ULTIMATE GUIDE TO SMALL BUSINESS CYBER SECURITY

PTG

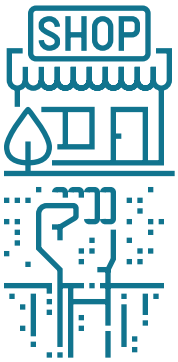
www.GoPTG.com

Info@GoPTG.com

Introduction

Cybercrime is in the news almost daily. We hear about large-scale attacks that damage companies' reputations, cost billions of dollars to remediate, and create significant stress for those who've been targeted.

But it's not just big corporations that are at risk of attack. Data from Symantec's 2016 Internet Security Threat Report shows that small businesses have increasingly become targets for cyber criminals. Symantec's report reveals that about 1 in 40 small- to mid-sized businesses are at risk of experiencing a cyber crime. And IBM's research shows that SMBs are the target of 62 percent of all cyber attacks. As more businesses move to the cloud, so do cyber threats. Microsoft reported seeing a 300% increase in attacks on cloud-based user accounts from Q1 2016 to Q1 2017.



IBM's research shows that SMBs are the target of

62%

of all cyber attacks.

We hear about cyber attacks so often these days that it's easy to become numb to the risks. But the cost of complacency is severe. Not only do companies face hard costs, which average more than $1.8 million dollars for SMBs, but there are soft costs to consider as well. The loss of business due to a damaged reputation is hard to measure, but those who have experienced it know it's substantial.

Small- to mid-sized businesses can proactively protect themselves against these attacks if they arm themselves with knowledge about the threats and take steps to secure their systems. This guide shares what you need to know and do in order to mitigate your risk of security breaches. Unfortunately, there is never a 100% guarantee when it comes to cybersecurity, but following the advice outlined in this guide will drastically limit the chances of falling victim - and help you prepare if you do experience an attack.

> Small- to mid-sized businesses can proactively protect themselves against these attacks if they arm themselves with knowledge about the threats and take steps to secure their systems.

Common Threats

While specific tactics vary, cybercriminals tend to use a few common strategies to accomplish their attacks. We'll look at three of these, as well as another significant-but-often-underestimated cause of breaches: human weaknesses.

1. RANSOMWARE

Ransomware has become one of the most popular ways for cybercriminals to make money. In fact, it's become a multi-million dollar industry (and make no mistake, cyber crime is an industry. It's a type of malware that encrypts your files until you pay a ransom fee).

The most common method for ransomware delivery is a Trojan Horse spread through email or a malicious link: a program masquerading as a helpful tool or a legitimate file with something sinister hidden inside. Once the program is downloaded, it quietly drops its "payload" (ransomware) onto your computer. The program then runs in the background, undetected, until it's too late.

Ransomware can be spread through other methods, though. The major Wannacry ransomware attack was spread through exploiting a vulnerability in older operating systems.

When a company has mapped network drives that connect back to the corporate server, the encryption will go beyond the local computer to infect the server and encrypt all of the company's files. Criminals are getting savvier and developing more complex attacks that use more advanced malware payload droppers (what they use to install the malware) and take advantage of encrypted web communication, making it even harder to detect an infection

The most common method for ransomware delivery is a Trojan Horse.

The Great Debate

The biggest debate in the cyber security community is whether companies should pay the ransom. One on hand, if you pay the ransom, ultimately you are giving the cyber criminals what they want, and the funds to continue what they're doing. On the other hand, if you can't access any of your files, your business is at a standstill (at best).

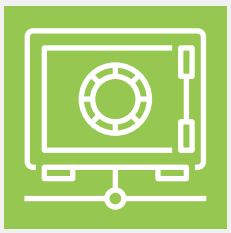
The best advice we can give here is to have **robust backups of your files**. That way, if your company does get ransomware, your files aren't lost and you don't have to pay the fee. You just need your IT team to remove the malicious files and restore your files from the back up.

