SMBs Under Attack

A guide to understanding cyber risks and protecting organizations

VIPRE®

TABLE OF CONTENTS

INTRODUCTION: TARGETING SMBs

No matter the size of your business, you can't ignore cybercrime. Nor can you overlook hackers and the increasingly sophisticated malware they are continually unleashing on the internet. Simply put, you can't be complacent and think you're not a target. **Everyone is a target.**

Yet too many small businesses still believe their data has no value, that they're too small for cybercriminals to bother targeting them. It's an appealing illusion, but it's just that—an illusion. The cold hard reality is that your data is valuable, and the thieves who steal data such as personally identifiable information, medical records and trade secrets sell them for a tidy profit every day.

If you handle sensitive data such as Social Security numbers and credit card information—or have any intellectual property you want to ensure doesn't fall into the wrong hands—you must understand the risks you face, and the solutions that are available to help you defend your data.

Hackers are nothing if not relentless; they never stop looking for undiscovered vulnerabilities and keep conjuring new, creative ways to break into networks. No business is immune, and denying that fact may have severe consequences, such as compromising employee and customer data, losing intellectual property and erasing your competitiveness in the marketplace.

66% Ransomware Infections are due to Spam and Phishing Emails

BOTTOM LINE

Suffering a data breach can destroy your reputation, incur penalties for non-compliance with federal and state regulators, necessitate insurmountable remediation costs, drive away customers and alienate partners...The risks go on, but the point is clear—data breaches can be devastating to a small business.

About 67% of small and medium businesses (SMBs) participating in the Ponemon Institute's 2018 State of Cybersecurity in Small and Medium-Sized Business study[i] said their companies had suffered a cyberattack and 58% reported they had data breaches involving customer and employee information in the past 12 months. Only 28% of the participants rated as highly effective their "ability to mitigate cyber risks, vulnerabilities and attacks."

Worryingly, the report also shows that SMBs face a variety of challenges when trying to create a stronger security posture. The biggest problem is not having the personnel to mitigate cyber risks, vulnerabilities and attacks (74 percent of respondents), followed by insufficient budget (55 percent) and no understanding of how to protect against cyberattacks (47 percent).

Such unpreparedness is particularly troubling because effective threats continue to proliferate. For example, phishing has become a favorite cyberattack method because it's easy and inexpensive for attackers, and often succeeds because it preys on users' trust and curiosity. It also plays a significant role in ransomware infections: a recent PCMag analysis[ii] reports that spam and phishing emails are responsible for 66 percent of ransomware infections.

SMB Stats

Companies had suffered a cyberattack

Had data breaches involving customer and employee information in the past 12 months

Rated their "ability to mitigate cyber risks, vulnerabilities and attacks" as highly effective

Phishing and ransomware are just two examples of cyber threats against which SMBs must defend. While these specific scourges have received a great deal of attention in recent years because of their prevalence, it's important to remember that cyber threats are numerous and varied—and you need to deploy systems, implement policies and educate users to effectively combat them all.

Other threats from which you need protection—and which are discussed in more depth later in this guide—include web-based threats (such as clickjacking and drive-by downloads) and exploit kits.

This guide also features a discussion on how to implement BYOD (Bring Your Own Device) policies to prevent new vulnerabilities when employees are allowed to connect their own smartphones, tablets and laptops to the network. In addition, we detail security best practices for SMBs, and address some of the most common user errors that can create cyber risks for your company.

The sad reality of doing business in a modern, connected world is there is no shortage of cyber risks. The cost of cybercrime keeps rising, and is projected to reach $6 trillion by 2021[iii]. A data breach costs companies an average of $4.24 million[iv]. These are alarming numbers, but you are not completely defenseless against cyber risks. That's what we intend to show you in the following pages.

Cost of Cybercrimes

By 2021, cost of cybercrime projected to reach

$6 trillion

Data breach cost companies an average of

$4.24 million

WHAT YOU NEED TO KNOW ABOUT PHISHING

Phishing vexes many organizations because they can't solve the problem by just throwing technology at it. Preventing phishing attacks requires a combination of robust email security and effective user training.

That latter consideration—the human factor—is the tough part. Even when users understand the risks of clicking on suspicious attachments or URLs, some still do it. In a recent study, roughly half of the subjects in an experiment clicked on links from strangers in e-mails and Facebook messages, even though most of them claimed to be aware of the risks.

