TECH SOURCE

February 2019

Volume 4 - Security

Phone: 504-888-8324

Visit us at:
888-tech.com

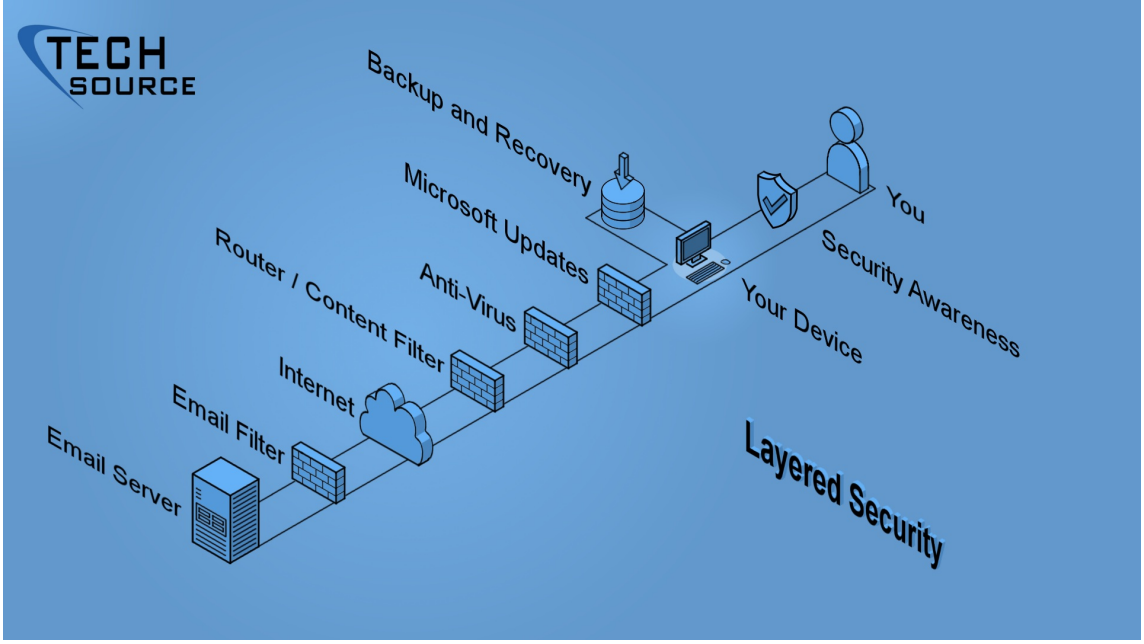
Security Assessment

Regularly assessing your security practices, training, and policies are vital for keeping up to date with constantly evolving cyber threats.

Did you know best practices recommend multiple layers of security?

Having layers of security slows down cyber attackers and gives the organization time to combat the breach.

- Do you have consistent ways to update and maintain your security infrastructure? In larger environments with ten or more devices, automation is the only way to accomplish this. If you would like to know more about how to automate your security, email us at marketing@888-tech.com.
- Do you have an internet security router with software that is updated on a regular basis, typically identified by an annual subscription cost?
- Do you have multiple software products on your devices that are updated and monitored on a regular basis? Examples include anti-virus, anti-malware, web-content filter, and temporary internet file removal.
- Does your router or service provider filter web content, have intrusion detection, or track website access?
- Do you lock your device when not in use?
- Do you have a way to train and test your team using Security Awareness Training? An untrained user could allow unwanted users to circumvent most security measures. For example, if a user opened a bogus link in their email or allowed a phone scammer to login to their computer remotely, almost all security levels would be bypassed.
- Is your Wi-Fi network secured with a password? Are you using at least WPA2-PSK encryption?
- Do your devices leave the office? If so, you should consider encrypting those devices. Contact us for further details on encryption services.



Security Awareness Training (SAT)

While our devices may be secure from direct cyber attacks, people themselves have become the new target of cyber criminals. These criminals will attempt to steal valuable information or assets from people using methods such as phishing. Keeping people aware of these methods is the core reason security awareness training has been developed. This training is intended to protect users by educating them on how to avoid making themselves vulnerable to human targeted cyber attacks.

Take the Cybersecurity Awareness Training quiz, created by the U.S. Department of Health and Human Services.

For more information on security awareness training, contact us and we will follow up with you.

Do you have policies updated and signed annually by all employees?

- Did you know payroll companies offer HR services which will incorporate your policies into an employee handbook which can require them to view and sign them each year? These policies are another mechanism you can use to educate your team and hold them accountable.
- Do you have computer use and email policies? We have these available upon request.

Security can be tied to automation

- Do you want to lower your risk and improve the productivity of your team? Automated tools can run scans and updates to identify issues more consistently.
- Do you need a high level overview showing compliance or protection?
- Do you need to wipe mobile devices? If so, contact us.

Other Security Tips

- Create backups and test them periodically to assure recovery in the event of a

ransomware attack. Use our Backup Questionnaire to assess your backup system.

- Always update windows to prevent virus or malware infection. We offer automatic windows update management.
- Change your passwords at least every nine months, and make sure they are adequately complex. Consider using a password manager to simplify this process. For tips on creating strong passwords, use our guide.

Register for Newsletter **Visit our website**