Variations and Imitations

Ransomware has become such a popular form of cybercrime that criminals are now using it as disguise for other types of malware. Unfortunately, it's almost impossible to distinguish these from ransomware just by looking at them.

Non-encrypting ransomware/scareware: This type of malware looks just like real ransomware, but doesn't actually encrypt your files. It's just trying to scare you into paying the ransom. Sometimes, these are made to look like it's a warning message from the FBI or another government organization saying you need to pay a fine. Although these attacks are frightening for the computer user experiencing them, the infections can usually be removed with a scan and removal of malware and rootkits.

Wiperware: This form of malware looks just like ransomware, but rather than encrypting your files, it erases them. Paying the fee won't get you your files back. This is usually the worst case scenario when it comes to ransomware, and why we recommend backups so strongly.



The best advice we can give here is to have robust backups of your files.

Steps to Prevent Ransomware

Fortunately, there are simple steps that will keep ransomware off your system if you follow them.

1. **Don't open emails or the files in emails from email addresses that you don't recognize.**

2. **Don't click on links in emails or open files from email addresses that you do recognize if there is anything abnormal going on.** Criminals have now learned how to "take over" an email account and can send ransomware from legitimate accounts (even those within your company). When in doubt, call to confirm with the sender that a link or file is safe before clicking on it.

3. **Don't go to websites that you don't recognize, and verify the URLs of websites** that seem legitimate. Hackers are building websites that look just like the real ones they are impersonating with URLs that are only slightly different than the real ones.

4. **Block executable file types** from coming through on email (here's how) or block file attachments entirely, requiring a safe word to allow emails with file attachments through. This step will stop Trojan Horse programs from entering through email attachments.

5. **Don't click on any links or open attachments when you're in a hurry**. You are less likely to notice the red flags when you are feeling rushed.

6. **Start running Deep Packet Inspection on all traffic** on your network, both encrypted and plain text. This protection is typically run on a firewall and will spot the network traffic of ransomware that's trying to communicate with its host. Deep Packet Inspection will then kill the connection, stopping the damage.

7. **As always, keep your antivirus, operating system, and programs up to date.** Updates patch vulnerabilities that have been discovered and exploited by these hackers.

8. Make sure that you **keep good, working backups** that are easily restored.

9. Ask your IT company (or IT manager) to **examine your users' permissions on shared folders on your servers.** Are there users that have full access where less will suffice? Encrypting ransomware takes advantage of the permissions of users on network drives, so limit access as much as possible.

10. Tell your users to not save anything locally on their computers. Instead, **save all important data on network drives or in Cloud storage.**

11. **Train your employees on data security.** One person clicking on one bad link can infect an entire company. Remind employees regularly about the importance of security and review warning signs, what to look out for before opening attachments or clicking links, and what to do if something goes wrong.

2. PHISHING ATTACKS

News that sounds too good to be true usually is. Phishing attacks originally began in the form of emails that announced that the recipient had won money or that asked for help with the promise of a reward.

Today, attackers have added new tools to their arsenal. What phishing attacks all have in common is the goal of tricking the target into thinking that the email is from a legitimate source to gain access to personal or business information or money.

Phishing attacks target both individuals and companies. In one example, criminals are sending emails that appear to be from the IRS. These emails say that you're entitled to an additional tax refund and ask you to click a link to receive the money they owe you (click the example to right to see a larger version).

Some more sophisticated phishing attacks impersonate someone in your company (usually a high-ranking individual or an HR manager), asking for money for various reasons. Other attacks directed at companies target based on apps or software you use. We've seen dozens of phishing attempts targeting Office 365 users. Most of these try to scare the user into clicking by claiming their account is suspended. Others try to trick them by blending in, like by imitating a spam quarantine notification.

Phishing attacks all have a goal of tricking the target into thinking that the email is from a legitimate source.

