prosource Technology Solutions

CYBER SECURITY TOOLKIT FOR SMBs

Everything you need to know to proactively keep your data safe

totalprosource.com | 888.698.0763

Table of Contents

Introduction

In a 2015 report from AT&T, 62% of businesses acknowledged they experienced some sort of a cyber attack.[1] In 2017, these incidents have become even more common. For today's companies, falling victim to a cyber attack is no longer a question of "if" but "when".

Cyber security is the technologies, processes, and practices designed to protect networks, computers, programs, and data from attack, damage, or unauthorized use.

Employees are connected to the Internet all day every day, communicating and sharing critical information with colleagues and customers. Today's data threats affect businesses of all sizes; however, small to medium-sized businesses (SMBs) are often less prepared to deal with security threats due to lack of resources towards cyber security efforts. With hackings, data breaches, and ransomware attacks on the rise, it's essential for all businesses to plan for the worst. This ebook contains practical advice and easy tips for training employees on cyber security best practices, as well as an outline of essential solutions designed to defend businesses against and recover from a cyber attack.

5 Types of Social Engineering Scams

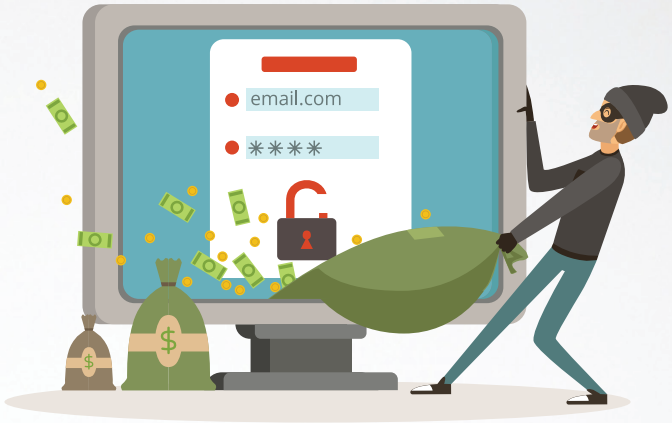
Phishing: a leading tactic leveraged by ransomware hackers where an attacker masquerades a reputable entity or person in email or another communications channel. Attackers utilize link shorteners or embed links that redirect users to suspicious websites in URLs that appear legitimate. Once redirected, threats, fear, and sense of urgency are used in attempt to manipulate the user into sending personal information.

Baiting: this scam involves offering something enticing to an end user in exchange for private data. Baiters may offer users digital rewards such as free music or movie downloads if they surrender their credentials to the site. Physical bait may include a branded flash drive that is left out on a desk for the user to find. Once the flash drive is inserted into the computer, malicious software is delivered directly into the victim's computer.

Quid Pro Quo: involves a request for the exchange of private data for a service. One common attack involve fraudsters who impersonate IT service people who offer IT assistance to their victims. They request the victim to facilitate the operation by disabling the AV software on their computer to install an "upgrade" or "software" which is really a malicious application.

Pretexting: attackers focus on creating a false sense of trust between themselves and the end user by impersonating someone else to obtain private information. Attackers rely on building a false sense of trust with the victim by creating a credible story that leaves little room for doubt from their victim.

Tailgating: involves an unauthorized person physically following an employee into a restricted area. One common scenario is when the attacker simply walks in behind a person who is authorized to access the area. Another example is when a hacker asks an employee to hold the door open for them as they've forgotten their access card, giving the hacker access to building.



What is Social Engineering?

The success of social engineers relies solely on the hackers' ability to exploit the one weakness that is found in every company – human psychology. Social engineering is a term that encompasses a broad range of malicious activity and uses a variety of media, including phone calls and social media, to trick people into offering them access to sensitive information.

How to Spot Common Cyber Scams

Inbox Scams

Phishing and scam emails are becoming harder to spot and more frequent. Malicious scam emails try to trick you into installing viruses on your computer so it's important to not click any links or open any attachments. Tips for recognizing inbox scams include:

- Bad grammar, typos, and/or unnatural syntax
- Lack of or improper use of official letterhead and/or logos
- Instructions to click a link or verify and/or reactivate accounts
- Demands for passwords or other sensitive information

Fraudulent emails have been sent out claiming to be from PayPal. The official looking message sent by scammers attempts to get the recipient to click on a malicious link. The email begins by warning the recipient that someone is using their PayPal account without their knowledge, claiming that there has been recent activity on their account from a suspicious location. The email requests the recipient to click on a link to login and confirm their account.

