Ntiva
Managed IT & Cloud Services

The Essential Cybersecurity Toolkit

Everything You Need to Know to Keep Your Data Safe

7900 Westpark Drive, Suite A100
McLean, VA 22102

1-888-996-8482 | www.ntiva.com

THE ESSENTIAL CYBERSECURITY TOOLKIT

CYBERSECURITY: technologies, processes and practices designed to protect networks, computers, programs and data from attack, damage or unauthorized access.

In a report from AT&T, 62% of businesses acknowledged they experienced some sort of a cyber attack. In 2017, these incidents have become even more common. For today's companies, falling victim to one of these attacks is no longer a question of "if" but "when."

Today's employees are connected to the Internet all day every day, communicating with colleagues and stakeholders, sharing critical information and jumping from site to site. With hackings, data breaches and ransomware attacks on the rise, it is essential for all companies to plan for the worst, with mandatory cybersecurity trainings for all employees and with the recommended solutions for mitigating the risks.

Today's data threats don't discriminate; businesses of all sizes are susceptible to attacks. However, small to medium-sized businesses (SMBs) – both commercial and nonprofit – are often less prepared to deal with security threats than their larger counterparts. The reasons for this vary from business to business, but ultimately it comes down to the fact that SMBs often have less resources to devote to cybersecurity efforts.

This ebook contains practical advice and easy tips for training employees on cybersecurity and industry best practices with real-world examples. We also outline the essential solutions designed to help today's businesses defend against and recover from a cybersecurity incident. There has never been a better time for this guide!

According to over 1,700 IT service providers, the lack of cybersecurity awareness amongst employees is a leading cause of a successful ransomware attack against an SMB.

CYBERSECURITY TRAINING FOR EMPLOYEES

According to over 1,700 IT service providers, the lack of cybersecurity awareness amongst employees is a leading cause of a successful ransomware attack against an SMB. That being said, employee training is a top component of a successful cybersecurity protection program and most likely the only way to ensure all staff understand the cyber threats they face and, most importantly, what they should look for in order to avoid falling victim to them.

Cyber Scams 101

From 2016-2017, nearly one million U.S. businesses fell victim to ransomware, resulting in an estimated eleven million hours of downtime.

At the root of the majority of ransomware attacks is the tactic of social engineering, leveraged by hackers, which involves manipulating a person or persons in order to access corporate systems and private information. Social engineering plays into human nature's inclination to trust. For cyber criminals, it is

