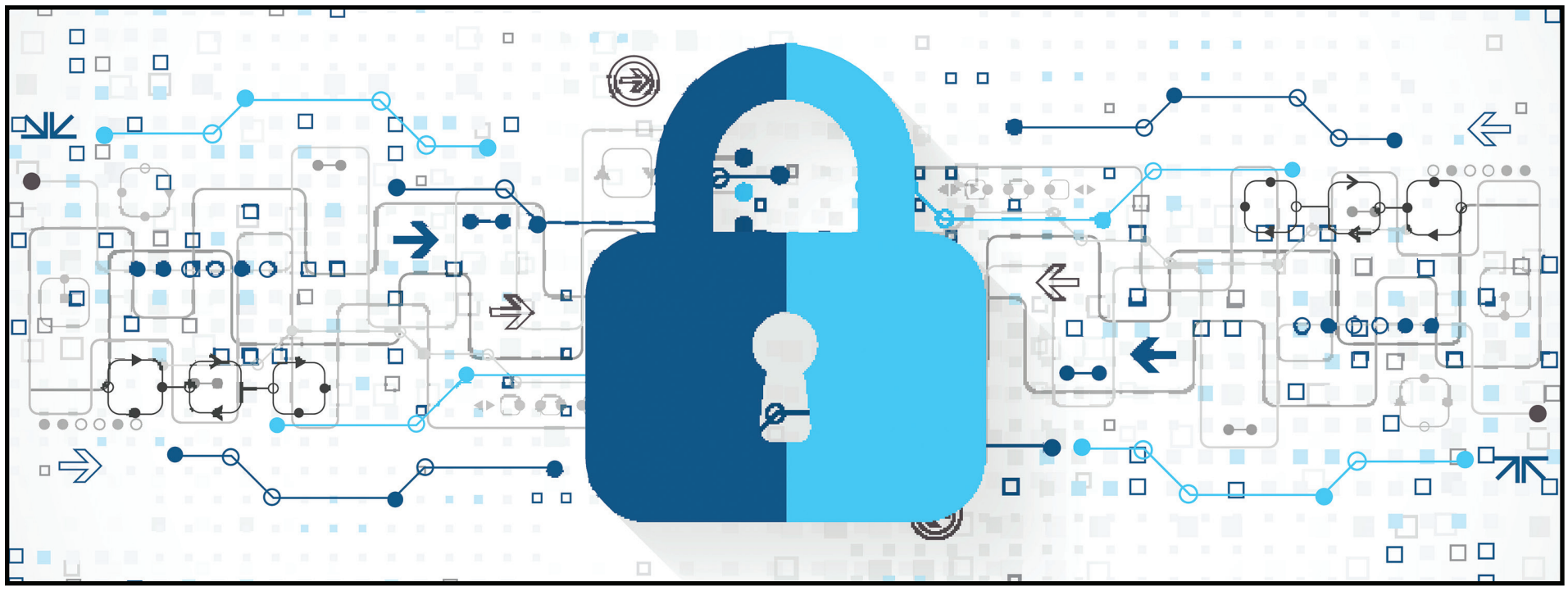

Seven cybersecurity recommendations for small businesses

BY MICHAEL KOKAL

Cybersecurity is a growing concern for businesses at all levels. The potential threats are numerous, and a successful attack can cripple or even destroy a small business.

Darrell Fortae, owner of Everlast Software, LLC. in Springfield, teaches community-based cybersecurity seminars at Lincoln Land's Capital City Training Center. Here are his seven recommendations for small businesses seeking to stay safe in the digital realm.

Focus on passwords.

Perhaps the easiest and most effective precaution you and your employees can take is to pay attention to your passwords. Regularly change them. Don't use the same password for any two accounts, and consider using a secure, offline password manager to keep track of your various passwords.

Pay special attention to selecting a password. Fortae recommends passwords that are at least ten characters in length, but for important work and financial information, he recommends passwords as long as 16 characters.

Another consideration in selecting a password is not using something which can be found in a dictionary. One of the most common decoding programs used by hackers is a "brute force" search for passwords found in the dictionary. Fortae recommends using phrases, as opposed to words, and to include a couple of special characters in the middle of the words. For example, the password "friedgreentomatoes" would not be found in a dictionary. Adding special characters ("fried77gre@en5tomatoes" or "fri!ed24green7tomatoes" makes it even harder for a hacker to decode. The longer the password, the more difficult it is for a computer algorithm to break.

Update software and patches.

