Can Your SMB Withstand a Cyber Attack?

Tools You Need to Safeguard Against a Cyber Attack

TOTALPROSOURCE.COM | 888.698.0763

Introduction

The use of advanced tools has made SMBs easy targets for cyber criminals. It's important to remain vigilant and take additional steps to protect your business against cyber attacks.

Using only one security program will leave security flawed and devices at risk to other threats. Layered security refers to security systems that use multiple security programs to protect your computer. These security programs work together, providing a layered protection to keep your business safe from cyber attacks.

In this e-book, you will find 14 cyber security tools that will help keep your SMB safe from today's leading cyber attacks.

Tip #1: Conduct a Security Assessment

When was your last security assessment? An unbiased, comprehensive review of your entire network will give you a clear, accurate picture of the health of your network, allowing you to protect your IT infrastructure from issues that may arise.

Tip #2: Install Proper Spam Filters

Ransomware attackers hide their malware in common attachments like text documents, invoices, faxes, etc., and an infection often starts with someone clicking on what appears to be an innocent email attachment. Most ransomware attacks originate in your email, so it's important to secure your email and reduce exposure to attacks on your staff via email.

Tip #3: Apply Password Security Policies on Your Network

It's important that your users create strong passwords as a first line of defense from scammers and hackers. Enable enhanced password policies such as password history limits, maximum age, minimum age, length, and complexity requirements.

81% of all breaches happen to SMBs.

Tip #4: Educate & Train Your Users on Cyber Security

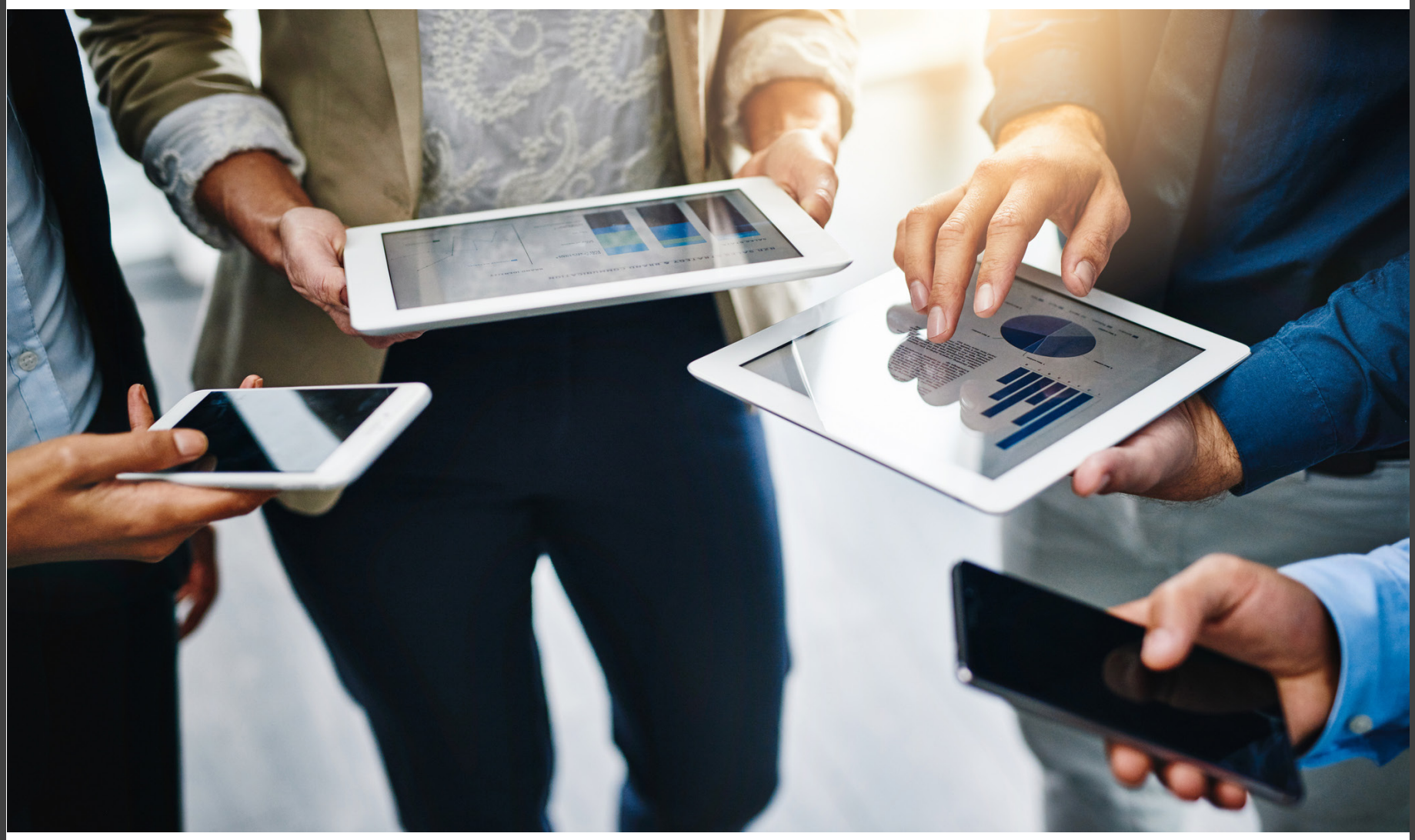
Most ransomware enters your network by a user clicking on a link in a phishing email. IT administrators play a more critical role than ever in educating users about the security risks they face. Training employees on cyber threats and what they should look for to avoid falling victim to an attack is the top component of a successful cyber security protection program.

