CYBERSECURITY

Best Practices for Business Owners

Bank of Marin

Cybersecurity is a critical topic for business owners.

Each year, millions of cyberattacks cripple businesses with significant loss of revenue and reputation. The vast majority of these incidents could be avoided through simple approaches to improving security.

Bank of Marin is here to help. This guide offers business owners an introduction to the various types of cyber incidents that can occur and how to prevent them.

Please contact your local Bank of Marin branch with any questions on how we can help protect your business from fraud and cyberthreats.

Bank of Marin

Building a Culture of Security

The world of cybercrime is ever-evolving, so be prepared to be ever-evolving with your company's security posture. You can help protect your business from cyberthreats by understanding some basic guidelines and putting them into practice. Start by creating a culture of security that includes training your employees on best practices for document and data management and employing experienced IT resources to build a secure online environment for your business.

1 Train your staff how to protect your computing environment and information.

- Provide the right training and information for employees to understand how to protect your business online.
- Ensure that employees be vigilant (suspicious) with all email links/attachments and website links. This is the most common mode of attack by cybercriminals.
- Update employees frequently as you learn about new risks and vulnerabilities.
- Review network access of employees and grant access on a least privilege basis.

2 Require strong passwords and change passwords frequently.

- Current best practice is to use long passwords that include a requirement for numbers, symbols, and upper- and lower-case letters. Consider the use of password management software, where effective passwords can be automatically generated for you.
- Ensure that passwords cannot be reused
- Direct employees not to share passwords by phone, text or email.
- Limit the number of unsuccessful log-in attempts to help eliminate password-guessing hacks.

3 Look to implement the current cybersecurity technologies that will help mitigate the latest types of cyberattacks.

4 Have a plan to respond to a data breach.

- To manage through a data breach, your plan should include how to notify customers and save data while continuing to run the business.
- To protect your business from a data breach, the Federal Trade Commission's (FTC) "Data Breach Response: A Guide for Businesses" is a good resource.

Cybersecurity Requires Strong Physical Security

While we think of cybersecurity as taking measures to protect ourselves online, lapses in physical security can expose sensitive company information to identity theft. This includes losing a flash drive that contains confidential information, throwing away financial records into an exterior trash bin without shredding them, or leaving building windows unlocked where files or computers can be stolen.

Protect your physical information

- Maintain only the files and data you need.
- Store paper files or electronic devices in a locked cabinet or password-protected room.
- Limit physical access to records or devices containing sensitive data.
- Encourage a clean desk culture and remind employees to put paper files in locked file cabinets, log out of the network and applications frequently, and never leave files or devices with sensitive data unattended.
- Keep track of who has access to devices that collect sensitive customer information.

Train your employees on the importance of physical security

- Always shred documents with sensitive information before throwing them away.
- Don't rely on the 'delete' function to remove files. This action alone does not remove the file from a computer.
- Before discarding or donating old computers, mobile devices, digital copiers and drives, ensure data is erased correctly using appropriate software.
- Promote consistent security practices for employees working at any location, whether working from home, the road or a different office.
- Know what to do in the event equipment or files are lost or stolen. Ensure employees know the plan, including whom to notify and what to do next.

Cybersecurity Requires A Strong Computing Environment

Protect your computing environment and information

- Regularly update your software. This is a simple yet important way to protect your business. Setting your system to update automatically makes it easy to stay vigilant.
- Ensure your files are secure. It's best to back up important files on an external hard drive or in the cloud.
- Encrypt all devices. It is important to encrypt any device or media containing sensitive personal information. This includes laptops, tablets, smartphones, removable drives, backup tapes and cloud storage solutions.
- Add more protection for sensitive information. In addition to requiring passwords, multi-factor authentication is an extra step that can provide added security for areas of your network that contain sensitive information. Examples include requiring a temporary code on a smartphone or a key that's inserted into a computer to obtain access.