Make sure that your computer and network use the latest versions of all computer software, and that all of your security patches or system upgrades are up to date. Hackers are continually finding computer software vulnerabilities, especially those based on Windows. Hackers may discover a vulnerability, - a so-called "zero-day exploit" – which is not publicly reported or announced before becoming active. That may leave software vendors with "zero days" in which to create patches or advise workarounds to prevent the exploit.

To fix the vulnerability, software vendors and developers will attempt to develop patches and upgrades, making them available as they are developed. Keeping all security patches and system updates up to date, though not perfect, provides a defense to the "zero-day" exploit.

Train your employees to recognize malware.

An untrained employee can thwart even the best computer defenses. Your business can have the most effective firewall on the market, but if employees are not trained to recognize a potential "spear-phishing" attack or malware, your network can be breached.

A phishing attack involves a malicious email sent to any random email account. However, spear-phishing is a more sophisticated means of attacking your computer because these emails are designed to look like they came from someone the recipient knows and trusts, such as a colleague, business manager, or human resources department. They can include a subject line or content that is specifically tailored to the victim's known interest or industry. If the user clicks on the malicious attachment in the email or visits a malicious website linked to the email, it may allow a criminal hacker to access that computer or the entire network.

Spear-phishing attacks are becoming more and more sophisticated. Fortae recommends training your employees with mock-simulated spear-phishing attacks to help employees recognize suspicious emails. Additionally, outside vendors may provide classroom teaching or even software that simulates phishing attacks, which can be helpful in providing "just-in-time" training messages to individuals who fail to recognize the mock attack.

Train your employees not to use public Wi-Fi networks.

Public Wi-Fi networks are inherently vulnerable to hackers. Anyone with a cheap wireless router or a device called a "Wi-Fi pineapple" can set up a Wi-Fi network. Hackers sometimes use this tactic to ensnare careless users and trick them into thinking they're connecting to legitimate access points. In order to further conceal their ruse, hackers may impersonate the names of known networks, such as those belonging to your local Starbucks or McDonald's. This type of attack is called the "evil twin." If an employee logs into the "fake" Wi-Fi server, it may allow a hacker to mount what is called a "man in the middle" attack, which allows the hacker to inspect the data flow between the victim and any resources they are accessing on the web or any computer that they are networked with.

Keep in mind that server administrators can capture unencrypted data being sent on even legitimate Wi-Fi networks.

Train your employees not to use USB devices from unknown sources.

Although USB flash drives are extremely useful for transferring data, they present substantial security risks if they come from unknown sources. Employees using USB drives at home and then plugging them back into the computer network at work is also a security concern.

USB devices can contain infected files that execute and spread malware when opened. For example, the Stuxnet worm which affected Iran's nuclear facilities was allegedly deployed on a USB device. USB devices can also be booby-trapped to emulate a keyboard and take over a Windows-based computer by sending keystrokes as soon as they are plugged in.

Back up critical system data.

Ransomware is a form of cyber malware based on encryption software that demands payment (ransom) to undo the damage. When the network is affected, the malware typically encrypts all data files, rendering them useless until the ransom is paid. According to Fortae, backing up your critical data remains the best recovery option to survive a ransomware attack.

Backups are best protected when they are maintained offline from the production environment because ransomware viruses can corrupt backup copies. Snapshots and replication copies can also be vulnerable to a time delayed ransomware attack. That means synchronized cloud backups are not good enough. In addition, backups should contain a complete, recoverable copy of not just data, but the entire server or network environment. A backup should be sequenced over many days, be a complete image and be located off site.

Anti-virus programs are ineffective.

Anti-virus software programs are generally ineffective and slow down your computer. This is because anti-virus software has a poor detection rate. The best anti-virus software only detects about 40 to 45 percent of viruses and malware. When an anti-virus program is operating, your computer may also become significantly slower – especially if you have real-time scanning enabled.

Before opening any file obtained from the Internet (email, website, etc.), Fortae recommends processing it through virustotal.com, a free online service from Google which analyzes files and URLs, enabling the identification of viruses, worms, Trojans, and other kinds of malicious content detected by anti-virus engines and website scanners.

These seven recommendations can't guarantee your company's cybersecurity, but they will go a long way toward helping you avoid the most common pitfalls. Taking these precautions is worth the effort to protect what you have built.

Michael Kokal is a certified privacy information professional (CIPP/US) and licensed intellectual property attorney. He practices law at the Springfield office of Heyl Royster where he is on the firm's cybersecurity committee. ◆