

Security Tips for Small Businesses

Too many small and medium businesses spend their limited funds on security products only to see their investment – and best intentions – wasted when they fail to implement the most basic security practices.

The simple truth for any business is that you are always just one bad user decision away from being infected by malware. Misconfigure your firewall, grant the wrong person administrator rights or fail to update your antivirus, and you open the door wide open to cybercriminals to steal your data.

Cybercriminals never give up. They're always looking for new ways to break into your systems. Don't let that happen. Here are 10 security best practices to shore up your defenses:

1. INSTALL ANTIVIRUS

We'll get this one out of the way first! Your best defense against the vast majority of active malware is your antivirus solution. Select an antivirus solution that performs strong with independent tests like AV-Comparatives. Look for advanced features that protect against prevalent threats like ransomware, and choose an endpoint security solution that offers protection at multiple attack points to defend against bad websites, phishing and spam, malicious URLs, Zero-days and other online threats.

2. RESTRICT ADMINISTRATOR RIGHTS

Only authorized, knowledgeable IT admins should have administrator rights to your PCs. While it may seem like an inconvenience at times for small organizations, granting administration rights to a broad user base is a big risk. To maintain the highest security standards, you need to ensure users cannot change critical settings, download and install whatever software programs they wish, or disable the security tools you've put in place.

Moreover, some malware is unable to execute and make malicious system changes if the user is logged in without admin rights – creating an additional layer of defense against malware users may encounter.

3. INSTALL AND UPDATE A FIREWALL

Be it the Windows firewall or a third-party firewall application, be sure to install a firewall to defend against malicious network traffic.

Firewalls monitor and control traffic in and out of your network. To protect against downloading malicious content or to stop communication to harmful IP addresses, a firewall is a critical line of defense. Always keep it updated or it will start to miss threats.



Top-Rated Antivirus

Build a strong foundation for your security practice with VIPRE Advanced Security's industry leading malware defense. VIPRE protects users from more than 350,000 new threats that emerge every day, including viruses, Trojans, malicious URLs, phishing attacks, ransomware and more. VIPRE consistently scores a 100% block rate with zero false positives from independent testing authorities.

Best Protection for the Price –

VIPRE outperforms the biggest names in the industry for \$12 per seat/year.*

Deploys in Minutes – Quick and easy install, VIPRE's pre-configured settings have you well defended from day #1.

Doesn't Slow You Down – VIPRE doesn't slow down your PCs, keeping users secure and productive.

*Pricing based on a 250 seat minimum.

Learn more at
www.VIPREAntivirus.com/Business

Leading the Industry

VIPRE receives top-ratings from the industry's leading independent testing authorities.



4. IMPLEMENT PATCHES

Don't ignore those prompts to update popular software applications used in your organization. In many cases, prompts to update Adobe, Java, Chrome, iTunes, Skype and others are to fix discovered security vulnerabilities in those products. Cybercriminals exploit vulnerabilities to open a backdoor onto your systems to drop malware and infect your network. Implement an automated patch management solution to address this issue, or select an endpoint security solution with patch management included.

5. ENFORCE PASSWORD POLICIES

Users may view password updates as a chore, but password implementation and enforcement are a must. Require strong passwords or passphrases to maximize effectiveness, implement regular updates and instruct users not to share them.

6. LOCK THOSE SCREENS

All computing devices, including laptops, tablets and smartphones, have screen-locking features for security purposes. Be sure to enforce a short lock-screen timeout as added protection, especially in environments where users can walk away from workstations without logging off.

7. SECURE WI-FI ROUTERS

Wireless routers and networks are notoriously easy to break into, so take extra precautions in securing them. Change the network names and passwords that come with each router, and don't forget to activate its encryption capabilities. Use a separate Wi-Fi network for business guests. Also consider not broadcasting your network ID for added protection against hackers trying to discover and access your network.

8. SECURE YOUR BROWSERS

Configure web browsers to avoid inadvertent malware downloads by users. Steps to take include disabling pop-up windows, which can contain malicious code, and using web filters that warn you of potential malware attacks and harmful sites. Also, pay attention to browser privacy settings to prevent any private information from being siphoned by fraudsters and cyber-thieves, limit users ability to install browser plug-ins, consider disabling vulnerable applications like Adobe Flash, and always ensure you're using current and fully patched browsers when possible.

9. USE ENCRYPTION

Many machines come with built-in encryption, both at the disk and file levels. Take advantage of each device's encryption capabilities to prevent data from getting into the wrong hands when laptops, external hard drives, USB drives and other mobile devices are lost or stolen.

10. TRAIN AND RECRUIT YOUR USERS

Security isn't successful in a vacuum. Your users can be your biggest liability or your biggest asset. Engage your users and educate them on security best practices and why they are important. Train your users to spot threats, like malicious phishing attacks or strange PC behavior, and alert your IT leader immediately.

In addition to investing in the right security tools, it is critical to implement these security best practices to ensure your network is well defended from cybercriminals.

About VIPRE

VIPRE Advanced Security gives you top-rated malware protection at the industry's best value. For \$12 per seat/year,* you can defend your data with the award-winning malware defense that consistently earns 100% block rates and zero false positives from AV-Comparatives, the world's most widely-trusted independent antivirus testing authority. VIPRE uses cutting-edge machine learning, one of the world's largest threat intelligence clouds, and real-time behavior analysis to protect millions of users every day from top threats like ransomware, zero-day attacks and other malware that easily evade traditional antivirus. Easy to use, fast to deploy and simple to maintain, VIPRE's small footprint never slows you down, and all VIPRE customers receive free U.S.-based technical support. VIPRE Advanced Security eliminates all confusion about which endpoint security solution is right for you because we only offer our best protection and broadest feature set at the industry's best price.

*Pricing based on minimum purchase of 250 seats of VIPRE Advanced Security.