As such, it requires a truly sustained effort to educate users so they'll stop doing what they intuitively know they shouldn't do...but do anyway.

Indeed, that's one of the reasons phishing is so successful. Rather than trying to hack into secured systems, cybercriminals choose the path of least resistance by tricking distracted or trusting users into opening the door for them.

Fraudsters certainly have no shortage of material for bait: a phishing email may pass itself off as an Apple Store communication, a message from a Facebook friend, a package delivery notification, a resume from a job applicant or adopt myriad other disguises. The victim may click on an attachment that proceeds to download malicious code onto their machine (potentially infecting the whole network), or the unwitting user may visit a website that asks for private data, which the victim provides because they believe it's a legitimate request.

Three Phishing Approaches

Phishing currently breaks down into three main categories. Regular phishing casts a wide net, with cybercriminals sending emails to large groups in an attempt to ensnare as many victims as possible.

A second, more refined approach—spear phishing—targets specific groups or individuals. Spear phishing typically entails efforts to steal private information such as social security numbers, credit card numbers and financial account information.

This technique is, by far, the most successful on the internet today, accounting for more than 90% of attacks. Spear phishers gather personal information about victims from social media and other sources to create bait emails that will seem more legitimate, and thus more credible, to their recipients.

A third technique—whaling—focuses on higher-profile targets such as C-level executives, politicians and celebrities. "Whaling emails and websites are highly customized and personalized, often incorporating the target's name, job title or other relevant information gleaned from a variety of sources," according to TechTarget.

PROTECT YOURSELF

To prevent phishing attacks, you must train users to identify and avoid phishing emails. Beyond that, you need to deploy an email security solution that includes advanced features designed specifically to combat this threat.

Such features include a sender policy framework, which checks if incoming email was sent by authorized hosts; auto-whitelisting, which automatically adds and removes listings based on preset criteria; and a regularly updated spam filter that recognizes and sifts out potential phishes.

Phishing is the most successful attack vector used by cybercriminals and the primary method used to deliver ransomware. Simply put, failing to effectively address phishing makes you highly susceptible to a cyberattack.

Secure Your #1 Threat Vector

The greatest security vulnerability within any organization is its employees, and they are targeted through email more than any other threat vector. Deploy the protection you need with best-in-class email security that doesn't slow you down.

VIPRE Email Security Cloud is an advanced, powerful, policy-based email security solution that defends networks against spam, phishing, viruses and other security threats transmitted via email.

Email Security Cloud also offers a comprehensive suite of add-on services:

- **Phishing protection** guards against phishing links, which are the leading cause of ransomware delivered via email; this component protects your users by ensuring bad URL links cannot become weaponized and redirect to harmful websites or download malicious files to your network.
- **Attachment sandboxing** evaluates unknown attachments for potentially malicious behavior using VIPRE's Behavioral Determination Engine, an artificial Intelligence engine that applies machine learning for true zero-day threat detection.
- **Encryption** enables you to stay in regulatory compliance and ensure customer data is securely transmitted; using this component you can protect private and confidential data while in transit—with no hardware or software to install for the sender, recipient or administrator.
- **Archiving** helps you meet today's increasingly stringent compliance and retrieval requirements, which demand that businesses store more data than ever before; this component makes searching and archiving your organization's entire mail history quick and easy, no matter how much data you must preserve.

RECOGNIZE & FEND OFF WEB-BASED THREATS

Phishing poses a serious cyber risk to SMB organizations, but it's far from the only one. Cybercriminals have a wide array of other methods at their disposal to break into networks and steal data. The hacker bag of tricks includes web-based threats such as website hijacks, drive-by downloads and plug-in exploits.

Hackers use web-based attacks to download malicious code onto networks to alter files, disrupt network operations and steal information. Common types of web-based attacks you need to know about include:

Clickjacking

Hijacking a legitimate website link and redirecting users to an infected website, where users either unknowingly share confidential information or trigger an intrusive action such as turning over control of their computer's camera or microphone to hackers.

Drive-By Downloads

Secretly downloading malware onto a system when the user visits a website. Typically, the malware hides in the background until it's ready to do its nefarious work, which could be stealing information or turning the machine into a bot controlled remotely by hackers.

