Ten Essential

Cybersecurity Best Practices

Brought to you by:

SBS institute

SBS CyberSecurity

The continued development of the internet has put the world at anyone's fingertips, which has made protecting personal information much more critical. With the constant development of new technology, comes massive innovation, and nonetheless, massive vulnerabilities. Due to these vulnerabilities, breaches and security implications by digital attacks are becoming far too common in today's fast-paced, technology-ruled world. As a result, innocent people are frequently becoming the victims of identity theft, phishing scams, and many other digital crimes. In order to help reduce cybersecurity related threats, SBS CyberSecurity has developed ten essential "Cybersecurity Best Practices" to help protect digital processes and information.

1. LOCK IT UP

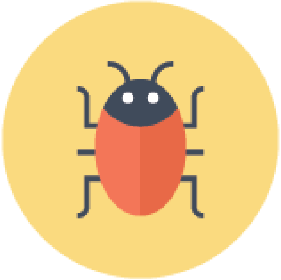
Always lock your computer before leaving your desk. While this best practice seems trivial, one would be surprised at how often this is not done in the workplace. Our computers house sensitive information and business processes and when a workstation is left unlocked there is a possibility an attacker 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.

2. PROTECT YOUR MACHINE

It is imperative to properly install and continually update software firewalls on every machine that contains digital information. A firewall helps to prevent unauthorized access to or from a network. It is the first line of defense when it comes to guarding digital information not intended for the public eye. Patching your operating systems and applications is a vital security practice as well. Patches are often released on a scheduled basis, however, there are times when patches are sent out “off schedule” in order to defend against new found threats. When these patches come out, it is important to immediately install them. Keep in mind, as time passes new threats will be found, so system patching will be a constant security measure.

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

3. THINK BEFORE YOU CLICK



This best practice tip is essential to keep in mind when it comes to clicking on links online. Once a link has been clicked it is possible that malicious software, like a virus, can install itself on the user's computer. Don't click on any link unless you know you can trust the source it is being sent from 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 individual prior to clicking on the link. Double checking the address from where the link came from can aid in determining if the link is actually valid or not. You can 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.

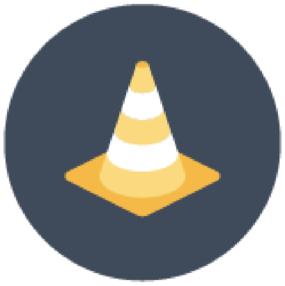
4. WATCH FOR THE "S"

One of the most common methods of secure communication online is https. "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 the webpage you are visiting. If you are surfing the web and attempt to access a webpage with a certificate that is expired or no longer secure; there is a chance you are accessing a website that could be loaded with malware, viruses, trojans, or even eavesdroppers.

quick tip

The best way to ensure you are on a website with a trusted certificate is by looking to the left of the URL and making sure there is a lock icon displayed. This means you are on a website with a trusted security certificate.

5. BE A CAUTIOUS SURFER

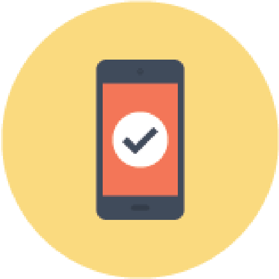


Surfing the web can be risky if you aren't careful, so use caution. This is due to the fact that it is possible for users to pick up malicious code that can infect a computer with viruses and other unwanted malware. Picking these viruses up could be as simple as clicking on a link that you think takes you to clothing website. It is also imperative 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 just 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. MIND YOUR MOBILE MANNERS



With the introduction of the smartphone it has become far easier for people to surf the web, check emails, or update social media statuses. When connected to the company network on an unprotected phone, there is potential to cause a lot of damage if one clicks on a bad link or visits the wrong page. If employees are allowed to use the company network, then proper security measures should be taken to secure the mobile device. Proper measures include:

- Phone encryption
- Using the guest Wi-Fi network
- Using strong phone passwords

7. BE ALERT

People are the weakest links when it comes to keeping sensitive information secure. One method used to gain sensitive information is called social engineering. Social engineering is the attempt to gain unauthorized information or access to facilities through the manipulation of someone. The social engineer will research the organization in an attempt to learn employee information that could aid them. They typically call the victim with a made up story designed to steal or access information. To help combat this, 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. The employee should ask questions that would be difficult for the social engineer to answer. If incorrect information is provided the employee should politely decline the individual, and alert management on the attempt to gain access to sensitive information.

8. USE STRONG PASSWORDS

It is critical for everyone to use and support strong passwords. Strong passwords contain at least 12 characters, upper and lower case letters, numbers and special characters. Passwords are used to ensure the safe keeping of sensitive information. They are an essential line of defense on a users' workstation, and will stop any attempt to gain access to restricted networks or systems. It is also necessary to set up strong passwords that are unique to one person and are not used in any other personal or business account by that person. Passwords should be changed or updated every 60 to 90 days, and should never be shared.

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

9. EDUCATE, EDUCATE, EDUCATE

If all employees have a basic understanding of security or know how to identify a potential incident your business is less likely to fall victim to an attack. On the first day of work new employees should be taught about the company’s information security policies and their role in protecting sensitive information. They should be informed on all policies regarding computer interaction, company networks, and the internet. They should know the expectations when it comes to the limitation of personal use on company provided equipment. Employees should be asked to sign a statement acknowledging that they understand the company’s business policies and any penalties that result if guidelines are not followed. 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.

10. BACK IT UP

Data Loss Prevention (DLP) software should be used to keep private information safe. There are a number of DLP software functions a user can choose, ranging from cloud prevention services all the way to e-mail services. The goal of DLP software is to monitor and protect each users’ sensitive data. A user that has DLP software installed on their system will be undoubtedly safer due to the fact that there is a “double-check safe guard” for information being processed on their workstation. For example: if an employee goes to send an e-mail and accidentally includes the sensitive information of customer at the institution, the email will not send until the info or data is erased from the message. DLP software should always be looked at as a viable option for information security.

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 cybercrime and why they are targets
- Understand their role in preventing corporate account takeover
- Learn how to continually improve security controls

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

OTHER CYBERSECURITY EDUCATION

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

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

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