Inbox Scam Takeaways & Red Flags

Ensure all employees are wary of any email containing an attachment they aren't expecting. Before clicking on anything, confirm with the sender via phone, text, or separate email what it is before opening or clicking anything.

An email from a retailer is probably suspicious if the recipient hasn't made a recent purchase. 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.

Missing sender or recipient information, generic greetings, misspelled email addresses (i.e. billing@paipal.com), and email addresses that don't match the company name should be cause for concern of malicious activity. Any emails that ask the recipient to download a form to complete a task are highly suspicious. All suspicious emails should be reported to IT.

PayPal™ PayPal™

Important : We noticed unusual activity in your PayPal account

What's going on ?,

We're concerned that someone is using your PayPal account without your knowledge. Recentactivity on your account seems to have occurred from a suspicious location or under circumstances that may be different than usual.

What to do ?

Log in to your PayPal account as soon as possible. We may ask you to confirm information you provided when you created your account to make sure you're the account holder. We'll then ask you to Confirm your password and security questions. You should also do the following for your own protection:

Confirm Your Account Now

Log in to confirm your account

PayPal Inbox Scam Example

In the PayPal example above, if the recipient clicked on the link in the email it would take them to a fake login site that was built to steal user's credentials and security answers.

How to Spot Common Cyber Scams
Malicious Websites & Malvertising

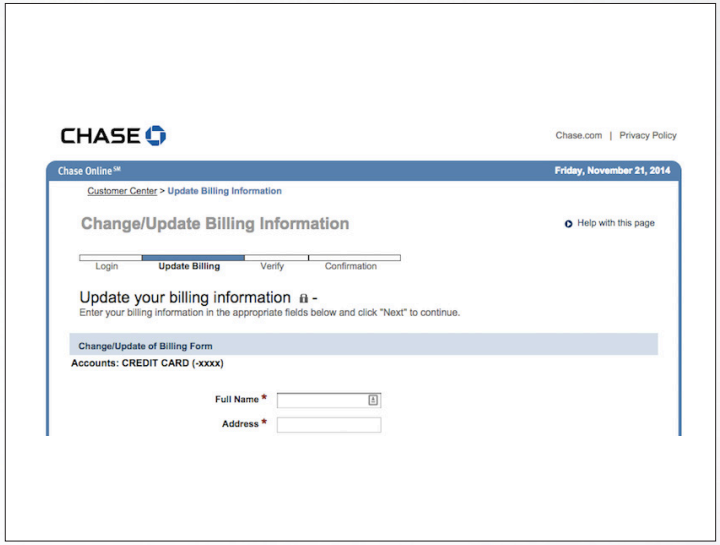
Malicious websites are designed to look like a page or ad on a legitimate website, and these sites can look incredibly real. Cyber criminals often utilize branding and logos, which is why users may easily fall victim and give cyber criminals their personal information or access to install malware onto their systems. To accomplish the redirect to a malicious site, hackers insert code into a legitimate site which redirects unsuspecting users to their malicious site. Tips for recognizing malicious websites and Malvertising include:

- Poor spelling, unprofessional imagery, and/or bad grammar
- Links that redirect to a different domain
- Misspelled URLs
- URLs with unusual domain extensions
- Unsecured sites that start with "http" – all secure sites start with "https://"

Malvertising increased by 132% in 2016 over 2015.[2] The increased sophistication of programmatic advertising technology has introduced powerful, highly accurate profiling capabilities which cyber criminals leverage across every link in the advertising delivery chain to target precise groups of users.

Malicious Websites & Malvertising Takeaways & Red Flags

Educate employees about the risk and practice safe browsing habits, making sure employees are accessing sites using the HTTPS secure communication protocol and being skeptical of any site asking for private information. Train employees how to check URLs that links point to – hover your mouse over the link to reveal the complete URL in the status bar at the bottom of the browser.



Malicious Website Scam Example

In the Chase Bank example above, cyber criminals created a malicious page that was designed to look like a page on Chase Bank's website to collect user information.