Watering Hole Attacks

Compromising a group of users through infected websites that a targeted group's members are known to visit. Once a user goes to one of the websites, malware is downloaded or sensitive information is stolen to gain network access.

Plug-In Vulnerabilities

Exploiting vulnerabilities in commonly-used tools such as Java, and file formats such as PDF, CSV and HTML, to deliver malware.

Social Engineering Data Theft

Using data shared willingly by users on social media to break into networks and to craft phishing emails that trick recipients into opening infected attachments or visiting compromised URLs.

Malvertising

Hackers can infect online advertising campaigns (such as banner ads) that run through ad networks and are encountered on popular, trusted sites to victimize unsuspecting users.

PREVENTIVE STEPS

Preventing web-based threats requires businesses to stay on constant alert. For example, you must educate your users on safe web browsing practices to help prevent them from downloading malware onto their machines and your network.

You must also deploy and maintain security tools such as antivirus solutions, firewalls and web filters. Keep these tools up to date because unpatched files and systems make it easier for hackers to inject malware onto networks. Resist the temptation to delay or ignore patch management; every time a software or security vendor releases a patch, be prepared to test it and implement it to minimize the chances of a web-based attack.

Lastly, you need endpoint security to protect the edges of your network by keeping your browsers free of infections, performing fast malware scans, removing compromised mobile devices from the network, and performing threat analysis whenever suspicious code is identified.

By taking these steps you minimize the chances of suffering a web-based cyberattack.

KEEP AN EYE OUT FOR EXPLOIT KIT THREATS

Web-based attacks sometimes involve exploit kits; an unfortunate side effect of the technology world's "as-a-service" evolution, these kits give cybercriminals yet another way to carry out their dirty deeds. While well-intentioned businesses can leverage software-as-a-service (SaaS) or infrastructure-as-a-service (IaaS) to cut costs and build new efficiencies, those with less noble intentions can just as easily utilize malware-as-a-service (MaaS) to execute their cyberattacks.

MaaS enables authors of exploit kits to monetize their "offerings" by making them available for sale or lease on the Dark Web to other cybercriminals, who may or may not possess the skillset to create these tools themselves. Exploit kits have lowered the barrier of entry into cybercrime, helping to fuel a much broader and more toxic threat landscape for businesses.

How Exploit Kits Work

An exploit kit essentially contains a library of known vulnerabilities in popular software applications like Adobe Reader, Skype, Internet Explorer, iTunes, Chrome, Firefox, Java and many others.

Exploit kits are unleashed via spam campaigns, or hosted on malicious or compromised websites. They can even be deployed via malvertising campaigns to compromise online ad networks. Users who click a link, browse to an infected site or open an infected email attachment unwittingly open themselves up to attack. The exploit kit first scans the PC looking for vulnerable applications; if found, the exploit kit can then open a backdoor onto the PC and your network.

But that's just the beginning; the exploit kit then calls back to a command and control server to accomplish its true mission—delivering a malicious payload through the door it has now opened onto your PC. That payload may be ransomware, a credential-stealing Trojan, code to turn your PC into a bot to power the spread of more exploit kits, or any number of other online threats.

Exploit Kits are Big Business

With names like Angler, Neutrino, Nuclear and RIG, exploit kits have helped create a widespread criminal enterprise with huge revenue potential. Cisco has estimated the Angler kit alone generates as much as $60 million annually.

Kit authors take a business-like approach to MaaS, even regularly updating their kits, much like software developers do with their applications, and offering their "customers" product guarantees. "Developers create tools that they sell or rent to customers through online black markets, complete with sales, money-back guarantees, and reputation systems to provide customers with assurances that they won't get ripped off," according to Trustwave[v].

EXPLOIT KIT DEFENSES

As exploit kits typically attack unpatched systems and applications, your best defense is to keep current with security patches. While zero-day attacks get the lion's share of headlines, the vast majority of vulnerabilities exploited by these kits are already known and addressed by security updates.

Too many businesses simply do not patch applications as often as they should. There are certainly legitimate reasons to use older versions of applications—for example, running legacy applications that only work on older versions of Java—but IT admins should take care to provide extra visibility into those systems. For all remaining systems, patching is absolutely critical.