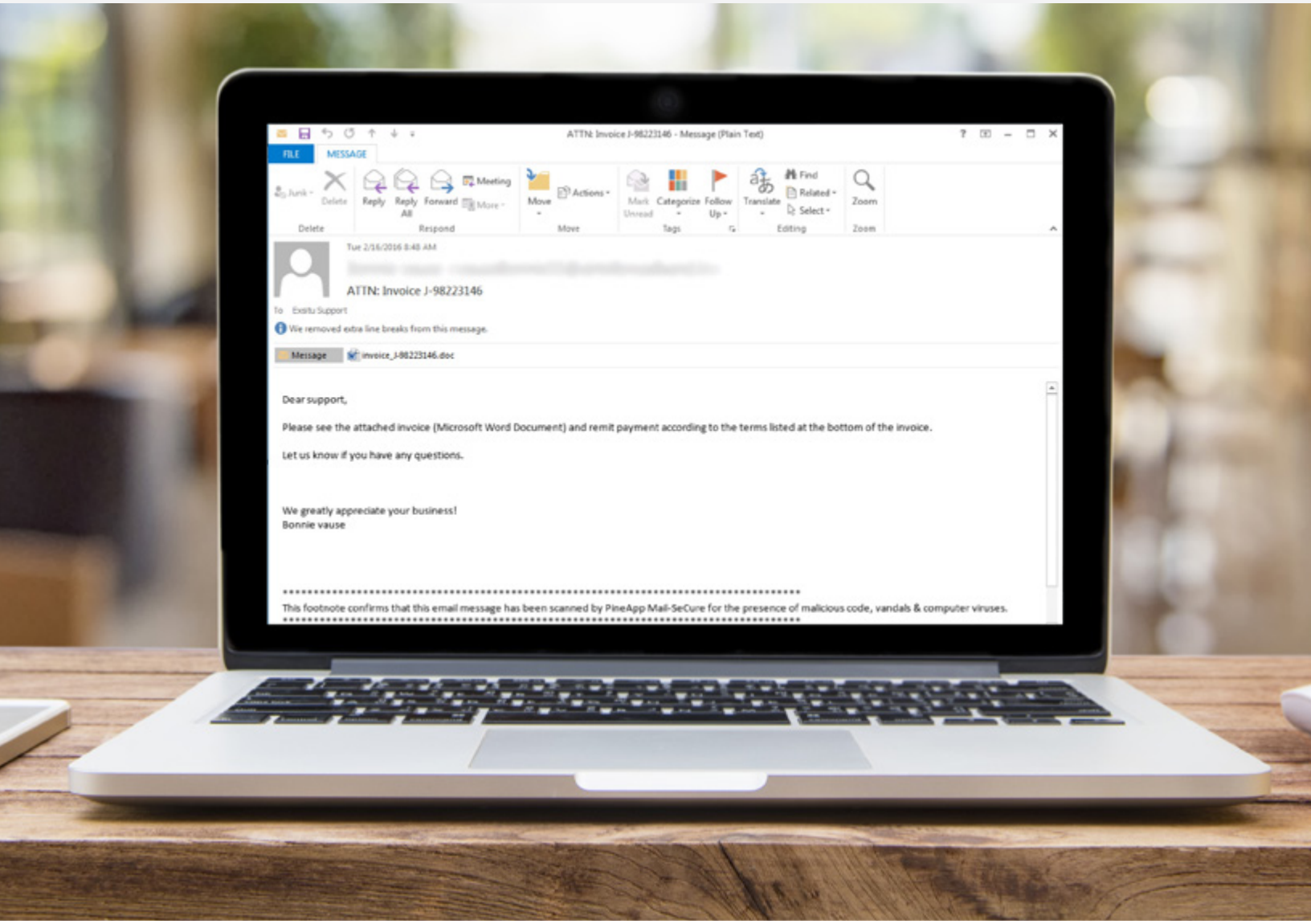
the easiest method for obtaining access to a private corporate system. After all, why would they spend the time trying to guess someone's password when they can simply ask for it themselves?

Let's help employees help themselves. Below is a quick and dirty overview of today's most common and effective social engineering scams. This is the list to hand employees on their very first day. Why not include it in their "Welcome" packet? If they don't know these leading hacker tactics, they WILL fall for them.

5 Types of Social Engineering Scams to Know:

1. **Phishing**
   Phishing is the leading tactic leveraged by today's ransomware hackers, typically delivered in the form of an email, chat, web ad or website designed to impersonate a real system and organization. Often crafted to deliver a sense of urgency and importance, the message within these emails often appears to be from the government or a major corporation and can include logos and branding.
2. **Baiting**
   Similar to phishing, baiting involves offering something enticing to an end user in exchange for private data. The "bait" comes in many forms, both digital, such as a music or movie download, and physical, such as a branded flash drive labeled "Executive Salary Summary Q3 2016" that is left out on a desk for an end user to find. Once the bait is taken, malicious software is delivered directly into the victim's computer.
3. **Quid Pro Quo**
   Similar to baiting, quid pro quo involves a request for the exchange of private data but for a service. For example, an employee might receive a phone call from the hacker posed as a technology expert offering free IT assistance in exchange for login credentials.
4. **Pretexting**
   Pretexting iis when a hacker creates a false sense of trust between themselves and the end user by impersonating a co-worker or a figure of authority within the company in order to gain access to private data. For example, a hacker may send an email or a chat message posing as the head of IT Support who needs private data in order to comply with a corporate audit (that isn't real).
5. **Tailgating**
   Tailgating is when an unauthorized person physically follows an employee into a restricted corporate area or system. The most common example of this is when a hacker calls out to an employee to hold a door open for them as they've forgotten their RFID card. Another example of tailgating is when a hacker asks an employee to "borrow" a private laptop for a few minutes, during which the criminal is able to quickly steal data or install malicious software.

TAKEAWAY:
Employee awareness of social engineering is essential for ensuring corporate cybersecurity. If end users know the main characteristics of these attacks, it's much more likely they can avoid falling for them. As many of us are visual learners, make sure to provide them with actual examples of these scams.