How to Spot Common Cyber Scams
Pop Ups

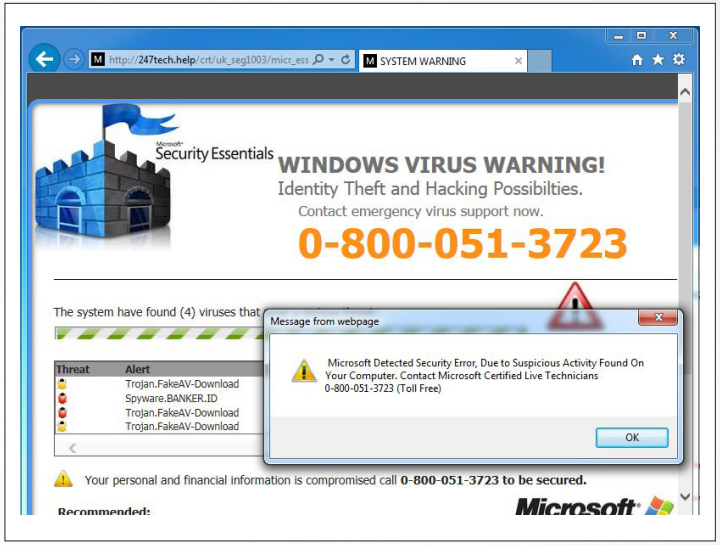
A fake pop up is a form of Internet fraud that implements social engineering and fear tactics to get the user to take the action the cyber criminal is requesting. Fake pop ups are designed to extort the victim to get their money as well as install malware to gain access to personal information. Tips for recognizing a fake pop up include:

- Poor spelling, unprofessional imagery, and/or bad grammar
- Links that redirect to a different domain
- Misspelled URLs
- URLs with unusual domain extensions
- Pop ups that require you to enter personal information

One common pop up scam is your web browser being redirected to sites that display tech support alerts, asking you to call a support number to fix your device. These fake tech support alerts are shown in a way that trick the user into thinking their computer has crashed or that a virus has been detected on the computer. The message displayed attempts to scare the infected user into calling one of the listed numbers to receive support. If the number is called, the person on the other end tries to sell the victim unneeded support contracts and services. The scammer may attempt to get the victim to allow remote access into their computer, and at that point personal information is stolen.

Pop up Scam Takeaways & Red Flags

Companies will never send unsolicited email messages or make unsolicited phone calls to request personal or financial information or fix your computer. Treat all unsolicited phone calls or pop ups with skepticism and never provide your personal information.



Pop Up Scam Example

In the Microsoft example above, a pop up was generated appearing to be from Microsoft stating that the user's computer had a virus. The user was instructed to call a number to get the error corrected.

Cyber Security Education for Employees

#1: Regularly talk to employees about cyber security

In 2016, the average data breach size was 29,611 records, and the number of breach reports per typical incident ranged from 5,125 to 101,520.[3] Your employees can be your strongest line of defense or your weakest link, so it's important to explain the potential impact a cyber attack may have on your business operations.

#2: Don't forget to educate top management & IT staff - they're employees too

Top managers are often targeted because they have access to more business-critical information, IT bends the rules for them, and the damage can be much bigger if successfully attacked. IT staff members have unlimited power and control over the network which makes the IT team more susceptible to an attack.

#3: Explain that a system is only as secure as the weakest link

Employees remain the weak link in business data protection, and careless or unaware employees are most likely to be victim of a cyber attack. According to EY's 19th Global information Survey 2016-17, 74% of the 1,735 global executives, information security managers, and IT leaders surveyed said that careless employees are the most likely source of a cyber attack.[4] It's important for employees to know their susceptibility to phishing tactics, and the financial, operational, and brand impact they impose on employers. Educating employees on their vulnerability will help reduce the frequency and severity of a cyber attack.

#4: Explore different types of cyber attacks with employees by conducting regular, focused sessions

While big data breaches such as Yahoo, Target, Home Depot, and Sony receive high volumes of public attention, data breaches have become commonplace and remain a real and growing financial threat to businesses of all sizes. The average cost of a data breach in North America for SMBs is currently $117,000.[5]

Mitigate Risk With Training

According to over 1,700 IT service providers, the lack of cyber security awareness amongst employees is a leading cause of a successful ransomware attack against a SMB.[6] Training employees on cyber threats they face and what they should look for to avoid falling victim to an attack is the main component of a successful cyber security protection program.

