EBOOK

3 Ways To Improve Your CYBERSECURITY POSTURE

Although important, cybersecurity is more than setting up a firewall and antivirus solution. Your employees are connected to the Internet every day, sharing critical information and jumping from site to site.

Small and medium-sized businesses (SMBs) are often less prepared to deal with cybersecurity threats than larger businesses because they typically have fewer resources to devote to this effort. Unfortunately, falling victim to a cyberattack is no longer a question of "if" but "when."

SMBs are a primary target for hackers. In the last five years there's been steady increase in attacks targeting SMBs — And in the past 12 months, 50% of all SMBs have been breached.

So, what is cybersecurity? Cybersecurity refers to preventative methods used to protect information from being stolen, compromised or attacked. It requires an understanding of potential information threats, such as viruses and other malicious code. Cybersecurity strategies include identity management, risk management and incident management.

What to do? You must be vigilant. With hackings, data breaches and ransomware attacks on the rise, you must plan for the worst. This requires the use of technologies, processes and practices that are designed to protect your networks, computers, programs and data from an attack, damage or unauthorized access.

The lack of cybersecurity awareness amongst employees is a leading cause of a successful ransomware attack against an SMB.

1. Employee Cybersecurity Training

Data breaches aren't always about bad people doing bad things. Many are the result of good employees making mistakes. If they aren't properly trained to recognize a cyber threat, your network and business are vulnerable.

Make sure they know how to keep your company's data safe by avoiding common dangers like opening attachments from unknown senders, improperly disposing of sensitive information, or using simple passwords.

Implement mandatory cybersecurity training for all your employees and teach them how to mitigate risks. This is the best way to ensure your staff understands the cyber threats they face and what to do to keep from falling victim to them. It will help them from being manipulated into exposing your private information.

Every employee should participate in this training — And you should hold refresher courses, as threats are constantly changing.

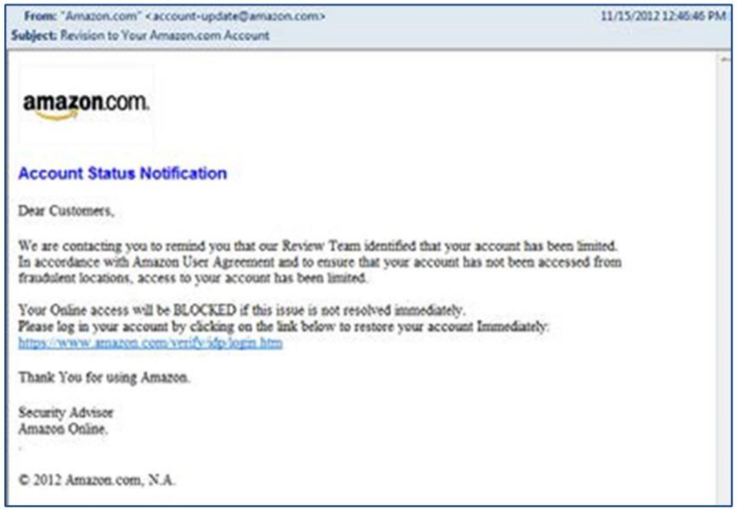
A good start would be to ensure all new employees receive this training as part of their orientation, and that all your employees receive training twice a year so they're informed about new threats. If you don't have the expertise to do this training, talk

Teach Your Employees About These Common Scams

Phishing: This is the leading tactic leveraged by today's hackers. It's typically delivered in the form of an email, chat, web ad or website designed to impersonate a real organization. Phishing attacks manipulate employees into clicking malicious links where they're asked to provide login credentials. 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.

Similar to fishing in a lake or river, phishing is tech language for fishing over the Internet for confidential information. Phishing uses link manipulation, image filter evasion and website forgery to fool your employees into thinking that a spoofed website is genuine and legitimate. Fortunately, phishing victimization is preventable. The following security precautions are recommended and should be taught to your employees:

- Always use updated computer security tools, such as anti-virus software, spyware and firewall.
- Never open unknown or suspicious email attachments.
- Never divulge confidential information requested by email.
- Double check the website URL to make sure it's legitimate by typing the actual address in a Web browser.
- Verify the website's phone number before placing any calls to the phone number in the email.