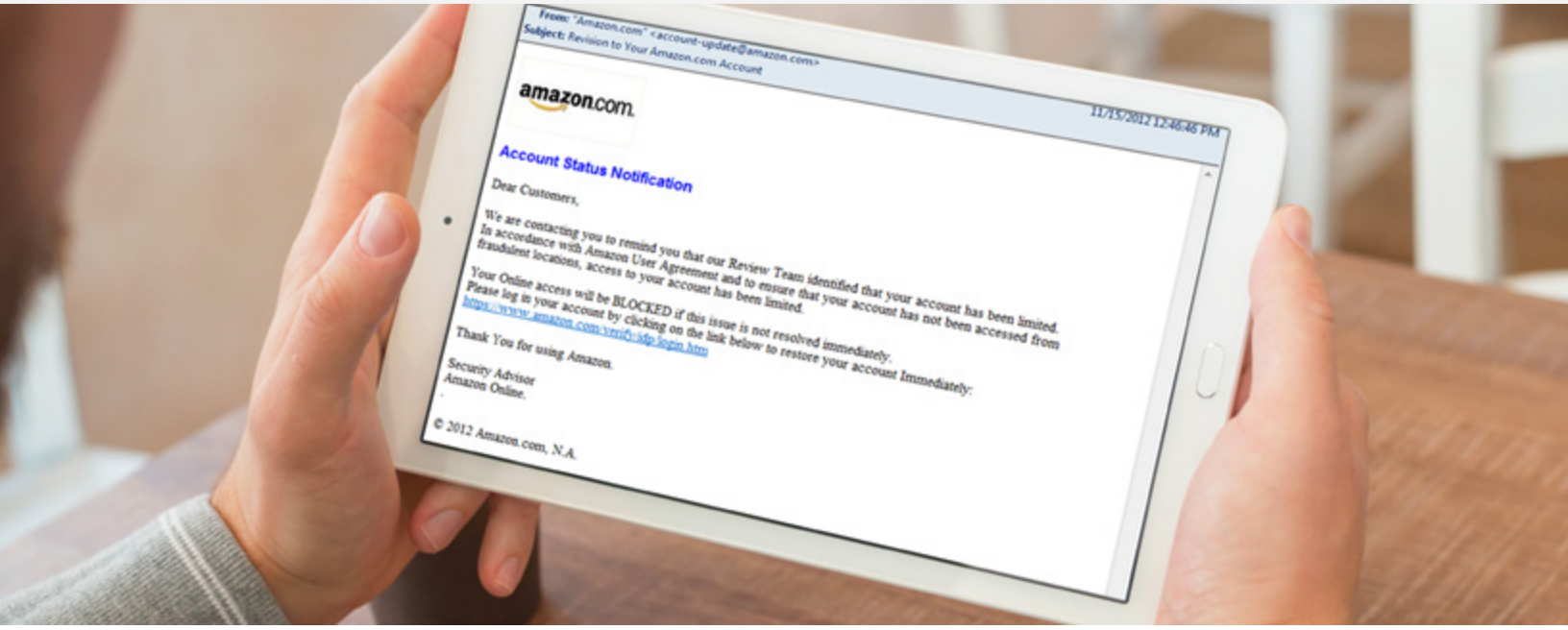


How to Spot a Cyber Scam

Inbox Scams

The above image is a prime example of a phishing email used to spread Locky, a common strain of ransomware. To the recipient, the email appears to come from a business partner asking the reader to "see the attached invoice" by clicking on the attached Word doc. Note how harmless this email appears and how easy it would be for a user to absentmindedly open and click, an action that would result in an instant ransomware infection. It happens every single day.

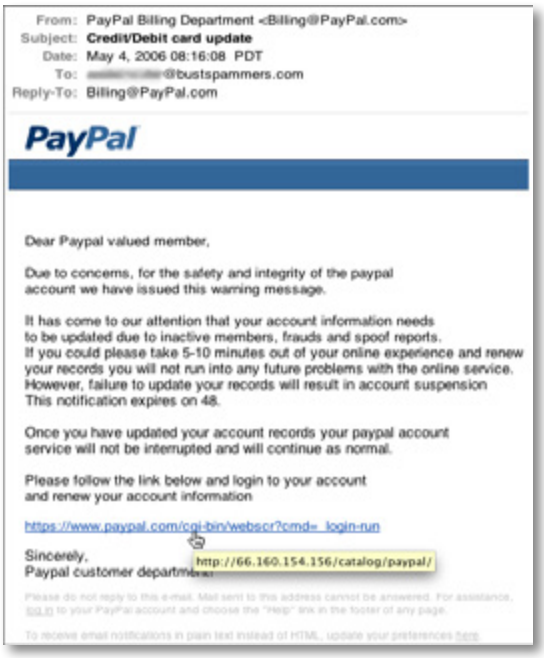
TAKEAWAY:
Ensure all employees are wary of any email containing an attachment they aren't expecting, especially if said attachment is a Microsoft Office file. Before clicking on anything, make sure they confirm with the sender (via phone, text, separate email) what it is before opening or clicking anything.