It's important to integrate cyber security training within your new hire onboarding activities and to regularly talk to employees about different types of cyber attacks throughout the year. Whether in lunch and learn format or another format, trainings should include specific rules for email, Web browsing, mobile devices, and social networks. Include basic cyber security preventative measures, including: physically unplugging your computer from the network, notifying your administrator of suspicious emails or unusual activity, and/or if you lose your mobile device.

#5: Warn employees to watch for social engineering activities

Social engineering threats are widespread, and while there's no guaranteed way to defend against them, half the battle is recognizing the methods they use. Employee awareness of social engineering is essential for ensuring corporate cyber security. If end users know the main characteristics of these attacks, it's much more likely they can avoid falling for them.

#6: Train employees to recognize an attack

Create and enforce policies that assume you'll be attacked – don't wait to react. Have a documented remediation plan in place and update or review it frequently to make sure your policies are up-to-date. Clearly communicate a step-by-step action plan about what to do if employees believe they have received a cyber threat. In-depth training regarding routine and new types of phishing is recommended, so make sure you have clear cyber security policies that are strictly enforced.

#7: If an incident happens, let your employees know as soon as possible

A lack of transparency or improper handling of a cyber incident may significantly increase the impact of the event. If there has been a data breach, let your employees know immediately. Be prepared with instructions on how they can help minimize the impact of the breach. In your communication with employees, be open and honest and provide information you know at the time. In the hours and days immediately following the attack, communicate frequently with your employees. Even if there is no new information to share, inform them that you are working diligently to repair the issue. Give talking points to mid and lower level managers and leaders so they can communicate with their teams about the issue as well.

Vigilance is Key to Protection

Your employees are one of your biggest assets. Making sure they are aware of types of cyber attacks, internal cyber security policies, and what to do if they are attacked is important to keep your business secure and/or minimize the effect of a security breach.

Layered Security Key to SMB Cyber Protection

Antivirus Software

Cyber security technology starts with antivirus software. Antivirus is designed to prevent, search for, detect, and remove software viruses and other malicious software like ransomware, keyloggers, backdoors, rootkits, trojan horses, worms, adware, and spyware. It's critical for users to have antivirus installed and up-to-date because a computer without anti-virus software installed will be infected within minutes of connecting to the Internet.

Firewalls

A network firewall is essential to cyber protection. Firewalls are designed to monitor incoming and outgoing network traffic based on a set of rules, acting as a barrier between a trusted network and an untrusted network. It controls access to the resources of a network through a positive control model – meaning that the only traffic allowed onto the network is defined in the firewall policy.

Patch Management

Cyber criminals design their attacks around vulnerabilities in popular software products such as Microsoft Office and Adobe Flash Player. Patch management involves acquiring, testing, and installing multiple patches (code changes) to an administered computer system. As vulnerabilities are exploited, software vendors issue updates to address them – using outdated versions of software products can expose your business to security risks.

Password Management

Weak passwords are a leading cause to a cyber threat. To mitigate this risk, businesses should adopt password management solutions for employees. Many people store a document on their computer that contains all their site login credentials which is unsafe and unnecessary. Password management apps should be used in place of a stored password document on your computer.

Why Layered Security

Using only one security program will leave security flawed and the computer at risk for other threats. To keep your computer's security protection high, you'll need more than one program working to protect your computer. Layered security refers to security systems that use multiple security programs to protect your computer. These security programs work together, providing a layered protection to keep your business safe from cyber attacks.

Disaster Recovery & Business Continuity

Disaster Recovery

Frequently backing up business data is critical to your business, and the frequency of data backups will depend on your business's needs. Today's backup products are designed to make incremental copies of data throughout the day to minimize data loss. Regular backups protect your business against cyber attacks by allowing you to restore data to a point in time before a breach occurred without losing all data.

Disaster recovery is an area of security planning that aims to protect an organization from the effects of a disaster and allows organizations to maintain or quickly resume business-critical functions following a disaster. Unlike business continuity, disaster recovery solutions involve restoring IT infrastructure and accessing copies of data stored off-site. A disaster can be anything that puts a business's operations at risk, including a cyber attack, equipment failures, natural disaster, and others.

