Defense in Depth is a security concept in which multiple layers of security controls (defense) are placed throughout an information technology (IT) system. While most people probably are not familiar with the technical language below, you can share this information with your IT department to ensure your business and your employees are protected against cyber threats. On the back of this page, you'll find information to assess how secure your company is in its banking practices.

Applicable Technical Controls

- Enhance the strength of your email or network authentication methods by using security tokens or even text messages as a 2nd authentication. Master password keeper tools like LastPass are also good and may offer the ability to automatically submit login information to popular websites.
- Limit what your employees can access from their computer workstations – do company computers allow unrestricted access to the internet? Consider centralizing software downloads within your IT groups. Online Services can provide valuable information about suspicious files and websites, for example: ***virustotal.com***.
- Ensure IT has configured email filters to restrict high-risk file types for executing malware (EXE, ZIP, SCR, etc.). Also, since modern malware is often disguised as a word document, pdf, or excel spreadsheet, consider a file sharing service to share documents instead of email messages. Backup valuable data offline; safe deposit boxes are an inexpensive way to store backups.
- Check with your IT resource to ensure Antivirus is regularly updated and enable optional features like "heuristics", "file reputation", "host intrusion prevention", "firewalls", and "application whitelisting".
- Talk to your IT resource about evaluating the "attack surface" of your network and "hardening" systems and computers, tablets and cell phones wherever possible. Also consider vulnerability scans of your network if it makes sense for your company.
- Install operating system updates and apply third party security patches quickly.
- Consider whether to assign employees to monitor web traffic, especially visits to newly registered sites and those without an established reputation, for example; "uncategorized" or "unrated" websites.
- Avoid using free web-based personal e-mail to do company business. Consider registering a domain and establish protected company e-mail accounts.
- If you use your own domain for email make sure to configure "anti-spoofing" mechanisms. Check out Microsoft's "Best Practices Guide for Configuring EOP" at ***technet.microsoft.com/en-us/library/jj723164***.
- If you host your own website make sure your IT person is regularly updating your Windows or other operating systems, as well as any third party software. Services like Qualys (***qualys.com***), Sucuri (***sucuri.net***), or StopTheHacker (***stopthehacker.com***) can automatically scan and alert if your site is compromised. Keep content management software (WordPress, Joomla, etc.) up-to-date. Many popular hosting services offer scanning as an add-on service.

Banking Self-Assessment

Security alone is not enough. Education is the key to prevention. Consider holding a staff meeting and using these questions to evaluate how prepared your company is to defend against potential payments fraud.

- If your employees regularly shop online for company supplies and materials, do you use a standalone computer not regularly used for banking or other transactional activities?
- Do you know where to go for cyber security help? Visit the Department of Homeland Security's business resource page for tips for your business at ***dhs.gov/publication/stopthinkconnect-small-business-resources***.
- Do you have a cyber plan? Consider using the FCC's free cyber planning tool at ***fcc.gov/cyberplanner*** so that your business is prepared in the event of an incident.
- Does your security awareness training include the following points?
  - ☐ Be on the alert for suspicious emails, and avoid logging into accounts from links in emails if you aren't certain it is legitimate. Read here why you can trust emails sent from the montecito.bank domain: montecito.bank/dotbank
  - ☐ Watch for changes in the performance of your computer: dramatic loss of speed, computer locks up, unexpected rebooting, unusual popups, etc.
  - ☐ How and to whom to report suspicious activity in your company & your bank.
    Contact your banker if you:
    - Suspect a fraudulent transaction.
    - If you are trying to process an Online Wire or ACH through online banking & you receive a "maintenance" page.
    - If you receive a suspicious email claiming to be from Montecito Bank & Trust and it is requesting username and/or password.
  - ☐ Be cautious about what is posted to social media and company websites to protect against social engineering attempts.
  - ☐ Be suspicious of phone or email requests for secrecy or pressure to take action quickly, or changes to vendor information.
  - ☐ Surf the Internet carefully, and avoid public Internet access points (i.e. libraries, coffee shops, etc.) for doing business computing to avoid eavesdropping by crooks. Use search engines to find legitimate sites rather than typing URL's to avoid mistyping an alternative site.
- Do you reconcile your accounts daily to watch for fraudulent transactions?
- Do you have an escalation process for wire requests in your company when adding new wire recipients or changing an existing vendor/recipient's bank account information?
- Do you employ the use of two-factor authentication, such as having a secondary sign-off for wire requests via PIN, text message, or phone call to a pre-established phone number?