



FREE OR DISCOUNTED TECHNOLOGY TOOLS FOR A SMALL BUSINESS

1) Productivity Tools (Email, Collaboration, Conferencing, etc.)

- a) Cisco WebEx will be available at no cost, for 90 days
 - i) For IT Teams: <https://www.webex.com/webexcovid19.html>
 - ii) For end users: <https://www.webex.com/webexremotework.html>
- b) Google My Business: allows small businesses to create a Business Profile and Website for free. Use this link to access website [Google My Business](#)
- c) Microsoft Office 365 (email, instant messaging, etc) offers a 6-month free trial version, available for small businesses. <https://docs.microsoft.com/en-us/microsoftteams/e1-trial-license>
- d) Zoom Business is available for a free 60-day trial to small businesses. For more product information, use <https://zoom.us/pricing>. If interested, contact john.mensik@zoom.us or Katie.williamson@zoom.us.
- e) TransparentBusiness, the platform designated by Citigroup as the Top People Management Solution, offers licenses free of charge (for up to \$1m dollars) for California small business. This platform ([click here](#)) makes all computer-based work easy to monitor and coordinate, while protecting a worker's privacy.

2) Internet Access

- a) AT&T, Century Link, Charter, Comcast, Cox, Frontier, Sprint, T-Mobile, US Cellular, Verizon and many other companies are providing the following services for 60 days:
 - i) Not terminate service to any residential or small business customers
 - ii) Waive any late fees for any residential or small business customers
 - iii) Open its Wi-Fi hotspots to any American who needs them

3) Anti-Malware Resources (at no cost for 6 months):

- a) CrowdStrike: <https://go.crowdstrike.com/WF-Request-Info-Remote-Workers.html>
- b) Trend Micro Maximum Security: <https://resources.trendmicro.com/Work-From-Home-Assistance-Program.html>

Please see Pages 2-3 for Teleworking Tips and Additional Resources

Any reference to a specific product, process or service or to the use of any vendor is for the information and convenience of the small business community and does not constitute or imply an endorsement by the California Department of Technology (CDT), GO-Biz, or the state of California.



TELEWORKING TIPS AND ADDITIONAL RESOURCES FOR BUSINESSES

4) Caution on Coronavirus Phishing and Scams

- a) Scammers are targeting consumers using phishing sites, phony websites, and even telephone-based scams. Be cautious and always validate the credibility of any phone call, website, and email to make sure it is legitimate. Report any suspicious activity to your Information Security Office.
- b) For more information see: <http://www.oesnews.com/california-cyber-security-integration-center-offers-guidance-for-teleworkers/>

5) Personal Computer Protection

- a) System and Software Updates
 - i) 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"
 - ii) Enable other application software, such as browsers and Office software to automatically update
 - iii) For Windows users, only use Windows 10 or other supported Operating Systems (Windows 7 is end-of-life)
- b) For Local Computer Passwords: Use complex passwords and PINs: At least 10 characters with upper and lower case letters, numbers, special characters
 - i) Avoid common dictionary words
 - ii) Change passwords periodically
 - iii) Don't use the same password for all of your accounts
 - (1) Using Password Managers helps store and manage multiple accounts securely, for example: <https://www.lastpass.com/password-manager>
- c) Anti-Malware:
 - i) Validate you are running anti-malware/anti-virus.
 - (1) Microsoft Defender Anti-malware is available on Windows 10 computers and tablets.
 - (2) MAC/OSX: Useful tips to validate anti-malware (XProtect) protection and other built-in security features are turned on: <https://mashtips.com/built-in-mac-security-software/>

Any reference to a specific product, process or service or to the use of any vendor is for the information and convenience of the small business community and does not constitute or imply an endorsement by the California Department of Technology (CDT), GO-Biz, or the state of California.



Office of the Small Business Advocate
Governor's Office of Business and Economic Development (GO-Biz)

- ii) Free Options for anti-malware / anti-phishing / and network security solutions (for 6 months):
 - (1) Trend Micro Maximum Security:
<https://resources.trendmicro.com/Work-From-Home-Assistance-Program.html>. Sign up using your State email account and optionally install it on your personal computer, smartphone, or tablet.
 - (2) CrowdStrike: <https://go.crowdstrike.com/WF-Request-Info-Remote-Workers.html>
 - (3) Most Internet Service Providers (ISP) provide free anti-malware/anti-virus products. Contact your ISP to check for availability.

6) Personal Phone Protection

- a) Free tools to protect your iOS and Mobile devices:
https://www.trendmicro.com/en_us/forHome/products/free-tools.html
- b) Regularly Clean up Privacy Settings on Mobile Devices:
 - i) For iOS: <https://apps.apple.com/us/app/mypermissions-privacy-cleaner/id535720736>
 - ii) For Android:
https://play.google.com/store/apps/details?id=com.mypermissions.mypermissions&hl=en_US

7) Physical and Data Protection Best Practices

- a) It is highly recommended to not connect to public or untrusted/insecure WiFi connection. However, if you need to use public WiFi, use extreme caution because of malicious and spoofed WiFi hotspots. Here are a few tips:
 - i) Only visit websites that are encrypted for business and sensitive personal use. This can be identified by looking at the browser address bar to see if the website address starts with HTTPS://
 - ii) Never ignore browser SSL/TLS certification warning when you access a website.
- b) Never disclose confidential or sensitive data to any unauthorized personnel including friends and family.
- c) Always lock your computer when leaving it unattended.
- d) Do not store sensitive or confidential information on your personal computer.
- e) Ensure confidential paper documents are properly disposed of, i.e. shredding
- f) Always comply with your organizations policies and procedures to protect specific high risk data elements regulated by HIPAA, IRS, PCI, etc.

Any reference to a specific product, process or service or to the use of any vendor is for the information and convenience of the small business community and does not constitute or imply an endorsement by the California Department of Technology (CDT), GO-Biz, or the state of California.