ADVISOR SOLUTIONS GROUP, INC

INTEROFFICE MEMORANDUM

TO: [RECIPIENT NAME]
FROM: [YOUR NAME]
SUBJECT: CYBERSECURITY FOR EMPLOYEE'S HOME COMPUTERS AND PERSONAL DEVICES
DATE: [CLICK TO SELECT DATE]
CC: [NAME]

Cybersecurity

The Threat

Home and small business computers are easy prey. Hackers may want to gain access to your financial accounts, or the target could be someone that you know that is a bigger target and the hacker is using you as a conduit. Another common reason home and small business systems are attacked is to gain control and use your computer (along with many others) in a coordinated cyber attack. Finally, there is malicious mischief where a hacker gains satisfaction from harming others, which could be you. According the Symantec 2013 Internet Security Report, 31% of cyber attacks were aimed at home users and small businesses because they are soft targets. You need to be aware of the threat and we will discuss specific steps you can take to protect yourself and your computers.

Nomenclature and General Principles

Perimeter, Interior and User Defenses – We will break down this discussion into three sections: perimeter defenses, interior defenses and user defenses. There is an over-emphasis on perimeter defenses. The truth is it is extremely difficult to keep a hacker out of your system even with the most hardened perimeter. However, what you can do is make it very difficult for the hacker to do harm once in the system by hardening the interior. Think of an M&M candy which is hard on the outside but soft on the inside. What we want to create is a peanut M&M which is hard on the outside and hard on the inside. This is analogous to protecting your privacy such as your Social Security Number. If someone really wants to get your SSN there is little you could do to stop them, however, by freezing your credit you could make it very difficult for someone to abuse your information. There are technological and human elements to security – Cybersecurity is not wholly a technological issue. One of the biggest vulnerabilities is a compromised user. Hackers can trick and trap users into compromising information or enabling a vulnerability that can be exploited (such as a virus). Awareness is the best

protection much like being aware when in an unfamiliar and potentially dangerous neighborhood.

Minimalist ("Less is more") – Fewer targets are easier to defend so a minimalist philosophy is a more secure philosophy. This theme will recur throughout this discussion.

Virtualization – Virtualization means utilizing the internet ("the cloud") for services and data storage. Generally, reputable cloud delivered services and data storage will be more resilient and more secure than analogous applications on your own hardware. Your computers could be stolen, damaged in a disaster, and are difficult to keep updated. While cloud delivered applications are not perfect they are probably better than the alternative on your own system. This will also be a recurring theme in this discussion.

Perimeter Security – "Close and Lock All of the Doors and Windows to Your System"

Inventory - The first step to securing your perimeter is to define your perimeter by taking an inventory of your devices and connections to your network (computers, mobile devices, remote access.) This inventory is a list of the entry points to your network and will be the focus of your perimeter defense. Remember one open window is all a hacker will need to easily breach your system so EVERY entry point must be secured.

Physical Security – One of the most common breaches emanates from lost or stolen equipment. In particular, mobile devices and portable storage (flash drives) are highly susceptible so be diligent and develop good habits including not leaving devices unattended for any length of time and not placing a phone on the table at a restaurant where it could be inadvertently left behind. If your home or office is vulnerable consider upgrading the security which could be as simple as installing deadbolts on doors or an alarm system.

Firewall – A firewall is a hardware or software system that creates a secure environment for network computing. This can be accomplished through a number of devices. Windows has a built in firewall which can be activated here:

<Start><Control Panel><System & Security><Windows Firewall>

Most of the comprehensive software security packages (antivirus software) also include firewall protection (covered below). In the case of a wireless network, the wireless router will serve as a firewall (also covered below.) Regardless of which system is acting as the firewall the important point is to make sure you have one and are thus operating in a secure environment. Note: we use the term secure environment but there are levels of security with some definitely more secure than others. The levels of security are beyond the scope of this discussion, however, be aware that most secure networks can be penetrated so the firewall is just one component of your defenses.