Even threats posed by exploits that have been developed to evade detection by antivirus engines are nullified if the systems they encounter are fully patched. To ensure patches are applied as they become available, consider an automated patch management solution, which enables IT to manage all security updates.

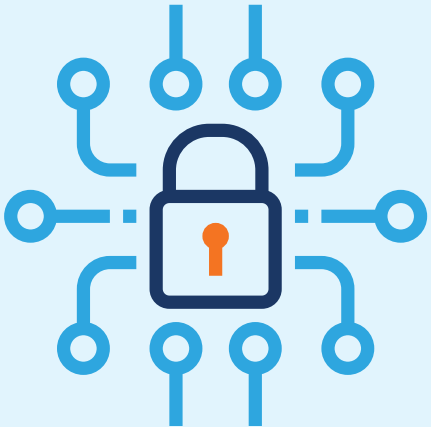
Ideally, you want to deploy an endpoint security solution with integrated patch management. VIPRE Endpoint Security gives you a single tool to defend against malware, eliminating vulnerabilities caused by unpatched/outdated applications by employing integrated patch management.

Each year software and secure vendors issue dozens—perhaps hundreds—of patches. It requires a great deal of effort to keep up with them all, which is why you should adopt a patch management strategy that includes automated tools. It is vitally important that you don't ignore security patches and leave your business vulnerable to cyber threats, including those delivered by exploit kits.

PATCHING MADE EASY

VIPRE's integrated patch management capability enables you to seamlessly manage updates for more than 30 popular software applications, including:

- Adobe Acrobat
- Adobe AIR
- Adobe Flash Player
- Adobe InDesign
- Apple iCloud
- Apple iTunes
- Apple QuickTime
- Google Chrome
- Java
- Mozilla Firefox
- VMWare Workstation
- WinZip
- Wireshark
- Yahoo Messenger



FOLLOW BYOD BEST PRACTICES

The BYOD trend has complicated the responsibilities of IT administrators and security managers who are tasked with defending their organizations against phishing, ransomware, web-based threats and other cyber risks.

Ever since BYOD (Bring Your Own Device) entered the IT lexicon, companies have been dealing with how to protect business networks while letting employees use personal mobile devices in the office, at home and on the road.

It's not an impossible challenge to meet, but it does take a solid understanding of the potential dangers BYOD presents to your organization. You must recognize the risks and their potential impact on your business, and then you can devise a strategy to address those risks by securing devices and preventing them from giving hackers a way onto your network. With the proper mix of robust security, management tools and user education, you can make BYOD work for you without exposing your data.

BYOD Popularity

The BYOD market is growing by leaps and bounds, projected to reach almost $367 billion by 2022—up from only $30 billion in 2014—according to a report[vi] by Global Market Insights. Clearly, the business world is embracing the BYOD concept, but how well is it handling it?

Not too well. A study[vii] by Bitglass found that 51% of survey respondents reported an increase in the volume of threats targeting mobile devices, following the rise of BYOD and mobile data access, but a full 43% did not know if their devices accessing corporate data were infected with malware.

This is troubling, especially considering that key sectors such as education and finance are favorite cybercrime targets. But whatever your industry, if you adopt a BYOD policy, make sure that you do it safely.

And that means taking steps such as:

- Deploying mobile device malware protection
- Implementing strong user authentication and password policies
- Blocking unsanctioned applications
- Wiping devices that are lost or stolen
- Installing VPN applications for secure network communications
- Creating a separate gateway with optimized security controls for mobile devices accessing your network
- Educating users on configuring devices for maximum security and avoiding unsecure networks
- Auditing mobile devices to ensure compliance

BYOD DANGERS

If you neglect to secure mobile devices, you are quite simply playing with fire. New malware threats are popping up constantly, and many specifically target mobile devices. Just a single infected device can unleash a virus, worm or ransomware that could potentially shut down an entire network.

Recovery costs and lost productivity can quickly add up. Depending on the size of your company, you might need to spend hundreds of thousands of dollars (or even millions) to remediate something that a much smaller investment could have prevented.

Protecting the Network

Any organization that embraces BYOD should seriously consider implementing a Mobile Device Management (MDM) solution that includes centralized security management of your mobile devices, enabling you to more efficiently prevent malware and quickly wipe data if needed.

As part of any mobile device management policy, you must enforce user access policies that require strong passwords or passphrases to protect data, along with controls to prevent access to unsanctioned applications and websites.