Above is another example of an email scam, which appears to be an official notice from Amazon.com and lures the reader to click a link rather than an attachment, but with the same business-crippling results.

In the image to the right, note the link appears to direct the reader to a legitimate PayPal web page and yet, when the mouse is hovered over the link, you see that it actually directs to a different site designed to inject malware or illegally collect personal information.

RED FLAGS: Missing sender or recipient information, generic greetings, misspelled email addresses (i.e., billing@amzaon.com), and email addresses that don't match the company name. Any emails that ask the recipient to download a form or macro in order to complete a task are highly suspicious and an employee should NOT click on anything. Instead, report the email to IT immediately.



TAKEAWAY: An email from a retailer is probably suspicious if the recipient has not made recent purchases from said site. Employees who receive this type of email should be instructed NOT to click anything. Instead, they should type the URL into a browser, login to their account and check for notifications there. Report any phishing emails to IT or your MSP and, most importantly, DO NOT CLICK!

Malicious Websites and Malvertising

Malicious websites and malvertisements are designed to look like a page or ad on a legitimate website. These sites can look incredibly real, featuring branding and logos, which is why so many end up giving cyber criminals their personal information or access to directly inject malware onto their systems. Typically, hackers will insert code into a legitimate site which redirects unsuspecting users to their malicious site. Above, you'll find an example of a malicious page that was designed to look like a page on Chase Bank's site.

TAKEAWAY: Be certain that employees understand this risk and embrace safe browsing habits, making sure they are accessing sites using the HTTPS secure communication protocol and being wary of any site asking for private information. Also, show employees how to check URLs that links point to (by hovering mouse over the link to reveal the complete URL in the status bar at the bottom of the browser).

Pop Ups

Another common lure is a pop-up that claims that a user's computer has been locked by the FBI because it was used to access illegal material such as child pornography, as you will see in the example above. The lure instructs users to click a link in order to pay a fine, which is bogus.

RED FLAGS: Links that redirect to a different domain, pop-ups that require you to enter personal information, misspelled URLs, and URLs with unusual domain extensions. This type of attack can be very hard to detect, even if employees are highly vigilant. This is why it is very important to deploy business-class malware detection software—which we will cover in detail in the next section of this ebook.

TAKEAWAY: Be certain that employees understand this type of cyber scam is designed to prey upon human fear of breaking the law. Instruct employees who encounter this type of pop up NOT to click. Instead, they should restart the computer in safe mode. Still there? Get IT (or your MSP) involved.

SETTING UP A CYBERSECURITY TRAINING PROGRAM

The cybersecurity training schedule you choose, will be dictated by the specific nature of your business and the systems, software and hardware you leverage. However, a good start would be ensuring that all new employees receive training as part of their orientation and all employees receive training on a bi-annual basis. It is important to have a formalized plan in place to keep security front of mind and employees informed about new threats.

While formal training is important, informal training can be very effective as well. Point staffers to blogs on key security topics, ask them to take an online cybersecurity quiz, print out and post funny IT security memes around the office, etc. Do whatever it takes to keep people aware and following safe browsing practices. If you don't have resources to put this type of training together, talk with your IT service provider and see if they can assist with educational materials or plans.

ESSENTIAL CYBERSECURITY SOLUTIONS FOR SMBS

Here's one thing the cybersecurity world can agree on: there is no single product available today that will solve all of your cybersecurity problems. In today's world, it takes many technologies and processes to provide comprehensive risk and security management. Instead, SMBs should continually be checking their systems for vulnerabilities, learning about new threats, thinking like attackers and adjusting their defenses as needed.

Must–Have Solutions for Cyber Protection: Layered Security

Antivirus Software

Cybersecurity technology starts with antivirus software. Antivirus, as its name implies, is designed to detect, block, and remove viruses and malware. Modern antivirus software can protect against ransomware, keyloggers, backdoors, rootkits, trojan horses, worms, adware, and spyware. Some products are designed to detect other threats, such as malicious URLs, phishing attacks, social engineering techniques, identity theft, and distributed denial-of-service (DDoS) attacks.