Types of Phishing Attacks

There are a few different types of phishing attacks, varying in severity.

1

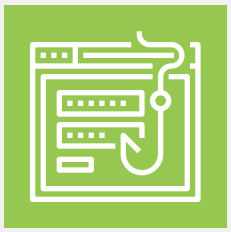
Phishing is an attempt to impersonate a reputable company or person in an attempt to trick you into giving up information, such as your password or banking information. Phishing attacks are usually widespread across hundreds of thousands of users, with the hopes of many people falling for the attack. The most common phishing scams are: IRS emails, password reset emails, or fraudulent credit card warnings.

2

Spear Phishing is a directed attack. The attacker has researched his or her target to better tailor the attack to increase the chance of success. For example, an attacker might learn the name of one of the Human Resources personnel and the type of coffee that this person drinks. The attacker will then create an email directed to this individual that appears to be from the favorite coffee brand announcing that the individual has won a coffee prize, with a link to claim the prize. Or the criminal will create an email to a lower-level employee that looks like it's from a member of the leadership team, asking the individual to wire money.

3

Whaling is a spear phishing attack directed at executive level users. Because companies often publish the names and contact information for their executives on their websites, hackers can easily learn what they need to know to successfully target high-ranking company officials. Here's a real world example from one of our customers, including how they were able to recognize it was an attack before it was too late.



How to Identify a Phishing Attack

Phishing emails often share a few telltale characteristics:

1. Bad grammar or misspelled words
2. Spoofed email addresses that appear with the name of someone that the recipient would know
3. A request to be contacted via a link or only one method of contact
4. A request for financial or other sensitive information
5. Fonts, colors, or a different writing style than the sender typically uses

Steps to Prevent Phishing Attacks

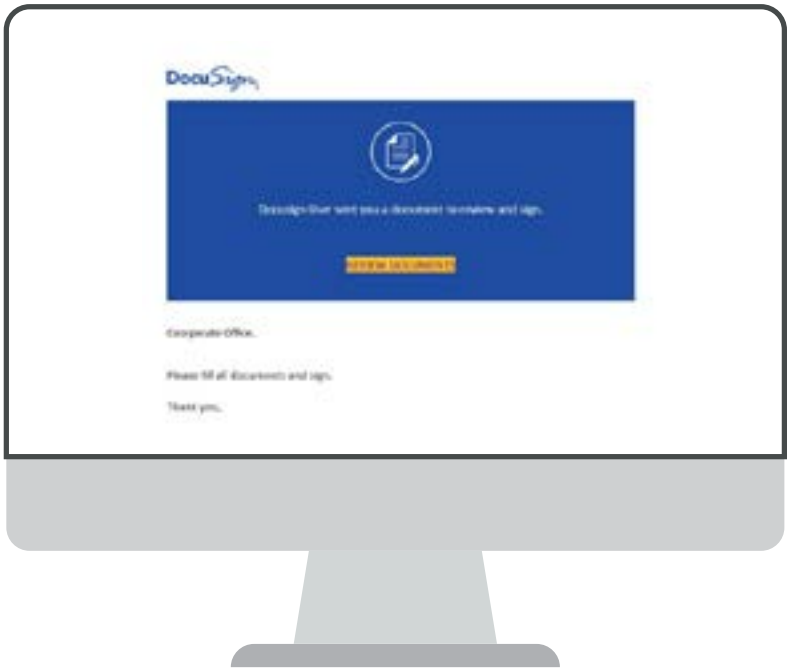
Fortunately, there are simple steps that will keep ransomware off your system if you follow them.

