WHITE PAPER

Small Business Security

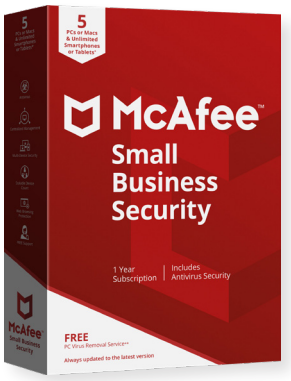
Smart Security Tips for Your Small Business

The truth is 53% of small businesses have been hit by a cyberattack, accournt to a recent survey by Verizon.

Today's small business owners have a lot on their plates, from focusing on growth, to managing employees, and making sure that the technology they invest in keeps their business running smoothly and their data secure.

It is no surprise that cybersecurity has become a top concern for many businesses, given the number of high-profile data breaches and ransomware attacks that we have seen in the news.

From the ransomware attack that left American city workers without computers or phones for months, to the denial of service attack that knocked Rokenbok Education completely offline, the threats can be daunting.



Top 3 Benefits of McAfee Small Business

- Virus, ransomware and malware protection
- Centralized license management
- Great for mixed BYOD environments

This is especially true for smaller businesses where the lines between professional and personal information are often blurred. Take, for instance, an entrepreneur who is using their personal credit card for business purchases. If their data is breached, the harm is twofold—potentially affecting both their business and their family finances.

What's more, the sheer number of attacks potentially affecting businesses is growing.

For instance, McAfee recorded 900,000 new phishing websites in the third quarter of last year alone, and the company notes that new malware attacks[1] can even target the intellectual property of all kinds of companies, even manufacturers.

While sweeping attacks against large companies dominate the news, small businesses are particularly vulnerable since they rarely have dedicated IT staff, and are frequently targeted by phishing attacks.

Take the case of a car dealership, Green Ford Sales. After their network was breached, the attackers stole $23,000 from their bank account, and even added nine fake employees to their payroll, costing them another $63,000.

Perhaps more concerning than the rate of small business attacks is a recent statistic released by the National Cyber Security Alliance, saying that 60% of small businesses3 that get hacked go out of business within six months. This is largely due to cost. According to a 2019 survey conducted by Continuum, cyberattacks cost small businesses an average of nearly $54,000, including the cost of cleanup and business interruption.

It's vital that small businesses safeguard against these threats before they happen. Here's what to look out for:

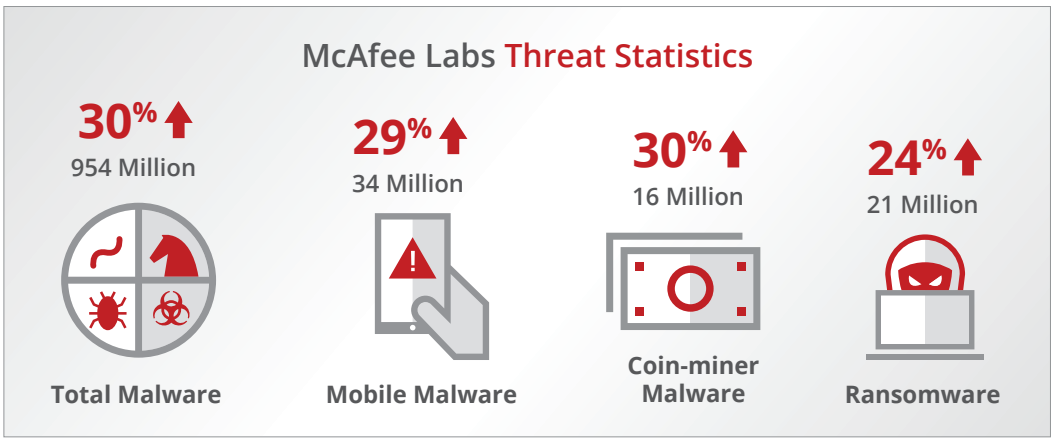
Official-looking Spam

Businesses are often targeted by emails that look like legitimate government requests for corporate payments or sensitive information. Some may even contain your correct federal, or state IDs.

However, clicking on these messages can lead you to dangerous websites, designed to steal your information and money, or even download malware onto your computer or devices. The same is true for delivery scams, and fraudulent emails inviting recipients to access company Google docs. These targeted attacks are successful because they mimic real day-to-day work activities.

Common Small Business Threats

- Ransomware
- Lost or stolen devices
- BYOD Threats
- DDoS Attacks



[5] Source: McAfee Labs Q1 2019—all percentages are increases from the past four quarters.