Tip #5: Deploy Multi-Factor Authentication to Increase Login Credential Security

Multi-factor authentication mitigates the ripple effect of compromised credentials by requiring additional evidence that confirms your identity. Utilizing multi-factor authentication wherever you can, such as on your network, banking websites, and social media, adds an additional layer of protection to ensure that even if your password is stolen, your data stays protected.

Tip #6: Protect Against File-less & Script Based Threats with Advanced Endpoint Detection & Response

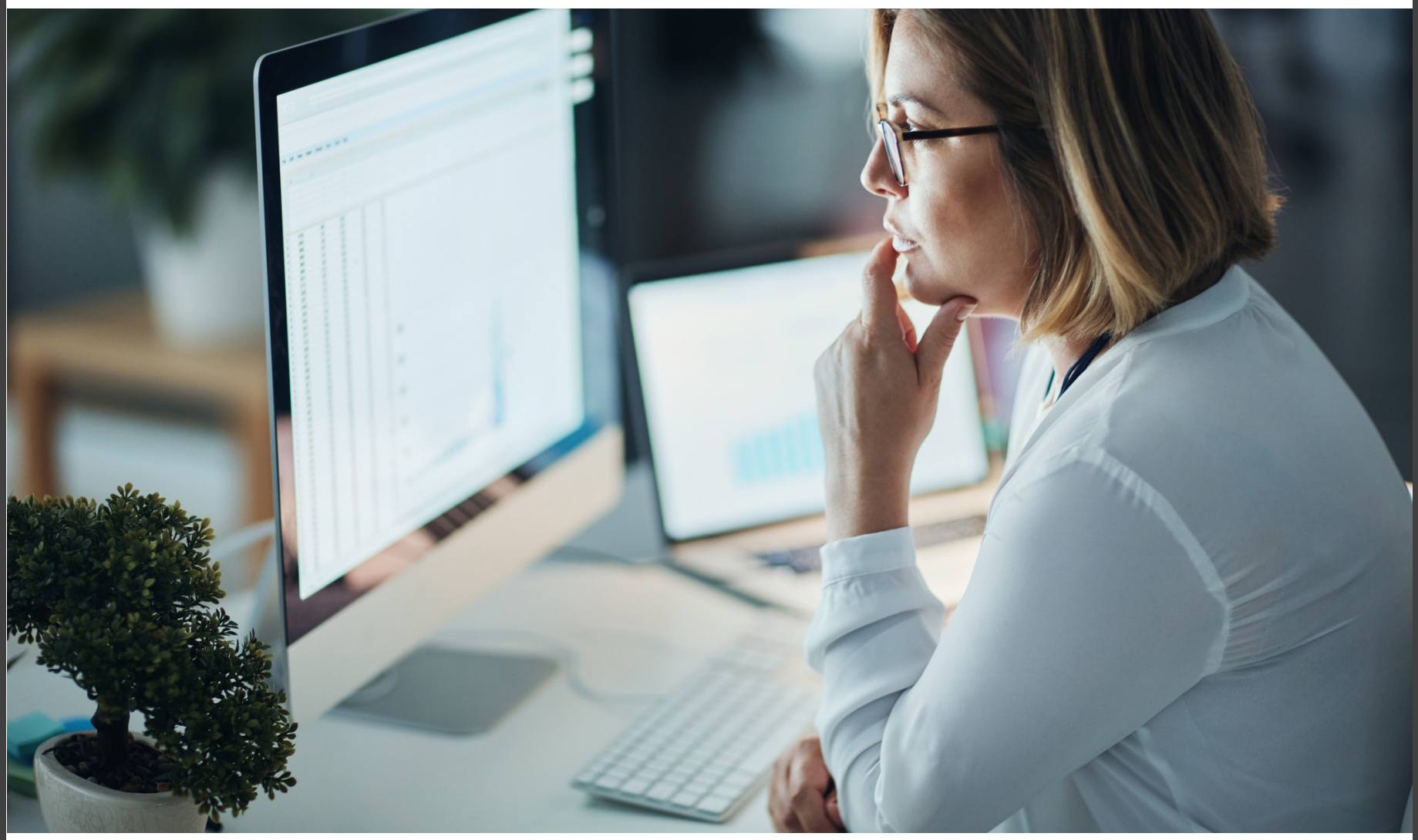
Any device, such as a smartphone, tablet, laptop, servers, workstations, and modems, provide an entry point for threats. File-less attack techniques are on the rise and current solutions aren't stopping them. More than just antivirus, endpoint detection and response combined with enterprise grade antivirus provides a security operation center to monitor and remediate alerts.



