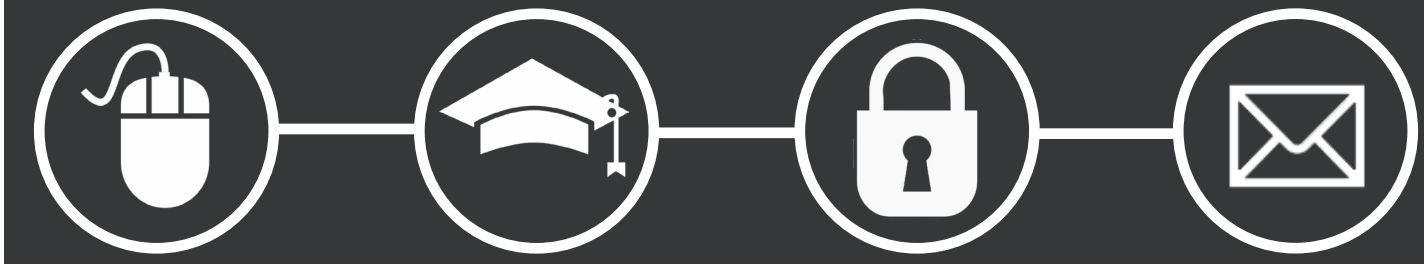

Ten Essential

Cybersecurity Best Practices

Banking ▪ Business ▪ Employees

Brought to you by:

SBS institute

SECURE BANKING SOLUTIONS SBS

www.protectmybank.com

Did you know?

One in five small-to-medium-sized companies were the victims of cyber breaches in 2013.[1]

In 76% of breaches, weak or stolen user names and passwords where a cause.[2]

Cyber crime and cyber spying costs the U.S. economy $100 billion a year and the global economy $300 billion a year.[3]

1. LOCK IT UP

You step away from your computer to grab another cup of coffee - did you lock your computer? While this best practice seems trivial, one would be surprised at how often it is not done in the workplace. Our computers house sensitive information and business processes and when a workstation is left unlocked there is a possibility an attacker could have unrestricted access to the system. To avoid possible information leaks, embarrassing photos being spread, or the occasional practical joker, simply remember to lock your computer before leaving your desks.

quick tip

Press the Windows Key + L to quickly lock your screen.

2. PROTECT YOUR MACHINE

How do you know if your machine is safe? A firewall is the first line of defense when it comes to guarding confidential digital information. It is imperative to properly install and continually update software firewalls on every machine that contains digital information.

Patching your operating systems and applications is another vital security practice. Although patches are often released on a scheduled basis, there are times when patches are sent out "off schedule" to defend against new found threats. Keep in mind, as time passes new threats will be found, so system patching will be a constant security measure.

quick tip

When applicable patches are released, it is imperative to immediately review and install them following your patch management process.

3. THINK BEFORE YOU CLICK

You just received your 50th email of the day! In your eagerness to get it out of your inbox, did you take a second to investigate the link before clicking? Once a link has been clicked there's not going back; it is possible that malicious software can install itself on your computer. Don't click on any link unless you know you can trust the source and you are certain of where the link will send you. If you are unsure about a link, the best thing to do is call the sender prior to clicking on the link.

quick tip

Hover the mouse over the link and check in the bottom of the browser to see if the actual URL link matches the link in the message.

4. WATCH FOR THE "S"

This message is brought to you by the letter "S". That simple letter makes a difference when it comes to secure online communication. "Http" stands for hypertext transfer protocol, while the "s" at the end stands for security. It is important to make sure that "https" is displayed as part of a URL you visit, as it shows the authenticity of the security certificate on that webpage. If you access a webpage without a certificate or one that is expired, there is a chance you are accessing a website that could be loaded with malware, viruses, trojans, or eavesdroppers.

quick tip

Look to the left of the URL to make sure there is a lock icon displayed. This should be a good indicator that you are on a website with a trusted security certificate.

5. BE A CAUTIOUS SURFER

The web can be risky if you aren't careful. It is easy for users to pick up malicious code that can infect a computer with viruses and other unwanted malware simply by clicking on a link. It is important that you do not surf the web if you are on an account that has administrator privileges. If you pick up malware using a computer with administrator privileges, you have successfully given the malware the same administrator rights that you have on your user account.

quick tip

Create a guest account that has access to the internet but has limited access to everything else to avoid this issue.

