



Small businesses are quickly deploying various technologies to better serve their customers and manage their business more efficiently. Different kinds of technologies, however, come with a variety of risks and, thus, require alternative strategies to protect them. This "Quick Wins" sheet can be used as a starting point as a content outline for your own security awareness training program.



QUICK WINS FOR COPIER/PRINTER/FAX SECURITY.

DIGITAL COPIERS/PRINTERS/FAX MACHINES ARE COMPUTERS TOO.

- ✓ Ensure devices have encryption and overwriting
- ✓ Take advantage of all the security features offered
- ✓ Secure/wipe the hard drive before disposing of an old device
- ✓ Change the default password to a strong and unique passphrase
- ✓ Learn More: <https://www.ftc.gov/tips-advice/business-center/guidance/digital-copier-data-security-guide-businesses>



QUICK WINS FOR EMAIL SECURITY.

WHEN IN DOUBT, THROW IT OUT.

BE EXTRA CAUTIOUS WHEN IT COMES TO EMAIL.

- ✓ Require strong, unique passphrases on email accounts
- ✓ Turn on two-factor authentication
- ✓ Do not use personal email accounts for company business
- ✓ Employees should know not to open suspicious links in email, tweets, posts, online ads, messages or attachments – even if they know the source. Employees should also be instructed about your company's spam filters and how to use them to prevent unwanted, harmful email
- ✓ Learn More: <https://www.ic3.gov/media/2017/170504.aspx>



QUICK WINS FOR FILE SHARING.

SHARING IS CARING, ONLY WHEN DONE SECURELY.

- ✓ Restrict the locations to which work files containing sensitive information can be saved or copied
- ✓ If possible, use application-level encryption to protect the information in your files
- ✓ Use file-naming conventions that don't disclose the types of information a file contains
- ✓ Monitor networks for sensitive information, either directly or by using a third-party service provider
- ✓ Free services do not provide the legal protection appropriate for securing sensitive information
- ✓ Learn More: <https://www.ftc.gov/tips-advice/business-center/guidance/peer-peer-file-sharing-guide-business>



QUICK WINS FOR MOBILE DEVICES.

KEEP A CLEAN MACHINE FOR ON-THE-GO DEVICES.

- ✓ Update security software regularly. Go ahead, update your mobile software now.
- ✓ Delete unneeded apps and update existing apps regularly
- ✓ Always download apps from a trusted source and check reviews prior to downloading
- ✓ Secure devices with passcodes or other strong authentication, such as fingerprint recognition
- ✓ Turn off Discovery Mode
- ✓ Activate "find device" and "remote wipe"
- ✓ Configure app permissions immediately after downloading
- ✓ Learn More: <https://www.stopthinkconnect.org/resources/preview/tip-sheet-stay-cyberaware-while-on-the-go-safety-tips-for-mobile-devices>



QUICK WINS FOR POINT OF SALE SYSTEMS.

HACKERS ARE OFTEN FINANCIALLY MOTIVATED.

DON'T MAKE IT AN EASY PAYDAY.

- ✓ Create unique, strong passphrases
- ✓ Separate user and administrative accounts
- ✓ Keep a clean machine: Update software regularly
- ✓ Avoid web browsing on POS terminals
- ✓ Use antivirus protection
- ✓ Learn More: <https://www.pcisecuritystandards.org/merchants/>



QUICK WINS FOR ROUTERS.

YOUR HOME OR BUSINESS NETWORK IS NOT TOO SMALL TO BE HACKED.

- ✓ Change from manufacturer's default admin password to a unique, strong passphrase
- ✓ Use a network monitoring app to scan for unwanted users
- ✓ Restrict remote administrative management
- ✓ Log out after configuring
- ✓ Keep firmware updated
- ✓ Learn More: <https://www.us-cert.gov/ncas/tips/ST15-002>



QUICK WINS FOR SOCIAL NETWORKS.

SOCIALIZE ONLINE WITH SECURITY IN MIND.

- ✓ Limit who has administrative access to your social media accounts
- ✓ Set up 2-factor authentication
- ✓ Configure your privacy settings to strengthen security and limit the amount of data shared. At the very least, review these settings annually
- ✓ Avoid third-party applications that seem suspicious and modify your settings to limit the amount of information the applications can access. Make sure you're accessing your social media accounts on a current, updated web browser
- ✓ Learn More: <https://www.us-cert.gov/ncas/tips/ST06-003>



QUICK WINS FOR SOFTWARE.

HAVING THE LATEST SECURITY SOFTWARE, WEB BROWSER AND OPERATING SYSTEM ARE THE BEST DEFENSE AGAINST THREATS.

