Cyber Security Basics - How to Protect your Business

1. Secure your business's computer network and your data.
    a. Prohibit access to web-based personal email on your network
    b. Prohibit the use of removable devices like flash drives
    c. Prohibit access to personal Social Media sites on your network
    d. Create a Whitelist of trusted web sites used in your business
    e. Encrypt your email or use a Secure Portal to exchange sensitive data and documents.

2. Protect email with filtering tools and employee phishing training.
    a. Leverage all available email filtering tools for filtering malicious emails from reaching user inboxes.
    b. Regularly educate and train your employees to spot and immediately report phishing emails and not to open or click on links within suspicious emails.

3. Manage vulnerabilities and patch regularly.
    a. Keep all systems on the latest, fully support operating system(s)
    b. maintain up-to-date anti-virus/anti-malware programs on computing systems, with signatures updated on a regular basis.
    c. Regularly scan all systems and computing devices (desktops, laptops, phones, tablets, servers, network devices, printers, etc.) for vulnerabilities and patch them appropriately.
    d. Scan applications vulnerabilities and remediate timely and appropriately.
    e. Don't forget your mobile devices!

4. Use Multi-Factor Authentication ("MFA") to protect user accounts. MFA can keep hackers out of your network and limit in-network movement.
    a. Enable Multi-Factor Authentication for email
    b. Enable Multi-Factor Authentication for systems that have sensitive information
    c. Enable Multi-Factor Authentication for users that have administrative or privileged access to systems
    d. Enable Multi-Factor Authentication for systems that are remote access to the network and all externally exposed systems

5. Manage passwords.
    a. Use strong passwords for all systems and user accounts.
    b. Require passwords of at least 16 characters for all privileged user accounts, and prohibit commonly used passwords.
    c. Avoid use of shared credentials for system or application access. Each user should have their own log-in credentials and should never share them with each other.
    d. Terminate computer access and disable credentials for employees that leave the company immediately.

6. Encrypt sensitive and Customer Information data at rest and in use.

7. Disable Remote Desktop Protocol access to your network from the internet.

8. Manage privileged access.
    a. Implement the principle of least privileged access - your employees should only be able to access the applications and systems needed to fulfill their job roles.
    b. Maintain a list of all privileged accounts and regularly review to confirm privileged access is still needed.

9. Monitor and respond to changes in your network.
    a. Monitor your network for intruders and respond to alerts of suspicious activity.

10. Develop a Business Continuity Plan.
    a. Create and maintain a business continuity plan that addresses business resilience and recovery from cyber-attacks and other threats.
    b. Regularly test the plan.

11. Maintain, test and segregate backups.
    a. Maintain comprehensive, segregated backups of your systems and data that will allow for recovery in the event of a ransomware attack.
    b. Test backups on a regular basis.

12. Create an Incident Response Plan.
    a. Prepare an incident response plan that addresses ransomware attacks in addition to other potential incidents. Practice and update this plan regularly.
    b. Have a crisis communications plan, along with contact information for key contacts, to respond quickly to a data breach or other security incident.

13. Secure your remote workers.
    a. Require employees to use separate work and personal devices.
    b. Remind remote employees to change their router login and password from the default settings.
    c. Prohibit use of personal email and personal devices to conduct business.
    d. Require remote employees to use the same physical and technical security practices used at the office.
    e. Remote employees should save and back up data frequently.

14. Protect against ransomware.
    a. Make sure computer networks are patched and up to date
    b. Backup your entire network; keep the back-ups up to date, offsite and tested!
    c. Immediately change default passwords.
    d. Segment your network to stop or slow the spread of ransomware.
    e. Use Multi-Factor authentication to protect your network from attackers.

f. Train staff on protecting the business. Everyone should understand their responsibilities when it comes to Data Security. Create an ongoing and repetitive Training Program for new employees and existing employees.
g. Know what's attached to your network. Any connection – including IoT devices - is a potential entryway to your network for attackers.
h. Check antivirus and firewalls.
i. Have a plan in place to respond to a ransomware attack.

15. Consult available cyber resources like FTC's Cybersecurity for Small Business (ftc.gov) and consider vendor resources to bolster your security.
    a. CertifID Wire Fraud Prevention and Recovery https://www.certifid.com/
    b. ClosingLock Real Estate Wire Fraud Prevention https://www.closinglock.com/
    c. Infrascale Backups https://www.infrascale.com/
    d. KnowBe4 security awareness training https://www.knowbe4.com/
    e. Email encryption https://zix.com/
    f. Premier One secure hosting https://premier-one.com/
    g. NY Dept of Financial Services (Not NY specific) https://www.dfs.ny.gov/consumers/small_businesses

Glossary of Terms:

Whitelist of trusted web sites - Whitelisting websites allows you to control internet access based on groups of users or computers to only a specific set of web sites that you deem necessary for your business. It also allows you to whitelist websites for some users without allowing them for all users.

Externally exposed systems – Any systems that are exposed to the outside world via the Internet.

Data at rest - Data that is housed physically on a computer, server or in the Cloud. Computer data storage in any digital form.

Strong Passwords - A password that is hard to detect both by humans and by the computer. Two things make a password stronger: (1) a larger number of characters, and (2) mixing numeric digits, upper - lower-case letters and special characters ($, #, etc.).

Remote Desktop Protocol - The Remote Desktop Protocol (RDP) makes it possible for employees to connect to their work desktop computer when they work remotely.

Business Continuity Plan - Business continuity is the capability of an organization to continue the delivery of products or services at pre-defined acceptable levels following a disruptive incident", and business continuity planning is the process of creating systems of prevention and recovery to deal with potential threats to a company.

Incidence Response Plan - An incident response plan is a set of instructions to help IT staff detect, respond to, and recover from network security incidents. These types of plans address issues like cybercrime, data loss, and service outages that threaten daily work.