CYBERSECURITY ADVISORY

13 March 2020

Teleworking Quick Reference Guide

Teleworking requires additional network security and user considerations. This document highlights some of the security concerns and best practices end-users and network administrators should consider when implementing a teleworking program.

Guidance for Teleworkers

1. Phishing Scams

Scammers are targeting consumers using phishing sites, phony websites, and even telephone based scams. The latest scam centers on Coronavirus (Covid-19) scams concerning supposed reporting sites, health care advisories and public emergency measures.

- Be cautious and always validate the credibility of any phone call, website, and email to make sure it's legitimate. Report any suspicious activity to your Information Security Office.

2. Personal Computer Protection

Below are some of the actions a user can take to increase the level of protection from malicious activity or harm.

- System and Software Updates
    - Ensure the automatic system update feature for your specific Operating System is turned on.
        - For Windows users, go to the **Start** button, then **Settings->Update & Security-> Windows Update, and select "Automatic Updates"**
    - Enable other application software, such as browsers and Office software to automatically update
    - For Windows users, only use Windows 10 or other supported Operating Systems (Windows 7 is end-of-life)

- For Local Computer Passwords:
    - Don't use the same password for all of your accounts
    - Use Password Managers, such as LastPass, to help store and manage multiple accounts securely.
    - Use complex passwords and PINs: At least 10 characters with upper and lower case letters, numbers, special characters
    - Avoid common dictionary words
    - Change passwords periodically
- Anti-Malware:
    - Validate you are running anti-malware/anti-virus and update your virus definitions directly from the manufacturers site. Sync.com offers helpful guidance for Windows 10 users on how to determine what anti-malware/anti-virus software is on your computer.
    - Microsoft Defender Anti-malware is available on Windows 10 computers and tablets.
    - For MAC/OSX users, Mashtips offers helpful guidance for Apple product users on how to determine what anti-malware/anti-virus software is on your computer.
    - Many internet service providers e.g, AT&T and XFinity include security software as part of their service.
- Network Security:
    - Enable domain name filtering to protect against phishing and malicious websites with OpenDNS.

3. Office Productivity Tools

There are multiple ways users can access their work and personal information from home or while away from the office.

- Users can run Microsoft Office applications (Outlook email, Word, Excel, etc.) from the Microsoft Office Portal.
- Users can activate an Office 365 is a subscription service that allows users to install on five different work or personal computers (Windows/Mac), five phones and five tablets.
- A wide array of helpful collaboration tools e.g., Teams, SharePoint, and OneDrive are all available on the Office portal.
- Microsoft has established training resources for Microsoft Office applications.

4. Mobile Phone Protection

Your phone is a valuable personal computing asset that also requires addition security considerations by users.

- Mobile Tools - Free tools for home users to protect their iOS and Mobile devices at Trend Micro.
- Users should regularly clean up Privacy Settings on Mobile Devices:
    - Apple's web site provides privacy guidance for iOS.
    - Google's web site provides privacy settings for Android devices.

5. Physical and Data Protection Best Practices users should consider:

- Never work at public places such as coffee shop, etc.
- Never connect to public or untrusted/insecure WiFi connection (at a minimum, use WPA2-PSK with a strong passphrase, or use WPA3-Personal)
- Never disclose confidential or sensitive data to any unauthorized personnel including friends and family.
- Always lock your computer when leaving it unattended.
- Do not store sensitive or confidential information on your personal computer.
- Store any sensitive or confidential information on encrypted media provided by your department.
- Ensure confidential paper documents are properly disposed of, i.e. shredding
- Report security incidents or security concerns to you supervisor immediately.
- Refrain from using personal email for business use.
- Always comply with your organizations policies and procedures to protect specific high risk data elements regulated by HIPAA, IRS, PCI, etc.

6. Additional Resources Available as Alternatives

- Consumer Reports offers information on anti-malware products:
  Note: Use of Kaspersky products is not recommended for personal use.
- WebEx offers a remote work and collaboration product.

Guidance for Information Technology Departments

1. Remote Access Suggestions for Critical Business Services

- Inventory all IT critical services that need to be accessed remotely
- Identify the best way to access each of the critical services
    - Intranet web applications – Securely expose intranet web applications externally, Virtual Desktop Infrastructure (VDI) or Virtual Private Network (VPN) access
    - Rich client applications - VDI or VPN access
    - Internet applications
        - Office365
        - Collaboration tools (Teams, Webex, Zoom)
        - Business applications
    - Business services requiring public interaction
        - Call Centers

        - Field Offices
- Look at re-platforming or relocating critical services to cloud, if current environment is too limited. For example: Many departments have productivity files and home directories on premises. If access to file shares is a need for telework, consider use of Microsoft's OneDrive, SharePoint, or Teams for departments using Office 365.
    - VDI/Desktop as a Service (DaaS) options
        - Amazon Web Services
        - Microsoft Azure
        - VMware
        - Citrix
    - Network considerations
        - Calculate Wide Area Network (WAN) bandwidth requirements
        - Intrusion Prevention System (IPS) capacities
        - Firewall rule

2. Microsoft Office 365 Information and Products to Support Telework

- Office 365 is a subscription service that allows users to install on five different work or personal computers (Windows/Mac), five phones and five tablets.
- Microsoft Defender Anti-malware is available for Windows 10.
- Enterprise Mobility & Security: makes Office 365 more mobile and secure.
  Azure Active Directory Premium: identity management
    - Enable Conditional Access
    - Azure Active Directory Risk
    - What is Application Proxy
    - Publishing internal apps with App Proxy
    - Azure Identity Protection
    - Multi-Factor Authentication Overview
    - Multi-Factor Authentication Support versions

a) Intune - Device management
    - Enrolling devices
    - iOS capabilities supported by Intune
    - All iOS features available in Supervised mode
    - Managing mobile devices with Intune
    - Role based Access for Intune
    - Application Protection Policies
    - Setting Device Compliance Policies
    - Compliance Settings for Windows
    - Compliance Settings for MAC

b) Azure Information Protection - Data Protection

- What is Azure Information Protection (AIP)?
- What files are supported?
- Using On-Premise AIP Scanner Utility

The Cal-CSIC recommends end-users and network administrators review these best practices in establishing their teleworking environment.

California Cyber Security Integration Center (Cal-CSIC)

Codified in Government Code Section 8586.5, the California Cyber Security Integration Center (Cal-CSIC) is a multi-agency center coordinating cybersecurity competencies and resources from across government and leads California's cybersecurity preparation, mitigation, and response efforts.

If you need further information about this issue contact the Cal-CSIC at our email address CalCSIC@caloes.ca.gov or by telephone at (833) REPORT-1.