1. A strong spam filter will help eliminate the majority of these attacks. The spam filters can analyze the message before it ever arrives in your inbox and refuse any blatant attacks.
2. A robust antivirus software will scan emails and attachments for any malicious programs or backdoors that may be working to break into your system and steal personal data. (Unfortunately, phishing attacks are getting better at disguising their true identity and intentions and are getting past spam filters and antivirus programs, so these two steps aren't foolproof.)
3. If you get an email from a co-worker or institution that looks suspicious, just give them a call and ask them if the email is legitimate before clicking or downloading any files or replying.
4. Look at the sender email address before opening, and don't rely merely on the sender name that appears in the email. Don't open emails that you aren't sure are legitimate.
5. If you do open an email that you realize is suspicious, don't open any attachments or click on any links.

Examples of Phishing Attacks.

Phishing attempts can take many, many forms. These are just a few different examples we've seen targeted at our customers:

1. Out of Office
2. Office 365 Account Notice
3. Spoofed Email Attacks
4. CEO Impersonation Attacks



3. PHYSICAL THREATS

Not every security threat comes via a computer on your network. Recognizing and protecting against physical threats is just as important to your data security as preventing ransomware and phishing attacks. Physical threats come in three main types: social engineering attacks, USB drive attacks, and stolen devices.

1

Social Engineering Attacks

Social engineering is when an attacker tries to trick you into giving up confidential information over the phone or in person. Attackers will call companies, claiming to be a representative from a government agency, their IT company, or bank, and ask for sensitive information that they can use for criminal purposes.

The best way to defend against these attacks is to train your employees to be suspicious of everyone. Instruct employees not to give out confidential information over the phone. Legitimate institutions will never call and ask for this type of information over the phone. The best way to handle calls that you're unsure of is to hang up and call the institution directly to verify if they called you.

2

USB Drive Attack

Criminals are creative. The USB drive attack strategy is exceptionally clever. It works like this: A criminal will drop an infected USB in your company's parking lot. One of your employees finds the USB drive and picks it up, intending to find its owner. The employee plugs it into his or her computer, hoping to find a name associated with the drive, and malicious software immediately begins installing in the background. Or, weeks later, the employee has forgotten where the USB came from and plugs it into his or her computer to use it.

3

Stolen Devices

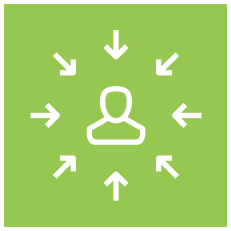
The rise in popularity of small, lightweight tablets, laptops, and smartphones makes it easy for criminals to walk off with sensitive data. The reality is that employees need to take devices home. But there are ways you can protect the data on these devices

One of the best ways to protect yourself is data encryption. Windows (in every version since Vista) includes a product called BitLocker. This product will encrypt the contents of your hard drive so that if your computer is stolen, the thief is required to enter your BitLocker encryption key to unscramble the contents of the hard drive.

Another strategy to consider is implementing policies for automated screen lock, password history, and complexity. Creating complex passwords and entering passwords dozens of times in a day is annoying, but these tactics make it harder for a criminal to take over an unattended workstation or device.

If you use removable storage like USB thumb drives, be sure to encrypt those devices as well. You can also buy products like Kingston's IronKey USB thumb drives, which can be centrally managed and have tamper-proof measures built in.

Mobile device management allows you to set automatic parameters that govern behavior at the device level. These policies can prevent thieves from accessing data once they've stolen a device.



1 Social Engineering Attacks

2 USB Drive Attack

3 Stolen Devices

4

Other Ways to Protect From Physical Threats

Consider how easy it would be for a criminal to access your company's data, network, or devices. Here are a few things to think about:

- How many doors stay unlocked, susceptible to unauthorized access?
- Is your server room locked? Do you have any way of tracking who is going in and out of it?
- Should you consider fingerprint scanners or keycard coded doors that allow your employees to come and go easily but keep criminals out?

4. HUMAN WEAKNESSES

A recent survey from Dell found that, in a variety of circumstances, more than 70% of employees would send out confidential company information. These employees aren't trying to harm the company intentionally – they're simply trying to do their jobs. But they aren't aware of criminal tactics or what behaviors are risky.