Business Continuity

Business continuity refers to the processes that businesses have in place to ensure that normal business operations can continue during a disaster. This plan provides uninterrupted access to data during a time of crisis and involves making sure that network connections, online systems, phones, network drives, servers, and business applications run without downtime. With risks ranging from cyber attacks to natural disasters to human error, it is critical for an organization to have a business continuity plan to decrease the chance of a costly outage. Unlike disaster recovery, which is data-centric, business continuity is business-centric.

Summary

Business continuity is the first defense against a disaster; however, disaster recovery is vital for businesses that cannot function without critical data. Outages are common and to ensure full business and data protection in the event of a disaster, businesses must adopt both disaster recovery and business continuity plans.

Mitigate Risk With Training

Business comes to a grinding halt when infrastructure fails, so it's important to have disaster recovery and business continuity plans in place. Disaster recovery and business continuity plans are closely related, but each play a unique and important role in a business's contingency planning. They are designed to work together and are often implemented at the same time following an outage.

Cyber Security Checklist

According to Datto's Global Ransomware Report, ransomware costs small businesses around $8,500 an hour, totaling over $75 billion per year.[7] With ransomware evolving into a full-fledged cyber security epidemic, a lack of employee training can be a disastrous combination. Use this checklist to ensure 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 cyber security 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 to be vigilant about patch management. Cyber criminals exploit software vulnerabilities using a variety of tactics to gain access to computers and data.

- [ ] **Create straightforward cyber security policies.** Write and distribute a clear set of rules and instructions on cyber security 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.

- [ ] **Backup 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, and ensure that employees use strong passwords for laptops and desktops. Administrative privileges should only be given to trusted IT staff.

Intelligent Business Continuity with VaultIT

Backup and recovery is not enough in today's technology environment. Cyber criminals, hackers, viruses, malware, ransomware, hardware failures, and natural disasters put your data even more at risk. You need a high availability business continuity solution that mitigates risk and eliminates downtime. Prosource's VaultIT is your intelligent business continuity system – off-site backup, instant data recovery, and full server virtualization.

Why Traditional Backups Don't Work

- Days or weeks to recover data after disaster
- High risk of human error due to manual administration
- Difficult to test if backup is working properly
- Physical to virtual conversions time consuming with high failure rates
- No redundant backups in multiple locations; high risk for original backup systems to be destroyed

The Prosource Advantage: VaultIT Intelligent Business Continuity

- Downtime after disaster reduced to hours, minutes, or seconds
- Automated backup process
- Automated screenshots taken & reported to ensure successful backups
- Inverse Chain Technology™ avoids broken backups chains, virtualization happens instantaneously
- Allows businesses to run off a secure cloud, stored at redundant data centers in event of disaster
- AES 256 and SSL key-based encryption ensures data is safe and meets industry regulations

VaultIT Features & Benefits

Each backup is automatically tested and a screenshot taken to ensure its success.

All backup data points can be virtulazied, restored, and deleted at any time.

Data is encrypted in transit and in the cloud. On-site hardware can optionally be encrypted.

Convert backups into a running system, a virtual server, in just minutes.

References

1. The CEO's Guide to Cyberbreach Response, AT&T Cybersecurity Insights, Volume 3
https://www.business.att.com/cybersecurity/docs/cyberbreachresponse.pdf

2. RiskIQ's 2016 Malvertising Report, RiskIQ
https://www.riskiq.com/infographic/riskiqs-2016-malvertising-report/

3. 2017 Cost of Data Breach Study, Ponemon Institute
https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=SEL03130WWEN&

4. The Weakest Link in Your Cyber Defenses? Your Own Employees, Forbes.com
https://www.forbes.com/sites/eycybersecurity/2017/03/20/the-weakest-link-in-your-cyber-defenses-your-own-employees/#3287c09a5d51

5. Cyber Attacks Cost U.S. Enterprises $1.3 Million on Average in 2017, CSO
https://www.csoonline.com/article/3227065/security/cyber-attacks-cost-us-enterprises-13-million-on-average-in-2017.html

6. Global State of the Channel Ransomware Report, Datto
https://www.datto.com/blog/report-dattos-global-state-of-the-channel-ransomware-report

7. Global State of the Channel Ransomware Report, Datto
https://www.datto.com/blog/report-dattos-global-state-of-the-channel-ransomware-report