Working Safely and Securely

Many incidents can be prevented by practicing safe and secure business habits. Unlike the previous section, which looked at programmatic steps you can take within your business, this section focuses on every-day activities you and your employees can do to help keep your business safe and secure. While criminals are becoming more sophisticated, most criminals still use well-known and easily avoidable methods. This section provides a list of recommended practices to help protect your business. Each employee should be trained to follow these basic practices.

Pay attention to the people you work with and around

Get to know them and maintain contact with your employees, including any contractors your business or building may employ (e.g. for cleaning, security, or maintenance). Watch for unusual activity or warning signs such as the employee mentions financial problems, begins working strange hours, asks for a lot of overtime, or becomes unusually secretive. In most cases, this activity is benign, but occasionally it can be an indicator that the employee is or may begin stealing information or money from the business, or otherwise damaging the company.

Watch for unusual activity near your place of business or in your industry. Similarly, know if other businesses in your area perform any activities which may pose an environmental or safety risk. An event that affects your neighbors may affect your business as well, or indicate new risks in your area, so it is important to remain aware.

Be careful of email attachments and web links

One of the more common means of distributing malware is via email attachments or links embedded in email. Usually the malware is attached to emails that pretend to be legitimate or from someone you know ("phishing" or "spear phishing" attacks). Links and attachments can be disguised to appear legitimate but in reality download malware onto your computer.

Do not click on a link or open an attachment that you were not expecting. If it appears important, call the sender to verify they sent the email and ask them to describe what the attachment or link is.

Before you click a link (in an email or on social media, instant messages, other webpages, or other means), hover over that link to see the actual web address it will take you to (usually shown at the bottom of the browser window). If you do not recognize or trust the address, try searching for relevant key terms in a web browser. This way you can find the article, video, or webpage without directly clicking on the suspicious link. Train employees to recognize phishing attempts and who to notify when one occurs.

Use separate personal and business computers, mobile devices, and accounts

As much as possible, have separate devices and email accounts for personal and business use. This is especially important if other people such as children use your personal devices. Do not conduct business

or any sensitive activities (e.g. online business banking) on a personal computer or device and do not engage in activities such as web surfing, gaming, downloading videos, etc., on business computers or devices. Do not send sensitive business information to your personal email address.

Personal or home computers and electronics may be less secure than business systems. Personal devices may be used for web surfing to untrustworthy sites and have untrustworthy applications installed such as games which are not required for work and which add vulnerabilities that a hacker could exploit.

Some businesses may want to consider using a separate computer that is not connected to any network for certain business functions or for extremely sensitive information. Because most cyber-attacks require network connectivity, disconnecting extremely sensitive information from the network prevents these kinds of attacks.

Do not connect personal or untrusted storage devices or hardware into your computer, mobile device, or network.

Do not share USB drives or external hard drives between personal and business computers or devices. Do not connect any unknown / untrusted hardware into your system or network and do not insert any unknown CD, DVD, or USB drive. These devices may have malware on them. Criminals are known to place USB drives in public places where their target business's employees gather, knowing that curious individuals will pick them up and plug them in. What is on them is generally malware which will spy on or take control of the computer.

Disable the AutoRun feature for the USB ports and optical drives like CD and DVD drives on your business computers to help prevent such malicious programs from installing on your systems.

Be careful downloading software

Do not download software from an unknown web page.

Only those web pages belonging to reputable businesses with which you have a business relationship should be considered reasonably safe for downloading software.

Be very careful if you decide to download and use freeware or shareware. Most of these do not come with technical support and some do not have the full functionality you might believe will be provided.

Do not give out personal or business information

Social engineering is an attempt to obtain physical or electronic access to your business information by manipulating people. A very common type of attack involves a person, website, or email that pretends to be something it's not. A social engineer will research your business to learn names, titles, responsibilities, and any personal information they can find. Afterwards, the social engineer usually calls or sends an email with a believable, but made-up, story designed to convince the person to give them certain information.