Here are the top ways that the Dell survey found employees are susceptible:

43%

They are directed by "management" to perform a task. (A common phishing attack is for a cyber criminal to pretend to be a high-level employee and email lower-level employees asking for a wire transfer or for personnel files.)

37%

They are sharing unencrypted files. Even if the person receiving the files is authorized, unsecured files can be hacked.

23%

They feel the risk is low and the benefit is high.

22%

They believe it will help them do their job more efficiently.

13%

They believe it will help the recipient do their job more efficiently.

Shadow IT

Shadow IT is one of the most common security holes businesses face. It refers to employees using apps and services outside of the control of the IT team. This may not seem like a big deal – so what if the marketing manager is using an image editing software the IT team doesn't know about? The reason it's risky, though, is because if the IT team doesn't know about it, they can't keep it secure.

Again, Shadow IT typically doesn't happen because employees are trying to do something malicious – they're just trying to do their job. But it can leave your company vulnerable.

How to Prevent Cyber Attacks that Target Human Weaknesses

1. The strongest protection against employees who just don't know better is twofold: tools and training. Give your employees the tools they need to do their job effectively and securely. They need access to reliable email and storage. If their job involves handling and sending sensitive data, they need encrypted email.

2. If employees don't have company-approved ways to do something (or if the company approved way is too cumbersome or unreliable), they're going to find some other way to get the job done – a way that may open your company up to a cyber attack.

3. You also need to have clearly outlined policies for how to handle company data. Policies should describe how employees can access company data (approved devices, approved apps, and software, etc.) and how they should interact with company data (rules for sharing, backing up, etc.). Your employees should be trained on all policies, and the policies should be strictly enforced.

4. Your IT team can even set some policies to be turned on and enforced automatically. For example, if you're an Office 365 user, you can implement Data Loss Prevention policies in Outlook and other apps. These tools automatically identify sensitive information (like social security numbers and credit card information) and prevent it from being shared outside of your company.

5. Make data security training part of your new employee onboarding and regularly re-train employees. Your employees are your first line of defense and potentially your biggest weakness. Your employees also need to be trained to use the company-provided tools to do their jobs. Even if you give your employees the best software available to work productively and securely, they're still going to use personal solutions if they don't know how to use what you've provided.

Other protections to consider:

Fortunately, there are simple steps that will keep ransomware off your system if you follow them.

1. Multi-factor authentication – Combining something you know (like a password) with something you have (like a phone app or a keyfob) makes it much harder for an attacker to access information.

2. Encrypted Email – Encrypting your email ensures that it can't be read by third parties.

3. Data Loss Prevention – Data Loss Prevention is a set of policies that allow email communications to be monitored for sensitive material. These rules scan all emails to and from an organization looking for information like credit card numbers, SSNs, Taxpayer Identification Numbers, and Passport numbers.

4. Outbound Internet Monitoring – Monitor your outbound Internet connections to ensure your Internet traffic is going where it should, and not being re-directed to a malicious site or server.

Getting Started

As a small- to mid-sized business, you have limited resources to spend on security. Cybercriminals know this, and they're betting that you've neglected to protect yourself. But with careful planning and creative strategy, you can keep your company secure.

GETTING STARTED

As a small to mid-sized business, you have limited resources to spend on security. Cybercriminals know this, and they're betting that you've neglected to protect yourself. But with careful planning and creative strategy, you can keep your company secure. (Please note: If you're in a regulated industry, especially healthcare, what you need will be a bit different. Reach out to us, and we can help you make sure you stay compliant.)

Essential Equipment

There are a few things you can purchase and install that will go a long way in protecting your data. Here are the essentials.

Firewall – A firewall acts as a gatekeeper between your local network and the Internet. Business-grade firewalls can seem expensive, but consider what you are getting in return: this device scans all traffic coming into and going out of your network from the outside world for threats. Most firewalls offer additional features like web filtering services, anti-virus scanning, and router capabilities. We've covered what to look for in a firewall here.