Firewalls

A network firewall is also essential. Firewalls are designed to monitor incoming and outgoing network traffic based on a set of configurable rules—separating your secure internal network from the Internet, which is not considered secure. Firewalls are typically deployed as an appliance on your network and in many cases offer additional functionality, such as virtual private network (VPN) for remote workers.

Patch Management

Patch management is an important consideration as well. Cyber criminals design their attacks around vulnerabilities in popular software products such as Microsoft Office or Adobe Flash Player. As vulnerabilities are exploited, software vendors issue updates to address them. As such, using outdated versions of software products can expose your business to security risks. There are a variety of solutions available that can automate patch management.

Password Management

Recent studies have reported that weak passwords are at the heart of the rise in cyber theft, causing 76% of data breaches. To mitigate this risk, businesses should adopt password management solutions for all employees. Many people have a document that contains all of their password information in one easily accessible file—this is unsafe and unnecessary. There are many password management apps available today. These tools allow users keep track of all your passwords, and if any of your accounts are compromised you can change all of your passwords quickly. Encryption is also an important consideration. Encrypting hard drives ensures that data will be completely inaccessible, for example if a laptop is stolen.

These measures protect against a wide array of cyber attacks. However, because threats like ransomware are always evolving, security solutions are just one part of an effective defense strategy. You also need solutions in place that enable you to return to operations quickly if you do suffer a cyber attack. Data protection technologies are an essential second layer of defense against cyber crime.

The #1 Solution for Cybersecurity Protection:

Backup and Recovery

Taking frequent backups of all data considered critical to your business is critical. The exact frequency of backups will vary based on your business' specific needs. Traditionally, most businesses took a daily backup, and for some businesses this may still be suitable. However, today's backup products are designed to make incremental copies of data throughout the day to minimize data loss. When it comes to protecting against cyber attacks, solutions that back up regularly allow you to restore data to a point in time before the breach occurred without losing all of the data created since the previous night's backup.

Some data protection products can take image-based backups that are stored in a virtual machine format—essentially a snapshot of the data, applications, and operating system. This allows users to run applications from the backup copy. This functionality is typically referred to as instant recovery or recovery-in-place. The ability to run an application from the backup instance of a virtual machine allows users to continue working while the primary server is restored following an outage, dramatically reducing downtime. Some solutions extend this capability to the cloud to protect against failures which impact primary and onprem backup copies, as well.

CYBERSECURITY CHECKLIST

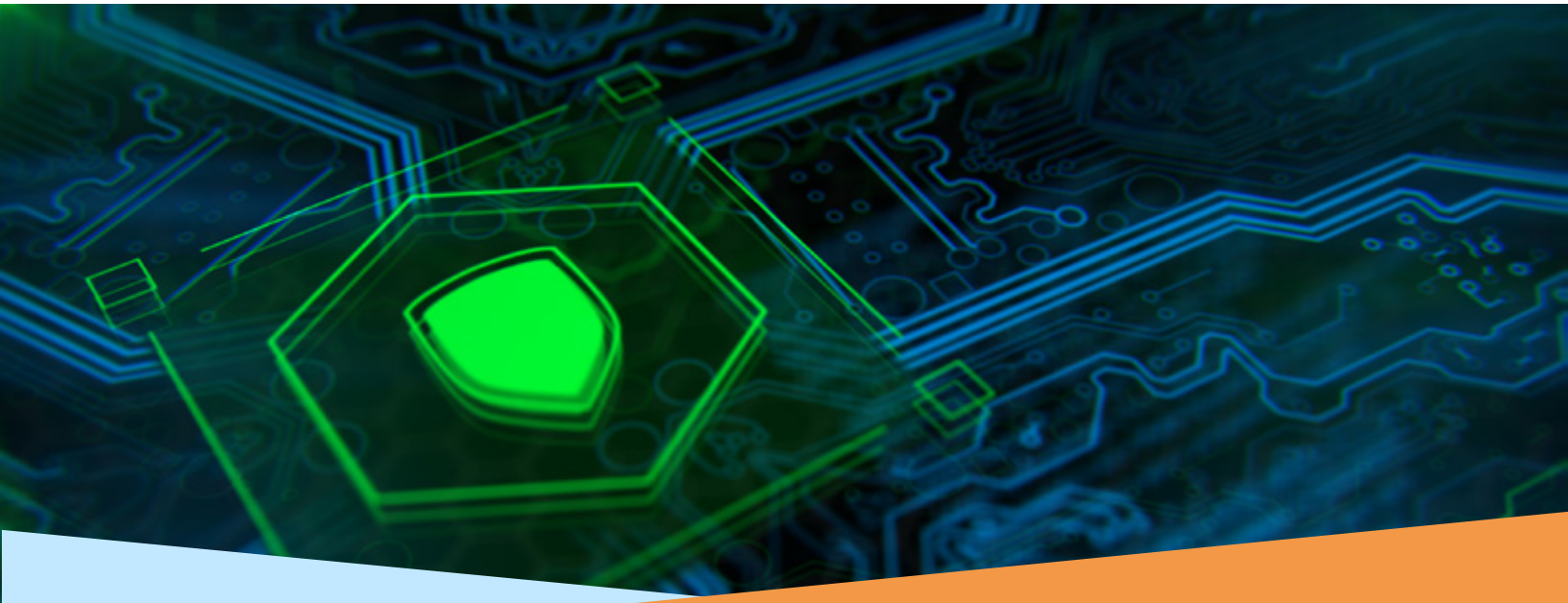
According to a recent SEC report, SMBs are the "principal target" of cyber attacks. Use this checklist to be sure your critical business data is protected.