6. BE SMART WITH YOUR PHONE

Smartphones are everywhere, and hackers know that. Although your smartphones make it far easier for you to surf the web, check emails, and look at your bank account, they have become yet another avenue for hackers to access sensitive data.

What you can do:

- Don't open email if you don't know the sender
- Don't answer text messages asking for personal information
- Use the guest Wi-Fi network at the workplace
- Using strong phone passwords
- Turn off Bluetooth when you aren't using it or when entering sensitive data.

quick tip

Smartphones are essentially pocket-sized computers and should be protected as such. Look into mobile antivirus to keep it secure.

7. BE AWARE

Social engineering is a non-technical approach hackers use to get sensitive information. Social engineering techniques include phishing emails, fake phone calls, and physical impersonation. Employees must be trained to be helpful, but stern when it comes to giving out information, as well as how to identify a potential social engineering attack.

quick tip

If something seems fishy, it probably is. Employees should politely decline the individuals request for information and alert management.

8. PASSWORD

Two of the most common passwords are "123456" and "password." Having more complex passwords can help protect you and your data.

Strong passwords should:

- Contain at least 12 characters
- Include upper and lower case letters, numbers and special characters
- Be unique to one person
- Not be reused on multiple account logins
- Change every 60 to 90 days
- Never be shared with anyone else

quick tip

Replace your written list of passwords that can easily be stolen, copied, or lost with a password management software that will store and organize passwords.

9. EDUCATE, EDUCATE, EDUCATE

Having all employees well-trained in the basics of network, system and information security is a huge step in today's cyber world and is one of the best investments that can be made. If you have a basic understanding of security or know how to identify a potential incident you are less likely to fall victim to an attack. At the office, each employee should be kept up to date on information security policies and their role in protecting sensitive information. They should know the expectations when it comes to the limitation of personal use on company provided equipment and should sign a statement acknowledging that they understand the policies and penalties that result if guidelines are not followed.

quick tip

Increase your cyber knowledge by going beyond simply understanding cyber policies. Webinars, conferences, trainings, and certifications are available through a variety of outlets.

10. BACK IT UP

Disasters that could cause data loss don't usually give much of a warning, so consider this your friendly warning. Businesses are often not prepared for fires, floods, power failures, employee errors, or even malicious programs. In each of these instances it is entirely possible for businesses to lose some, if not all data and information stored on the computer systems. The best way to ensure all data/information is safe is to automatically backup all critical data at least once a week. Data backups should be stored in a secure, off-site location.

quick tip

There are several free or cheap automated backup solutions out there. Look into some options now, thank yourself later!

FOR MORE INFORMATION

The FDIC lists Corporate Account Takeover (CATO) as #1 on its top five fraud threats list, and also states that it is responsible for millions of dollars in losses, frayed business relationships, and litigation affecting both banks and commercial accounts. Extending your security awareness training program to your commercial customers can help fight against CATO and create the culture of cybersecurity for your customers.

Why Commercial Customers Should Attend

- Gain important insight into cyber crime and why they are targets
- Understand their role in preventing corporate account takeover
- Learn how to continually improve security controls

OTHER CYBERSECURITY EDUCATION

The SBS Institute provides a variety of cybersecurity education opportunities, both online and onsite.

- Customer security awareness training
- Employee security awareness training
- Board of director cybersecurity training
- Nationally recognized banking specific, role-based certifications

Contact sbsinstitute@protectmybank.com or 605-923-8722 for more information about SBS Institute training opportunities.

Join our mailing list at www.protectmybank.com.

Resources:
1. http://smallbusiness.foxbusiness.com/entrepreneurs/2015/03/11/cyber-hacks-against-smbs-on-rise-what-can-do/
2. http://bits.blogs.nytimes.com/2013/04/22/the-year-in-hacking-by-the-numbers
3. http://www.theguardian.com/business/2015/jan/21/cybersecurity-small-business-thwarting-hackers-obama-cameron