Mobile malware protection is also critical; at its most basic, mobile antivirus performs malware scans that prevent infections. But solutions have become increasingly sophisticated, even offering some of the same features as MDM, such as remote monitoring, device lock, alarm and wipe, as well as GPS capability to locate lost or stolen devices.

Productive and Secure

BYOD can yield significant benefits by giving users device choices, which makes them happier and more productive at their jobs. Just don't let BYOD compromise your security.

ASSESSING YOUR VULNERABILITY TO RANSOMWARE

What is Ransomware?

Ransomware is malware that infects your PC or network by encrypting your data, and then demanding a ransom to restore access to your files.

As the ransomware epidemic continues to spread, it would be prudent to ask yourself how susceptible your business is to cyber extortion. A vulnerability assessment is a good first step towards strengthening your defenses.

Fending off ransomware attacks requires a multilayered strategy. If all you've done so far is to rely on antivirus scans and the good sense of your users to not click on suspicious emails, you're frankly doing less than the bare minimum. Yes, antivirus solutions are certainly a vital element in your malware defense, but they cannot do the job alone. And failing to educate users on the dangers of phishing virtually amounts to business malpractice.

With those points in mind, here are six questions you should ask when assessing your ransomware vulnerability. Your answers should make it obvious in which areas of security you need to invest.

1. **Are you training users on the dangers of phishing?**
   With so many phishing emails containing ransomware, this is a must. You need to invest in an education program that explains how phishing attacks occur and, through repeated training exercises, conditions users to spot and report suspected phishing emails.
2. **Do you back up your business data regularly?**
   Surveys have found that up to 53% of businesses don't back up every day, which in a digital context amounts to begging for trouble. Backing up is the most basic (and one of the most effective) steps to avoid having to pay a ransom to retrieve your data.
3. **Do you have anti-phishing email security?**
   You should deploy policy-based email security at the server level to defend against phishing as well as spam, viruses and other threats. Your email security solution should include secure email inspection, cleansing and management.
4. **Have you deployed endpoint security with specific ransomware protection?**
   As malware threats increase in sophistication, so should the tools to combat them. Endpoint security is integral to a layered defense strategy; you need to leverage an advanced solution that effectively helps prevent ransomware, and defends against the malware and attack vectors that cybercriminals use to spread this pervasive threat.
5. **Are your mobile devices secure?**
   Your security strategy must take into account all the devices that access your network, which means all laptops, smartphones and tablets should be secured. You also should consider encryption and strong authentication policies for added protection.
6. **Do you have a patch management policy?**
   Ransomware authors often exploit vulnerabilities in Microsoft Office files, JavaScript downloaders and Windows Scripting Files (WSF) to carry out attacks. That's why testing and implementing patches when they are released is imperative. An automated patch management solution is your best bet.

If You Said No

If your answer to any of the above is "No," you have a problem. If you want to avoid a ransomware attack, start working on turning those noes into yesses.