- ✔ **Conduct a security risk assessment.** Understand potential security threats (e.g., downtime from ransomware) and the impact they may have on your business (lost revenue). Use this information to shape a security strategy that meets your specific needs.
- ✔ **Train your employees.** Because cybersecurity threats are constantly evolving, an ongoing semi-annual training plan should be implemented for all employees. This should include examples of threats, as well as instruction on security best practices (e.g., lock laptops when away from your desk). Hold employees accountable.
- ✔ **Protect your network and devices.** Implement a password policy that requires strong passwords that expire every 90 days. Deploy firewall, VPN and antivirus technologies to ensure your network and endpoints are not vulnerable to attacks. Consider implementing multifactor authentication. Ongoing network monitoring should also be considered essential. Encrypt hard drives.
- ✔ **Keep software up to date.** It is essential to use up-to-date software products and be vigilant about patch management. Cyber criminals exploit software vulnerabilities using a variety of tactics to gain access to computers and data.
- ✔ **Create straightforward cybersecurity policies.** Write and distribute a clear set of rules and instructions on cybersecurity practices for employees. This will vary from business to business but may include policies on social media use, bring your own device, authentication requirements, etc.
- ✔ **Back up your data.** Daily backups are a requirement to recover from data corruption or loss resulting from security breaches. Consider using a modern data protection tool that takes incremental backups of data periodically throughout the day to prevent data loss.
- ✔ **Enable uptime.** Choose a modern data protection solution that enables "instant recovery" of data and applications. Application downtime can significantly impact your business' ability to generate revenue.
- ✔ **Know where your data resides.** Maintaining oversight of business data is an important piece of the security puzzle. The more places data exists, the more likely it is that unauthorized individuals will be able to access it. Avoid "shadow IT" with business-class SaaS applications that allow for corporate control of data.
- ✔ **Control access to computers.** Use key cards or similar security measures to control access to facilities, ensure that employees use strong passwords for laptops and desktops. Administrative privileges should only be given to trusted IT staff.

CONCLUSION

Cyber crime is growing at a rapid rate and businesses are increasingly targeted. According to the National Small Business Association, 44% of small businesses have been the victim of a cyber attack and the number of breaches reporter per year continues to climb. A recent Juniper Research study estimates that cyber crime will cost businesses $2.1 trillion globally by 2019, increasing by almost 4X the cost of breaches in 2015.

Developing a robust, multi-layered cybersecurity strategy can save a business. Ongoing employee education and security technology will boost your front line of defense and dramatically decrease the likelihood of any breaches. Lastly, a solid, reliable backup and recovery solution is the second and most essential layer of defense, allowing businesses to quickly recover unscathed should things turn ugly.



ABOUT NTIVA

Ntiva is a trusted Managed IT and Cloud services provider that offers IT services and support to businesses of all types, building and maintaining infrastructure, securing networks, and providing strategic technology expertise. Our team of world-class talent genuinely cares about the relationships we build and understands that response and precision are fundamental keys to a successful partnership. Ntiva's ultimate objective is to help our clients leverage their technology investments to improve their overall business performance.