Encryption – Encryption keeps your data safe if you experience a data breach or if a computer or hard drive is lost or stolen. It scrambles your data so the information cannot be read without an encryption key. If you're using Windows, you probably already have basic encryption software: BitLocker. If you're on a different operating system or if you think you need something more robust, you'll want to consider additional encryption software. If you have specific compliance requirements, like HIPAA, you will also need to get encryption for email.

Backups – Data backups can save your business if you fall victim to a cyber attack. Even if you pay the fee to a ransomware criminal, there's no guarantee you'll get your files back. With a robust backup system, you'll only lose files created after your last backup, and you won't have to pay the ransom. In addition to data security, backups protect you from data loss due to natural disasters or accidentally deleted files.

Training

As we mentioned earlier, employees can be your weakest link or your first line of defense when it comes to data security. Onboarding training and regular re-training will help employees remember the best practices of data security. Giving your employees the knowledge and tools they need to do their job securely is one of the best ways to protect your company from attacks.

It's also a good idea to regularly test your employee's security knowledge to identify any holes in their awareness. This testing will help you know where to focus your training.

Training and testing should never be used as punishment, though. Punishing your employees for falling victim to an attack isn't going to make them less likely to fall victim to an attack in the future – but it may make them less likely to report it.

Essential Tips

The basics are easy to overlook, but following them will prevent the majority of cyber attacks. Here are the do's and don'ts.

1. **Don't use the same password(s) for multiple accounts.** No one likes looking up passwords they can't remember or having to reset because a password has been lost. But using the same password means a hacker only needs to figure out one password to access all of your accounts.

2. **Use long, complex passwords with letters, numbers, and special characters**. Don't use references to things that a hacker could guess or find elsewhere, like a favorite food, your address, phone number, or date of birth.

3. **Don't enter your password on an unsecured WiFi network**. Hackers troll for passwords being entered on WiFi networks in public locations.

4. **Regularly back up your data and make sure it's easy to restore**. The best backups offer mirroring of your server, so nothing is lost.

5. **Don't open an email attachment or click on a link from an unknown sender**. And even if you know the sender, be cautious. There is always a chance someone you know has been compromised.

6. **If you're shopping online, double check the URL of the site before you buy**. It's also smart to check that the site is secure (to do this, click on the lock on the toolbar).

7. **Don't share your passwords, even with coworkers**. If a coworker needs to access your computer when you aren't there, change your password afterward.

8. **Don't store your passwords in an unsecured location.** If you need to store passwords somewhere, use a secure password manager like LastPass or 1Password.

9. **Keep all the software and operating systems on your computer, phone, and tablet up to date**. Yes, it can be annoying to have to restart your computer when an update is available, but these updates usually contain essential security patches.

10. **Lock your computer when you walk away from it**. Your IT company can implement a security policy to lock your computer during idle time after a set amount of time, but it's a good idea to get into the habit of locking the minute you step away.

11. **Use malware prevention programs to check your computer for malware**. Regularly run scans, so you're protected against the latest threats

HOW TO SAVE MONEY

It can be tempting to try to save money by going to a big box retailer and getting equipment meant for personal use. But you'll be better protected if you spend a little more money for business grade equipment. Firewalls meant for personal use just can't handle the same amount of traffic as a commercial grade firewall and will result in slow Internet speeds that hamper productivity, reducing profitability in the long run.

If you're working with an outsourced IT company, get them involved in choosing equipment. They'll be able to help you pick the best firewall and backup solutions for your network and your budget. A lot of IT companies already have relationships with vendors and can get equipment at a discounted rate that you won't have access to yourself.

Firewalls are now available in a firewall-as-a-service option with low monthly pricing. This is often an attractive option for budget-conscious business owners. (PTG customers have this option as part of our SecuritySuite, which includes firewall and monitoring services).