If you receive an unsolicited phone call asking for personal information from a company you recognize (such as from your bank or doctor's office), ask for identifying information that only a person associated with the organization would know. If this is not possible, ask the person for their name and office or

division and tell them you will call them right back. Call the company using the information from their website or on your contract or bill – do not use any phone number provided by the person who called you. Then ask for the representative who called you.

Never respond to an unsolicited phone call from a company you do not recognize that asks for sensitive personal or business information. Employees should notify their management whenever there is an attempt or request for sensitive business information.

Never give out your username or password. No company should ask you for this information for any reason. Also, beware of people asking what kind of operating system you use, what brand firewalls you have, what internet browser you use, or what applications you have installed. This is all information that can make it easier for a hacker to break in to your system.

Watch for harmful pop-ups

When connected to and using the Internet, do not respond to popup windows requesting that you click "OK" for anything. Use a popup blocker and only allow popups on websites you trust.

If a window pops up on your screen unexpectedly, DO NOT close the popup window, either by clicking "okay" or by selecting the X in the upper right corner of the popup window, especially if the pop up is informing you that your system has a virus and suggesting you download a program to fix it. Do not respond to popup windows informing you that you have to download a new codec, driver, or special program for the web page you are visiting. Some of these popup windows are actually trying to trick you into clicking on "OK" which will allow it to download and install spyware or other malware onto your computer. Be aware that some of these popup windows are programmed to interpret any mouse click anywhere on the window as an "OK" and act accordingly.

If you encounter this kind of pop-up window, disconnect from the network and force the browser to close (in Windows, hit "ctrl + alt + del" and delete the browser from running tasks. In OSX, right-click the application in the bar and select "force close"). You should save any files you have open and reboot the computer, then run your anti-virus software.

Use strong passwords

Good passwords consist of a random sequence of letters (upper case and lower case), numbers, and special characters, and are at least 12 characters long17. For systems or applications that have important information, use multiple forms of identification (called "multi-factor" or "dual factor" authentication). For example, when a user logs in with a password, they may be sent a text message with a code they have to enter as well. Biometrics (e.g. fingerprint scanners) and other devices may be used, but can be expensive and difficult to install or maintain.

Many devices come with default administration passwords – these should be changed immediately when installing and regularly thereafter. Default passwords are easily found or known by hackers and can be used to access the device. The manual or those who install the system should be able to show you how to change them.

Passwords that do not change for long periods of time allow hackers time to crack them and may be shared and become common knowledge to an individual user's coworkers. Therefore, passwords should

be changed at least every 3 months18. Consider configuring systems and devices to require users to change their passwords every 3 months if possible.

Passwords to devices and applications that deal with business information should not be re-used. If a hacker gains access to one account, they will have access to all others that share that password. It may be difficult to remember a number of different passwords so a password management system may be an option. However, these systems place all passwords into one place which may be lost or compromised. Carefully compare password management solutions before purchasing.

You may want to consider using a password management application to store your passwords for you. Ensure the application encrypts all passwords stored on it. Use a strong password on the application and change the password regularly.

Conduct online business more securely

Online business/commerce/banking should only be done using a secure browser connection. This will normally be indicated by a small lock visible in the lower right corner or upper left of your web browser window.

Erase your web browser cache, temporary internet files, cookies, and history regularly. Make sure to erase this data after using any public computer and after any online commerce or banking session. This prevents important information from being stolen if your system is compromised. This will also help your system run faster. Typically, this is done in the web browser's "privacy" or "security" menu. Review your web browser's help manual for guidance.

If you do online business banking, you may want to consider having a dedicated computer which is used ONLY for online banking. Do not use it for Internet searches, personal banking, or email. Use it only for online banking for the business and disconnect it when not in use.

Questions or in need of cyber security guidance?

Email us at info@sidechannelsec.com

Visit our website at www.sidechannelsec.com

Reference - NISTIR 7621 REV. 1 SMALL BUSINESS INFORMATION SECURITY: THE FUNDAMENTALS