Spear Phishing

Another common threat to small businesses is targeted phishing attacks, known as spear phishing, in which a scammer sends an email that appears to come from someone within the company, requesting sensitive information such as employee salaries and Social Security numbers, admin passwords, or client data. Since these spoofed emails appear to come from someone with authority, like the company's CEO or accountant, employees often reply with the sensitive information without question.

Ransomware

It only takes one careless click to put your small business in danger of a ransomware attack. Ransomware is malicious software that locks up your computer and demands that you pay a ransom to regain access to your files. The ransom is often demanded in Bitcoin because it is untraceable. Even if you manage to pay it, there's no guarantee that your files will be unlocked.

Lost Laptops/Devices

One prevalent fear among small business owners is that a laptop or device that contains critical work information, such as the company's intellectual property, or client details, could be lost or stolen. That's why it's crucial to have security tools that allow you to locate, and even lock, lost devices remotely.

BYOD Threats

Because not all small businesses have the budget to supply employees with company computers and smartphones, many companies allow employees to use their personal devices. This practice is known as "bring your own device." While BYOD can save small businesses on initial expenses, it may cost them a lot later , if the personal devices are not properly secured. Say an employee device is infected with malware; this infection could easily spread once the employee connects to the office network.

DDoS Attacks

Of concern for web-based businesses is the possibility of a distributed denial of service attack (DDoS). This is when cybercrooks flood a company's server, network, or application with traffic, in order to shut it down, or gain access to valuable corporate data. While these types of attacks have been around for a long time, there have been reports of a resurgence in early 2019, aided by the vast number of internet bots, which are used to create traffic spikes. Make sure your business stays protected.

While sweeping attacks against large companies dominate the news, small businesses are particularly vulnerable since they rarely have dedicated IT staff.

Follow these 7 helpful tips:

1. Make sure your company network is secured.
   Change the default password on your router, since hackers often know these default passwords and can easily use them to enter your network. Check your router's manual to learn how. Also, make sure that your router encrypts the data that flows over your network. And, don't forget to use a firewall to block unauthorized access.

2. Use password managers.
   To avoid lost and stolen passwords, make sure everyone in the company uses a password manager. This valuable piece of software can both generate strong passwords and save them securely.

3. Delete any software or applications you don't use.
   This way, you reduce your exposure to potential vulnerabilities.

4. Ensure safe web surfing and email practices.
   Look into employing a web advisor on all your computers, to help employees avoid risky websites and dangerous downloads. You'll also want to talk to employees about phishing dangers and encourage them to flag any suspicious emails, even if they appear to come from within the company.

5. Keep your software up to date.
   Make sure all the software on your servers and devices are up-to-date to protect them from known threats. This also goes for your company website and applications. Pay attention to any notifications you may receive regarding updates or security issues.

6. Use comprehensive security.
   Invest in software, like McAfee's Small Business Security and hardware, as well as Dell's Latitude laptops with a security chip solution and a fingerprint reader that can protect your network from the latest threats. Use a VPN for encryption, private browsing services, to help keep all your online activities and information private and secure from cybercriminals—even on public Wi-Fi or open networks.

7. Foster a culture of security.
   Talk to your employees about common security concerns and have plans in place to diminish the risks. If you allow BYOD, ensure that all the devices that connect to your network are protected. You also want to keep your employees updated on the latest scams, so everyone knows what to look out for latest scams, so everyone knows what to look out for.

McAfee and Dell Partnership

Thanks to a partnership between Dell Technologies and McAfee, small business customers can now order hardware with McAfee Small Business Security preinstalled, giving them multi-device protection, spam control, safe search tools, the ability to track, lock, or wipe a lost or stolen device, and much more from one easy to manage location.

About McAfee

McAfee is the device-to-cloud cybersecurity company. Inspired by the power of working together, McAfee creates business and consumer solutions that make our world a safer place. www.mcafee.com

About Dell Technologies Advisors

Dell Technologies Advisors work with millions of small businesses, entrepreneurs and innovators around the world every day. And as a trusted partner to small businesses, we can advise security solutions for your technology. Call a Dell Technologies Advisor today at 1800 425 2054

[1] 2018 IDC Vertical Insights survey.

[2] Verizon 2019 Data Breach Investigations Report.

[3] Vistage Cyberthreats and solutions for small and midsize businesses.

[4] Continuum commissioned Vanson Bourne to conduct the 2019 State of SMB Cyber Security report research. It was carried out between January and March 2019.

[5] https://www.mcafee.com/enterprise/en-us/assets/reports/rp-quarterly-threats-dec-2018.pdf

2821 Mission College Blvd.
Santa Clara, CA 95054
888.847.8766
www.mcafee.com