HOW TO BOOST SECURITY EVEN FURTHER

Once you've got the basics in place, you may want to think about boosting your security even further. There are additional apps, add-ons, and steps you can implement to take security to the next level.

A Mobile Device Management – Whether you're giving your employees cell phones to use for work or have a Bring Your Own Device (BYOD) policy, employees are likely using mobile devices to access company information (like email and sensitive line-of-business applications). You need a mobile device policy to protect your data in the event an employee's phone is lost or stolen. Policies can be set at the device level and should include requirements like setting a passcode, storing passwords in an encrypted password vault, and preventing devices from being "jailbroken".

Multi-Factor Authentication – Authentication is a method of proving you are who you say you are. It can take several forms, including a password or PIN code, an RSA token or smart card, or a fingerprint or retinal scanner. Multi-factor authentication is simply using more than one of these methods for access. It dramatically increases protection. Want to see it in action? Watch this on-demand webinar about multi-factor authentication.

Advanced Threat Protection – Advanced Threat Analytics (ATA) is an add-on to Office 365 that detects suspicious activity and prevents malicious attacks from hitting your network. It combines the typical analysis that happens with security products (such as anti-virus) with machine learning. So over time, it actually gets smarter. Because it can identify normal behavior and irregular behavior, ATA can help target potential security issues earlier in the process. One of the most valuable services that ATA provides is email protection.

Data Loss Prevention – Microsoft provides another feature called Data Loss Prevention. This feature is essentially a set of policies that Office 365 provides that allows the organization to monitor email communications for sensitive material. Once turned on, these rules scan all emails to and from an organization looking for information like credit card numbers, SSNs, Taxpayer Identification Numbers, and passport numbers.

HOW TO MANAGE IT

Cybersecurity is serious and can be complex, so you need a skilled expert with experience to manage your system for you. This expert can be an internal person who's been trained and has managed security for other companies in the past, or you can outsource security management to an expert team. Cybersecurity is serious and can be complex, so you need a skilled expert with experience to manage your system for you. This expert can be an internal person who's been trained and has managed security for other companies in the past, or you can outsource security management to an expert team.

Traditionally, data security has been treated as a capital expense. Even if they're regularly updated, firewall and antivirus programs have only been purchased and thought about every few years. But because cyber threats are advancing and evolving quickly, companies are now shifting security to business operations, which not only keeps the business safer but also makes budgeting easier.

The best way to achieve this switch is to use a monthly security-as-a-service plan (some options are called firewall-as-a-service). Look for a monthly security plan that rolls multiple security expenses, like firewall, antivirus and monitoring into one to get the most bang for your buck. PTG offers a security-as-a-service plan called SecuritySuite – a comprehensive, single security solution made from the best industry solutions and administered by our support experts. The service includes:

1. **Secure firewall** with 24/7 software updates and annual hardware replacements, so you're always protected
2. Cloud-based, robust **antivirus software and web security software** scans in real time to keep you protected without affecting performance
3. **Email configuration** services with optional encryption to lessen the chance of malicious emails reaching your inbox
4. **Real-time monitoring** of outbound Internet connections, making sure you're actually going where you think you're going online, and not to a malicious site

Wrapping It Up

Data security can seem intimidating due to the potential risks involved if it isn't done right. But SMBs have more security tools and options available today than ever before. Smaller companies don't need to dedicate large budgets to get the security they need. Putting best practices in place and providing your people with the tools and training they need will go a long way in protecting your business.

ABOUT PTG

Palmetto Technology Group (PTG) is an outsourced IT company in Greenville, SC. We take the guesswork and frustration out of IT by working with businesses to help them align their technology to meet business goals. Want to learn more about how can we can help boost productivity and make your business more secure? Visit our website or read some of our Success Stories.

PTG

www.GoPTG.com

Info@GoPTG.com