FIGHT BACK AGAINST RANSOMWARE

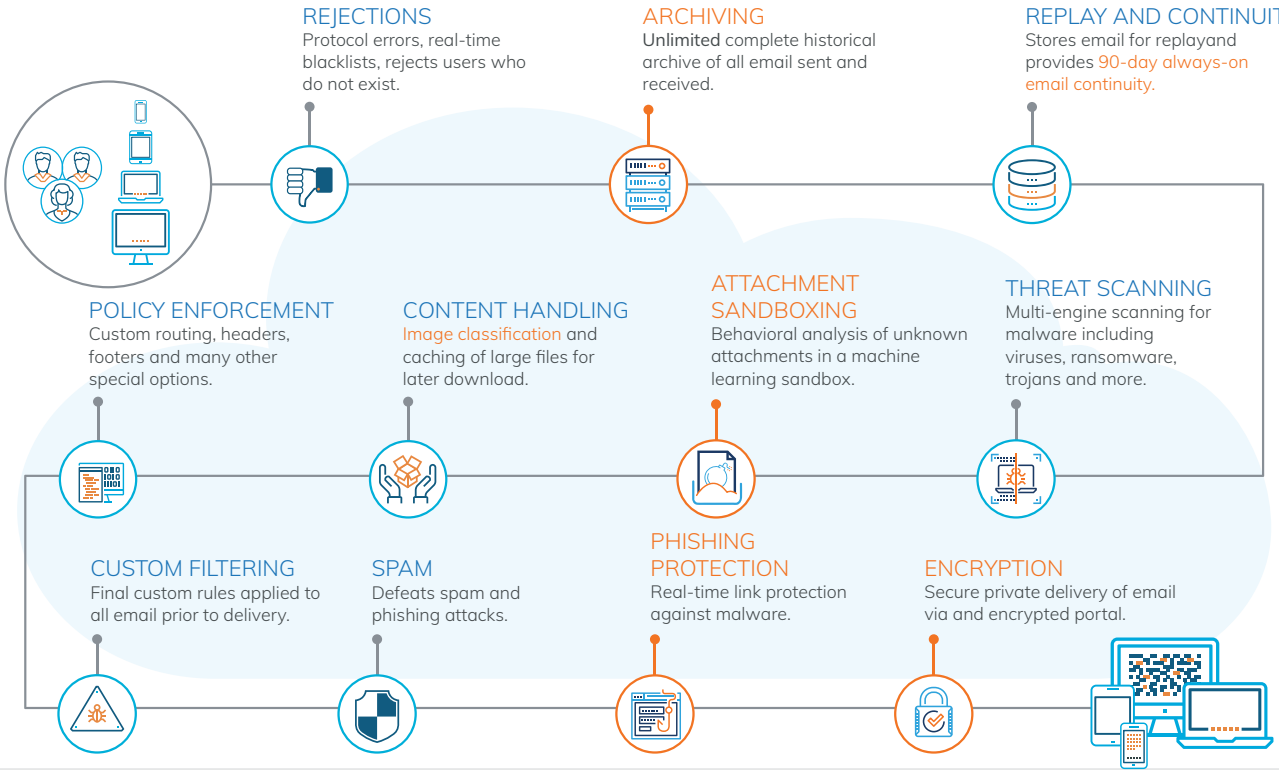
Virtually every business large or small relies on email as the primary business application for communicating both internally and externally. The challenge is cybercriminals and threat actors know this to be true as well, and perpetrate attachment, phishing and URL attacks against businesses every day. Most organizations employ a basic form of email scanning, backed up by an endpoint security solution. Unfortunately, with today's complex security climate, passive scanning is not enough protection.

VIPRE Email Security Cloud

VIPRE offers superior ransomware protection by preventing many of these threats before they can infect PCs. VIPRE puts the world's most sophisticated anti-malware technologies in your hands, using cutting-edge machine learning, one of the largest threat intelligence clouds and real-time behavior monitoring to protect you from ransomware, zero-days and other pervasive threats that easily evade traditional antivirus.

VIPRE Email Security Add-on Solutions

Zero-hour threats, polymorphic malware and weaponized attachments demand a sophisticated multi-layered approach to keep businesses safe. VIPRE Email Security and suite of add-on solutions, delivered from the convenience of cloud-based architecture, is the secure choice for today's pervasive email threats.



10 SECURITY TIPS FOR SMBs

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 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 for cybercriminals to steal your data.

Here are 10 security best practices to shore up your defenses:

1. **Install Endpoint Security**
   We'll get this one out of the way first!

   Your best defense against the vast majority of malware is your endpoint security solution. Select one that performs strongly with independent tests such as 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 restricting rights may sometimes feel inconvenient for small organizations, granting administrator rights to a broad user base is a major risk. To maintain the highest security standards, you must ensure that users cannot change critical settings, download and install whatever software programs they wish, or disable the security tools you've put in place. Fortunately, some malware is unable to execute and make malicious system changes if the user is logged in without admin rights, thus creating an additional layer of defense for users who may encounter malware.

3. **Install and Update a Firewall**
   Whether it's 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 users 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.

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 newly-discovered security vulnerabilities in those products. Cybercriminals exploit vulnerabilities to open a backdoor onto your systems so they can 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.

10 SECURITY TIPS FOR SMBs (CONT'D)

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. You should also pay attention to browser privacy settings to prevent any private information from being siphoned by fraudsters and cyber thieves. Additional steps include limiting your users' ability to install browser plug-ins, possibly disabling vulnerable applications like Adobe Flash, and always ensuring 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 greatest asset. Engage with your users and educate them on security best practices, and why they are so important. Train them to spot threats or unusual activity, such as malicious phishing attacks or strange PC behavior, and to immediately alert your IT team.