From: "Amazon.com" <account-update@amazon.com> 11/15/2012 12:46:46 PM
Subject: Revision to Your Amazon.com Account

amazon.com

Account Status Notification

Dear Customers,

We are contacting you to remind you that our Review Team identified that your account has been limited.
In accordance with Amazon User Agreement and to ensure that your account has not been accessed from fraudulent locations, access to your account has been limited.

Your Online access will be BLOCKED if this issue is not resolved immediately.
Please log in your account by clicking on the link below to restore your account Immediately:
https://www.amazon.com/verify/idp/login.htm

Thank You for using Amazon.

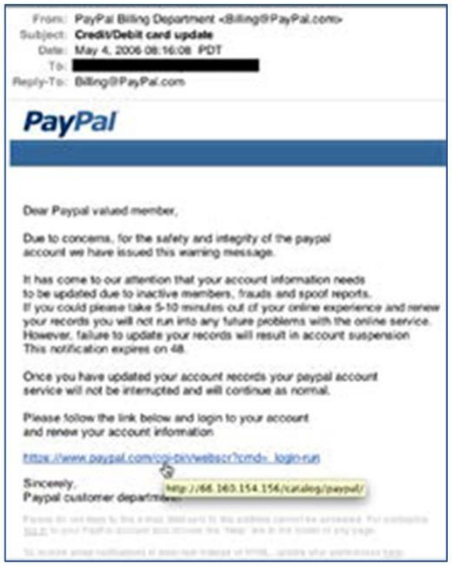
Security Advisor
Amazon Online.

© 2012 Amazon.com, N.A.

Above is an example of an email scam. *Note these 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.

Baiting: Similar to phishing, this offers something enticing via email to your employees in exchange for confidential data. The "bait" can come in both digital and physical forms, such as a movie download, or a flash drive labeled "Executive Salary Summary Q3 2017" that's put on an employee's desk. Once they take the "bait," the malicious software is delivered to their computer. The strongest defense against baiting is educating your team.

Quid Pro Quo: Similar to baiting, quid pro quo attacks promise a benefit in exchange for information. This benefit is usually service such as free IT assistance in exchange for login credentials. Or, the criminal will promise a quick fix in exchange for your employee disabling their anti-virus program so a "software update" can be installed (where the update is actually malware).



From: PayPal Billing Department <Billing@PayPal.com>
Subject: **Credit/Debit card update**
Date: May 4, 2006 08:16:08 PDT
To: [redacted]
Reply-To: Billing@PayPal.com

Dear Paypal valued member,

Due to concerns, for the safety and integrity of the paypal account we have issued this warning message.

It has come to our attention that your account information needs to be updated due to inactive members, frauds and spoof reports. If you could please take 5-10 minutes out of your online experience and renew your records you will not run into any future problems with the online service. However, failure to update your records will result in account suspension This notification expires on 48.

Once you have updated your account records your paypal account service will not be interupted and will continue as normal.

Please follow the link below and login to your account and renew your account information

