NAS) devices
  - Other smart home devices
- Install firmware updates promptly when available

Quarterly Tasks (Every 3 Months)

☐ **Password Rotation**

- Change passwords for critical accounts (banking, primary email, work accounts)
- Review password manager for any duplicate or weak passwords
- Update security questions and recovery information for important accounts

☐ **Security Review**

- Review router firmware for updates and install if available
- Check router security settings and ensure they're still properly configured
- Review list of installed software and remove any unused programs
- Check for and remove any suspicious or unknown applications

Yearly Tasks

☐ **Comprehensive Security Audit**

- Change ALL passwords (or at least those not changed quarterly)
- Review and update all Multi-Factor Authentication settings
- Perform comprehensive security review of all devices and accounts
- Update contact information for account recovery across all services
- Review privacy settings on all social media and online accounts

☐ **Hardware and Software Review**

- Evaluate antivirus/security software performance and consider alternatives
- Review VPN service effectiveness and pricing
- Consider upgrading router firmware or hardware if significantly outdated
- Backup important data and test restore procedures

Daily Habits (Best Practices)

☐ **Public Wi-Fi Safety**

- Avoid accessing banking, shopping, or sensitive accounts on public Wi-Fi
- Avoid connecting to Wi-Fi networks without passwords
- Use your cell phone hotspot instead of public Wi-Fi when possible
- Use VPN when connecting to any public Wi-Fi network

☐ **Website Security Awareness**

- Don't ignore browser warnings about invalid security certificates
- Only enter sensitive information on HTTPS-secured websites
- Download software and files only from official, reputable websites
- Avoid third-party download sites that may bundle malicious programs

☐ **Safe Browsing Vigilance**

- Double-check any unexpected login prompts before entering credentials
- Verify links before clicking, especially in emails and messages
- Type web addresses manually for sensitive sites (banking, shopping)
- Check for URL misspellings and verify each character in web addresses

☐ **Email and Communication Security**

- Be cautious with suspicious emails and links from unknown senders
- Avoid clicking links or opening attachments from unfamiliar sources
- Don't scan QR codes from unexpected or unfamiliar sources
- Verify legitimacy of communications that appear to be from known contacts but seem suspicious

Emergency Response

If You Suspect a Security Breach

- Immediately change passwords for potentially compromised accounts
- Run full antivirus scan on affected devices
- Check account activity for unauthorized access
- Contact financial institutions if banking information may be compromised
- Consider temporarily freezing credit reports
- Document the incident for potential reporting to authorities

---

Remember: Cybersecurity is an ongoing process, not a one-time task. Consistency with these practices will significantly improve your digital security posture.

Need more help? Whittier Trust advisors are available to assist you and, if needed, connect you with the appropriate resources. We're always here for you.