EDUCATE USERS ABOUT THESE COMMON MISTAKES

The need for proper cybersecurity training for users cannot be stressed enough simply because user actions contribute to most breaches. As Verizon cheekily counsels in its 2018 Data Breach Investigations Report, "The use of default or easily guessable passwords is as en vogue as tight rolling your jeans. Stop it."

But mishandling passwords is just one of many mistakes users make that can put your business at risk. The following is a list of eight common no-noes that your users may be committing; if they are engaging in these activities, you need to come up with an education plan that will modify those risky behaviors.

1. **Sharing passwords, intentionally or not**
   Whether users intentionally share passwords with colleagues, friends and family or just leave them on sticky notes by their computers, the effect is essentially the same: An unauthorized person can use the password to get into the network.
2. **Using weak, or default, passwords**
   Users often don't bother to change default passwords—whether on websites, applications, machines or Wi-Fi routers—which creates vulnerabilities. Or they'll use easy-to-guess names or dates because they're simpler to remember.
3. **Opening suspicious emails**
   Even when users suspect an email is bad, many will still click on an attachment or a URL, possibly unleashing a virus or ransomware in your network.
4. **Sharing personal information**
   As with #3, users often act against their own instincts, providing information such as bank account numbers, credit card information and Social Security numbers when requested by an email or a website reached through a suspicious link.
5. **Turning off security controls**
   Be it a firewall, antivirus solution or pop-up blocker, turning off any security tool poses a serious and immediate risk. Yet users sometimes do this because they view these tools as an inconvenience or waste of time.
6. **Leaving machines unattended**
   Leaving laptops on and unlocked and then walking away is a big no-no, but users are guilty of this, both in the office and in public places such as coffee shops.
7. **Using social media carelessly**
   Social media-related risks abound, from revealing too much information to sharing employer dirty laundry to clicking malware-infected links.
8. **Improperly sharing files**
   Users that transfer files from work to personal machines, either by email or using USB sticks, could be flirting with malware infections—and they may be violating applicable data privacy laws.

CONCLUSION

Every day, new cyber threats seem to pop up. Keeping up with them all is no easy task for SMBs, but you simply cannot ignore them because doing so puts your business at risk. Avoiding risk takes a combination of technology, well-crafted policies and user education. If you follow the advice put forth in this guide to secure your business, you will minimize your chances of falling victim to a cyberattack.

Learn more about keeping any size business safe with layered protection: https://www.vipre.com/products/business-protection/

ABOUT VIPRE

VIPRE is a leading provider of internet security solutions purpose-built to protect businesses, solution providers, and home users from costly and malicious cyber threats. With over twenty years of industry expertise, VIPRE is one of the world's largest threat intelligence clouds, delivering unmatched protection against today's most aggressive online threats. Our award-winning software portfolio includes comprehensive endpoint and email security, along with threat intelligence for real-time malware analysis. VIPRE solutions deliver easy-to-use, comprehensive layered defense through cloud-based and server security, with mobile interfaces that enable instant threat response. A proud Advanced Technology Partner of Amazon Web Services, VIPRE is headquartered in Florida and operates globally across North America and Europe. VIPRE® is a subsidiary of J2 Global, Inc.
www.VIPRE.com

[i] 2018 State of Cybersecurity in Small & Medium Size Businesses, Ponemon Institute; November 2018
[ii] How IT Can Defend Against Ransomware, PCMag; January 2019
[iii] 2019 Official Annual Cybercrime Report, Cybersecurity Ventures; December 2018
[iv] 2018 Cost Of Data Breach Study, Ponemon Institute; October 2018
[v] 2016 Trustwave Global Security Report
[vi] Bring Your Own Device (BYOD) Market Size By End-Use (Small Businesses, Mid-To-Large Sized Businesses), By Device (Tablets, Smartphones, Laptops), Industry Analysis Report, Regional Outlook, Application Potential, Price Trend, Competitive Landscape & Forecast, 2015 – 2022, Global Market Insights
[vii] Mission Impossible: Securing BYOD, Bitglass; November 2018

VIPRE_2020_EB_SMBs_UnderAttack_0106