Protect your wireless network

- Secure your router
- Once the router is set up, it is important to change the default name and password, turn off remote management and log out as the administrator.
- Ensure that your router has WPA2 or WPA3 encryption and that it is turned on.

Consider these cybersecurity technologies to help mitigate risks

- Anti-malware/anti-virus software for endpoints (identifies and cleans malware and viruses from endpoints like workstations and servers)
- Web-filtering services (that block malicious/undesirable websites from computer users)
- Email filter services (that remove/identify malicious emails and/or malicious links/ attachments in emails)
- Network and endpoint firewalls (help block malicious internet or network traffic from workstations and servers)
- Password managers (which help users support good password creation and use habits)
- Cloud backup services (help businesses attain proper protection schemes against data loss)

Understanding different types of cyberthreats and how to protect against them

What is ransomware?

Ransomware threatens to publish data or block access to it unless a ransom is paid. Often a ransomware attack begins with what looks like a “real” email containing a link or attachment that someone clicks on or opens. This simple email hack can link downloaded software that freezes your network, holding your data – and your company – hostage. The cybercriminals ask for money or cryptocurrency in exchange for releasing your data or files, which they often don’t do even with payment. As a result, sensitive data about your customers, employees and your business can be at risk in criminal hands. Ransomware attacks are unfortunately quite common and can take a serious toll on your business.

There are a few ways criminals can start an attack, including:

- Sending scam “phishing” emails that contain infected links and attachments. Often these emails look like they are from a vendor or someone you know. They may ask that you click on a link to update your account or even ask for your network password. When clicked on, these can spread viruses that attack or freeze your network.
- Malware, which is malicious software automatically downloaded onto a computer to infect websites.
- Server vulnerabilities can also be pinpointed and exploited by online hackers.
- Online ads - even on websites you know and trust - can include malicious code which when clicked on can potentially infect your system or steal data.

How to avoid ransomware attacks:

- **Educate your staff about phishing scams.** Share the following tips for spotting and protecting against ransomware in ongoing trainings and new employee orientation:
  - An email or text includes a link and asks for your password, bank account information or other sensitive data.
  - It looks real. It's easy to create logos and make up fake email addresses.
  - It requires an immediate response. Look out for messages that pressure you into acting urgently or something bad will happen.
- I**f you don't trust the sender or the request for information, check it out.** Look up the website or person behind the email or text, and make sure you are getting the real company. Make a call if you're not sure to confirm that they really need the requested information. And, use a number you know to be correct – not just the number provided in an email or text.
- **Make data backup an ongoing part of your routine business operations.**
- **Ransomware attacks can sometimes go undetected for days or weeks.** Make sure your backup strategy incorporates periodic backups that would allow pulling files from several periods of dates and times.
- **Stay up to date on security best practices.** Be on the lookout for the latest means of protection, like email authentication and intrusion prevention software.
- **Perhaps most importantly, create a plan for how you would keep your business up and running after a ransomware attack.** Train your employees about the plan and share it with everyone who needs to know.

If your business is attacked:

- **Work quickly to limit the damage,** including disconnecting the infected computer(s) or devices from your network. Notify those who have been affected if your data has been stolen.
- **Contact the authorities right away** (police, FBI).
- **Notify your customers or other affected parties immediately** as they could be at risk for identity theft.
- **Implement your business recovery plan.** Having data backed up will help.
- **Alert coworkers.** Phishing attacks often happen to more than one person in a company. It is helpful to talk to your colleagues and share your experience, so it doesn't happen to others.

Protecting against business email impostors

In addition to phishing scams, businesses also need to be on the lookout for email impostors. These spoofers send out messages to your customers or partners that seem to come from your company. Their intent is to secure passwords and bank account information or get someone to send them money. This puts businesses at risk in several ways, including losing the trust of their customers who may be affected by this scam.