https://www.paypal.com/cgi-bin/webscr?cmd=_login-run

http://68.160.154.156/catalog/paypal/

Sincerely,
Paypal customer department

This link above 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

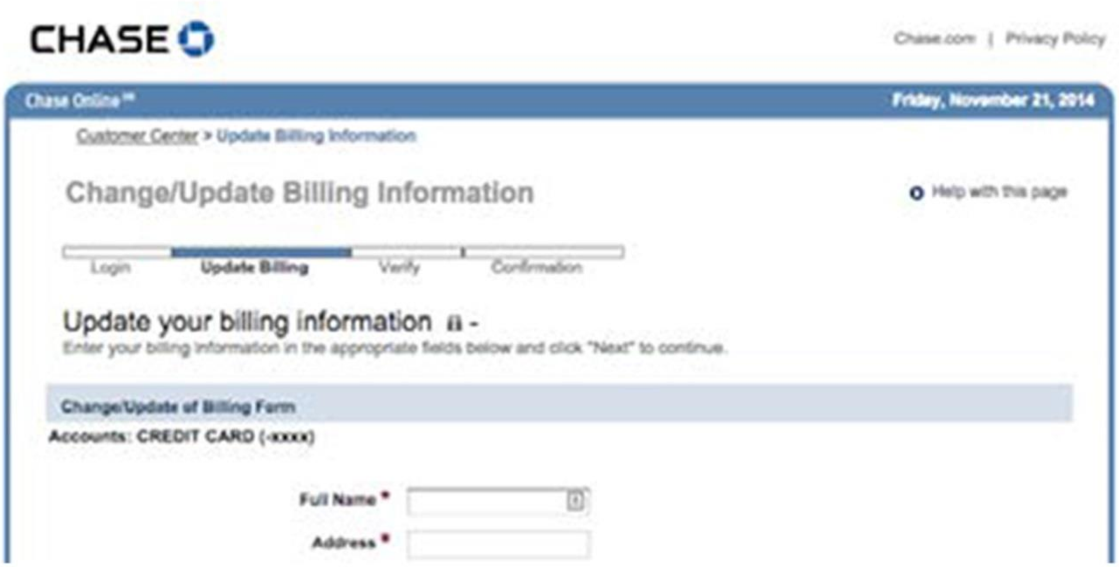
Pretexting: Pretexting is another form of social engineering where criminals create a good pretext, or a fabricated scenario, to steal their victims' confidential information. The hacker tries to create a false sense of trust with your employee to gain access to private data. They may send an email or text message posing as the head of IT Support, and saying they need the employee's private data to comply with a corporate audit.

Tailgating: This occurs when someone who lacks the proper authentication follows your employee into a restricted area. They may pose as a delivery person who needs entry to drop off a package. When your employee enters, the criminal asks them to hold the door open for them to gain access to your facility. Another example of tailgating is when a criminal asks your employee to "borrow" their private laptop for a few minutes. The criminal then steals data or installs malicious software on the laptop.

Employee awareness of social engineering scams is essential for ensuring cybersecurity.

Malicious Websites and Malvertising: Cybercriminals design malicious websites and malvertisements to look like a page or ad on a legitimate website. They look real, and contain branding and logos from the company. However, they also contain malware that can get downloaded into your employees' computers.

Here’s an example:


CHASE
Chase.com | Privacy Policy
Chase Online℠
Friday, November 21, 2014
Customer Center > Update Billing Information
Help with this page
Login
Update Billing
Verify
Confirmation

Change/Update Billing Information

Update your billing information

Enter your billing information in the appropriate fields below and click "Next" to continue.

Change/Update of Billing Form

Accounts: CREDIT CARD (-xxxx)

Full Name *

Address *

Make sure your employees use safe browsing habits. Any site they access should have an HTTPS secure communication protocol. Teach them to check URLS by hovering their mouse over the link to reveal the complete address in the bar at the bottom of their browser.

Pop Ups: This is another common scam. It claims that your computer has been locked by the FBI because you accessed an illegal site. Your employee will be asked to click a link to pay a fine. Tell them not to do this!

More Tips to Share with Your Employees.

- The IRS and Department of Revenue (DOR) won't contact you by email to request confidential or financial information. Nor will they will send text messages, use social media channels or call you with threats of lawsuits or arrests.

- Any emails that ask the you to download a form or macro in order to complete a task are highly suspicious and you shouldn't click on anything. Instead, report the email to IT immediately.

- Always be vigilant and be skeptical. Never open a link or attachment from an unknown or suspicious source. If it's from a known person, still proceed with caution. Cybercriminals are skilled at mimicking trusted business associates.

- Make sure you're using up-to-date security software to protect against malware and viruses. Some security software can help identity suspicious websites that are used by cybercriminals.

- Use strong passwords for your online accounts. Use a unique password for each account. By using the same password repeatedly, you'll give criminals access to multiple accounts if they get your password.

- Use multi-factor authentication when offered. Two-factor authentication means in addition to entering your username and password, you'll have to enter a designated code that's been sent as a text to your phone.

- When in doubt, don't open an email. Contact the sender to determine if it's legitimate.