85% of hacking-related breaches leveraged stolen and/or weak passwords.

Tip #7: Update Your Software When Prompted

Most ransomware attacks exploit security vulnerabilities that have already been resolved through a patch or security update. Skipping software updates is a mistake that makes it easier for hackers to access your information. Since updates include security fixes, it's important to install updates whenever you are prompted.



Tip #8: Get Familiar with the Dark Web

The dark web is a collection of websites that exist on an encrypted network. It isn't visible to search engines and requires the use of an anonymizing browser called Tor to be accessed. You can buy credit card numbers, guns, counterfeit money, stolen subscription credentials, hacked Netflix accounts, and software that helps you break into other people's computers. Knowing what passwords and accounts have been posted on the Dark Web will allow you to be proactive in preventing data breaches.

Tip #9: Discover Hackers During the Breach, Not After with SIEM

Security Incident & Event Management (SIEM) collects and aggregates log data generated throughout a business's technology infrastructure, from host systems and applications to network and security devices such as firewalls and antivirus filters. This helps protect against advanced threats, allowing you to uncover hackers during the breach rather than days, weeks, or months later.

97% of breaches could have been prevented with today's technology.

Tip #10: Protect Data Stored on Mobile Devices

Over 50% of business PCs are mobile, and the increase in Internet of Things (IoT) devices poses new challenges for network security. Mobile device security fully protects data on portable devices, such as smartphones, tablets, and personal computers and the network connected to the devices.

Tip #11: Enable Enhanced Firewall Security

Turning on Intrusion Detection and Intrusion Prevention features, as well as sending log files to a managed SIEM will help you uncover intrusions such as exploitation attacks or compromised endpoint devices.

Tip #12: Keep Unsecured Traffic from Entering Your Network with Web Gateway Security

Web gateway security protects users from accessing and being infected by malicious Web traffic, websites, viruses, and malware. This cloud-based security detects web and email threats as they emerge and blocks them on your network within seconds – before they reach the user.

64% of SMBs have experienced web-based attacks

Tip #13: Make Your Data Unreadable & Unusable with Encryption

Encrypting your files at rest, in motion (email), and on mobile devices keeps sensitive information protected. By encrypting your files, your data will be unreadable and unusable until a password is provided.

Tip #14: Backup Your Data Frequently, in Multiple Locations

When it comes to preparing for a disaster, you can never be too careful or prepared. Backup your data locally and in the cloud frequently, and have an offline backup run every month. Be sure to test your backups to make sure they are working properly.

About Prosource

The rising number of mobile users, digital applications, and data networks means that individuals and businesses are becoming increasingly vulnerable to cyber exploitation. Ransomware attacks are on the rise and your data could be at risk. At Prosource, we combine products from leading cyber security and technology providers with our state-of-the-art IT services and solutions to help your business operate efficiently, effectively, and securely.

If you're interested in enhancing your cyber security efforts with a layered security approach, contact our cyber security experts by calling 888.698.0763 or by visiting totalprosource.com/contact-us.

Prosource is the trusted managed services provider and managed security service provider of businesses across Greater Cincinnati and Northern Kentucky. We combine best-in-class IT resources and expertise with our trademark customer-centered approach to power and protect your business with secure, cost-effective, and scalable IT solutions.

From managed IT services, cybersecurity, business continuity and disaster recovery, cloud solutions, and hosted voice—you can lean on us for your technology needs while you get back to running your business. Increase your uptime, decrease your risk, reduce your costs, and eliminate headaches with technology solutions built to give you a strategic advantage.

TOTALPROSOURCE.COM | 888.698.0763