There are several important ways to protect your business from email impostors:

- **Configure your email solution to enable email authentication.** With email authentication, you can configure your company's email system to allow other companies to confirm that an email from you actually came from your company's server.
- **Keep your security up to date.** Always install the latest patches and updates and set them to update automatically on your network. Additional means of protection, such as intrusion prevention software, checks your network and sends alerts of any suspicious activity.
- **Train your staff.** The importance of ongoing training and sharing tips with employees about how to avoid scams and protect your business cannot be overstated.

If your business email is affected by a spoofer or impostor:

- **Report it immediately to local law enforcement.** Additional resources to report an email scam include the FBI's Internet Crime Complaint Center at IC3.gov and the Federal Trade Commission at FTC.gov/Complaint.
- **Notify your customers immediately.** If you email your customers, do not include hyperlinks in your notification to avoid looking like a phishing scam.
- **Alert your staff.** Use the experience to update your security practices and train employees.

Other schemes to watch out for include tech support scams

These attacks happen when you get a phone call, pop-up or email telling you there's a problem with your computer.

In these cases, scammers may pretend to be from a well-known tech company, like Microsoft. By using technical jargon to lure you into thinking that they are skilled and the problem with your computer is real, they may ask you to open some files, run a scan on your computer or ask for remote access.

These scams are vicious because impostors can install malware that gives them access to your computer, including usernames and passwords, and sensitive data. Additionally, impostors will try to sell you other products or services and ask for credit card information to bill for phony services.

Protecting your business from these types of scams takes vigilance.

- If a caller says your computer has a problem, hang up immediately. An unexpected tech support call is most likely a scam even if the number is local or looks and sounds legitimate.
- If you get a pop-up message on your computer to call tech support, ignore it and most importantly don't click on it or open it.
- If you are unsure about a call you receive, or any type of cyberthreat, consult a trusted IT or security professional. Or, call your security software company directly using the phone number on their website, the product packaging or sales receipt.
- Never, ever give someone your password. And do not provide remote access to your computer to someone who contacts you unexpectedly.

In the event your business gets hit with a tech support scam:

- Get rid of malware and update your security software.
- If passwords were shared with a scammer, change the password on every affected account or service.
- If the affected computer is on your network, ensure that the entire network is clear of intrusions.

Focus on Vendor Security

Working with vendors and other third-party partners also makes businesses vulnerable to attack. For instance, what if your tax preparer loses a laptop with your financial data? Or a vendor whose network is connected to yours gets hacked. The consequences may be just as devastating to your business as if it were your own computer or network that was affected.

Some tips for working with business vendors to ensure you are protected:

- Develop vendor contracts that include non-negotiable provisions for data security.
- Establish processes and procedures to verify that vendors are in compliance.
- Adapt to ongoing cybersecurity threats and ensure vendors keep their security up to date.

To create a culture of security with your vendors, the following are some basic guidelines and tips to follow:

- Control access to any databases with sensitive information. In working with vendors, you can restrict access on a need-to-know basis or to a specific amount of time when a vendor needs to do a job.
- Employ multi-factor authentication. Creating additional steps for vendors to log into your network – like a temporary code or a key that's inserted into a computer – provides additional protection.
- Protect your network with strong passwords and limit the number of unsuccessful log-in attempts.
- Employ properly configured, strong encryption to protect your data when it's transferred between a vendor and your business network.

In the case of a data breach with one of your vendors:

- **Contact the authorities** - your local police department or the FBI, as needed.
- **Notify your customers immediately** as they could be at risk for identity theft.
- **Confirm the vendor has a solution to fix the issues.** You will want to ensure that your information will be secure going forward, should you choose to continue working with that vendor.

Bank of Marin is here to help you protect your business from fraud and cyberthreats.

For more information or to ask a question, contact your local branch or visit bankofmarin.com

G-CSBP 01/20

Bank of Marin

NORTH BAY | SAN FRANCISCO | EAST BAY | BANKOFMARIN.COM