2. Employ a Layered Cybersecurity Solution

There's is no one product today that will solve all of your cybersecurity issues. It takes a combination of technologies and processes to ensure the security of your business and data. Developing a robust, multi-layered cybersecurity posture can save your business.

Antivirus/Anti Malware

Cybersecurity technology starts with antivirus software. It's designed to detect, block, and remove viruses and malware. The right solution can protect against ransomware, keyloggers, backdoors, rootkits, trojan horses, worms, adware, and spyware. Some of these can even detect other threats like malicious URLs, phishing attacks, social engineering techniques, identity theft, and distributed denial-of-service (DDoS) attacks.

Firewalls

A network firewall is essential for your complete cybersecurity. They monitor incoming and outgoing network traffic based on a set of configurable rules. They separate your secure internal network from the Internet, which isn't secure. Firewalls are typically used as a separate appliance on your network. They can also provide additional functionality, such as virtual private network (VPN) for remote workers.

Some attacks can be very hard to detect, even if your employees are highly vigilant. This is why it's very important to deploy business-class cybersecurity

Patch Management

Vulnerabilities in popular software products such as Microsoft Office or Adobe Flash Player can provide a way for cybercriminals to get into your computers and network. Software vendors issue patches and updates to address these as they occur. Using outdated versions of software exposes your business to cybersecurity risks. There are a variety of solutions available to automate your patch management.

Password Management

Weak passwords cause 76% of data breaches. It's essential that you adopt password management solutions for all your employees. There are many password management applications that you can use. They'll help your employees keep track of all your passwords, and if any of your accounts are compromised you can change all of your passwords easily and quickly.

Encryption

This is also important to do. By encrypting your hard drives, you can ensure your data will be completely inaccessible. This is especially important if a laptop is stolen.

Ask Your IT Provider To:

Conduct vulnerability assessments. This will help you identify potential security threats.

Provide ongoing training for your employees in cybersecurity tactics. Threats are constantly evolving. This requires up-to-date training from professionals.

Protect your network and devices with an up-to-date, layered solution. They can deploy firewalls, VPNs and antivirus technologies to ensure your network and endpoints aren’t exposed to attacks. Ask them to encrypt your hard drives as well.

Keep your software up to date and deploy automated patch management solutions. This keeps cyber criminals from exploiting software vulnerabilities.

Help you create effective, written cybersecurity policies. A set of rules and instructions on cybersecurity practices for employees is highly recommended.

3. The #1 Cybersecurity Protection Is Backup and Recovery

You also need to return to operations quickly if you suffer a cyberattack (or disaster of any kind). Data protection technologies are an essential layer of defense against cybercrime.

Executing frequent backups of all your data is critical for the survival of your business. The frequency of backups will vary based on your unique needs. Most use daily backups, however today’s backup solutions are designed to make incremental copies of your data throughout the day. This is the best way to prevent data loss. This allows you to restore data to a point in time before the breach occurred without losing all of the data created after the previous night’s backup.

The best data protection products take image-based backups. This is like a snapshot of the data, applications, and operating system. With this type of backup, you can run applications from the copy. This is referred to **as instant recovery or recovery-in-place.** The ability to run an application from your backup lets you continue working while the primary server is restored. Some solutions also provide this via the cloud to protect against failures that occur in

Ensure you effectively back up your data. Daily or incremental backups are a requirement to recover from data loss resulting from security breaches.

Enable uptime with a solution that enables "instant recovery" of data and applications. Application downtime can significantly impact your business' ability to generate revenue.

Identify where your data resides. Maintaining oversight of business data is key to cybersecurity.

Control access to computers, with key cards or other security measures.

Deploy a Ransomware Protection and Recovery Solution to identify a ransomware attack, and roll systems back to a point in time before the attack hit.

In Summary

Cybercrime is growing at a rapid rate and small businesses are increasingly being targeted. With ongoing employee education, a layered security solution, and a reliable backup and recovery solution you'll boost your defense posture and decrease the likelihood that a data breach will take down your business.

For more information, or assistance establishing a strong cybersecurity posture for your business, contact Nachman Networks in Northern Virginia at: (703)600-3301 or sales@nachnet.com