- ✓ Make sure your computer operating system, browser, and applications are set to receive automatic updates
- ✓ Ensure all software is up to date. Get rid of software you don't use
- ✓ Your company should have clear, concise rules for what employees can install and keep on their work computers
- ✓ When installing software, pay close attention to the message boxes before clicking OK, Next or I Agree
- ✓ Make sure all of your organization's computers are equipped with antivirus software and antispyware. This software should be updated regularly
- ✓ Limit access to data or systems only to those who require it to perform the core duties of their jobs
- ✓ Learn More: <https://www.lockdownyourlogin.org/update-software/>



QUICK WINS FOR THIRD PARTY VENDORS.

DO YOUR DUE DILIGENCE.
GET IT IN WRITING AND MONITOR COMPLIANCE.

- ✓ Spell out your privacy and security expectations in clear, user-friendly language to service providers
- ✓ Understand how their services work and to what you are giving them access
- ✓ Build in procedures to monitor what service providers are doing on your behalf
- ✓ Review your privacy promises from the perspective of a potential service provider
- ✓ Spell out expectations and scope of work in a formal agreement/contract
- ✓ Learn More: <https://www.ftc.gov/news-events/blogs/business-blog/2018/04/lesson-blumake-right-privacy-security-calls-when-working>



QUICK WINS FOR USB DRIVES.

THESE SMALL DEVICES CAN EASILY CREATE HUGE SECURITY ISSUES.

- ✓ Scan USBs and other external devices for viruses and malware
- ✓ Disable auto-run, which allows USB drives to open automatically when they are inserted into a drive
- ✓ Only pre-approved USB drives should be allowed in company devices. Establish policies about the use of personal, unapproved devices being plugged into work devices
- ✓ Keep personal and business USB drives separate
- ✓ Don't keep sensitive information on unencrypted USB drives. It is a good practice to keep sensitive information off of USB drives altogether
- ✓ Learn More: <https://www.us-cert.gov/ncas/tips/ST08-001>



QUICK WINS FOR WEBSITE SECURITY.

CREATE A SAFE ONLINE SHOPPING EXPERIENCE FOR YOUR CUSTOMERS.

- ✓ Keep software up-to-date
- ✓ Require users to create unique, strong passphrases to access
- ✓ Prevent direct access to upload files to your site
- ✓ Use scan tools to test your site's security - many are available free of charge
- ✓ Register sites with similar spelling to yours
- ✓ Learn More: <https://www.ftc.gov/news-events/blogs/business-blog/2018/02/hiring-web-host-ftc-has-security-tips-small-businesses>



QUICK WINS FOR WI-FI SECURITY.

THINK BEFORE YOU CONNECT.

- ✓ Use separate Wi-Fi for guests or customers than you do for business
- ✓ Physically secure Wi-Fi equipment
- ✓ Use a virtual private network (VPN) when using public Wi-Fi
- ✓ Do not connect to unknown, generic or suspicious Wi-Fi networks. Use your mobile carrier's data plan to connect instead
- ✓ Turn off Wi-Fi and Bluetooth when not in use on your devices
- ✓ Secure your internet connection by using a firewall, encrypt information and hide your Wi-Fi network
- ✓ Learn More: <https://www.consumer.ftc.gov/articles/0014-tips-using-public-wi-fi-networks>



CyberSecurity4biz.com

can your business survive without its data?

Put these Resources into Action!

FREE CONTENT YOU CAN USE TO DESIGN YOUR OWN CYBERSECURITY AWARENESS PROGRAM

- Tips, posters and videos for kids, home, business and mobile:
 - o www.staysafeonline.org
 - o www.onguardonline.gov
- Federal Trade Commission's cybersecurity awareness publications bulk order site:
 - o www.bulkorder.ftc.gov
- Federal Inter-Agency Ransomware Guidance: How To Protect Your Networks from Ransomware:
 - o <https://www.justice.gov/criminal-ccips/file/872771/download>
- Capture the Flag:
 - o <https://github.com/facebook/fbctf>

STAY UP TO DATE ON THE LATEST SCAMS BY SIGNING UP FOR THESE ALERTS

- Federal Trade Commission Scam Alerts:
 - o www.consumer.ftc.gov/scam-alerts
- Better Business Bureau Scam Alerts:
 - o www.bbb.org/council

TEACH EMPLOYEES ABOUT STRONG AUTHENTICATION

- Lock Down Your Login's 6 simple steps to improve your online security:
 - o www.lockdownyourlogin.org
- Telesign's step-by-step instructions for enabling 2-factor authentication:
 - o www.turnon2FA.com

OTHER HELPFUL ONLINE SAFETY CONTENT

- National Cyber Security Alliance's CyberSecure My Business online resources and videos:
 - o <https://staysafeonline.org/cybersecure-business/>
- National Association of State Chief Information Officers' national map linking to each state's cybersecurity awareness website:
 - o <https://www.nascio.org/Advocacy/Cybersecurity>
- Small Business Big Threat:
 - o www.smallbusinessbigthreat.com