Wireless Networks – Wireless networks are inherently vulnerable but that must be weighed against the low cost and convenience. An open network is an open door so make sure you secure the wireless network. Here are a few steps that should be taken:

1. Change the Administration Password. The two most common wireless routers on the market are Linksys and Netgear and hackers know the default Admin passwords so make sure you change the password.
2. Use WPA or preferably WPA2 Encryption. If you are required to enter a password to allow a device to connect to your wireless then you have enabled encryption.
3. Change the Default Service Set Identifier (SSID)(Name your network). Again, if you have the factory default a hacker will target your system on the assumption that if you did not name the network you probably did not take other steps such as encryption. To see the name of your network go to:

    <Start><Control Panel><Network and Internet>

    If it needs to be changed consult the manual for your wireless router. If you have misplaced the manual, do an internet search on the name of your router and you should be able to find a manual online.

Antivirus Software – There are many good vendors and even free products. For example, centrally managed client-server solutions are offered by such companies as ESET, TrendMicro, Kaspersky, Norton Internet Security, and others. Each of these include the options of antivirus, malware and firewall protection. Antivirus software has become somewhat of a misnomer because many of these programs perform other critical functions. Having a robust security program such as Norton is ABSOLUTELY essential.

http://us.norton.com/internet-security/
www.eset.com
www.trendmicro.com
usa.kaspersky.com

Operating System Patches – Make sure you turn on Windows Automatic Updates

<Start><All Programs><Windows Update>

On the second Tuesday of each month (dubbed "patch Tuesday") when you turn off your computer you should see "installing update 1 of __" and this is how you will know that you have automatic updates turned on. Windows is updated when vulnerabilities are identified and patched. Hackers exploit known vulnerabilities on systems that have not been updated, so make sure you turn on automatic updates. Incidentally, the second Wednesday of each month is called "hacker Wednesday" because hackers attempt to

exploit vulnerabilities immediately and the highest number of breaches occur on the second Wednesday of the month.

Mobile Devices – Smartphones and tablets are a window to your network so make sure they are secured using these four steps:

1. Password protect AND encrypt your data. This may be done via <Settings> in either Apple or Android systems. Although inconvenient, you should be required to sign in when turning on the device. Without the password the encrypted data on the device will be secure. If your Smartphone does not have an encryption option, you can purchase a third-party solution.

2. Install antivirus software. Android is particularly vulnerable and an example of a mobile antivirus application for mobile Android devices is Avast Mobile Security & Antivirus:

http://www.avast.com/en-us/free-mobile-security

If you are a typical iPhone user you probably don't need antivirus software because apps via iTunes are screened by Apple for malware.

3. Virtualize your data using iCloud (Apple devices) or Gmail (Android devices). Your data will be automatically backed up in the cloud. Avast has a backup utility and below are instructions to setup iCloud.

http://www.apple.com/icloud/setup/

4. Have the ability to remotely locate or wipe the device if it is lost or stolen. Avast Anti-theft and Google's Android Device Manager have these capabilities. For the iPhone the free app "Find My Phone" works well. With these apps you can use your computer to bring up a GPS map showing the location of your phone, and if necessary, you can wipe the data from the device.

Browser Security – Many viruses are transmitted via websites so browser security is important. One browser does not preclude you from using another. You can install and use multiple browsers depending on the needs of the websites you are visiting. Consider using Chrome as your default browser. From Chrome type in Chrome://extensions and <Get More Extensions>. Here are three security extensions to consider:

1. HTTPS Everywhere. Many websites offer a secure connection. With HTTPS Everywhere installed Google Chrome will automatically create a secure connection to the supported website.

2. Ad Block Plus. As the name implies this is an ad blocker, however this extension as well as the others mentioned here could cause some websites to malfunction. In this case you might need to switch to Firefox or Internet Explorer.

3. Ghostery. Like Ad Block Plus, Ghostery is a privacy extension that blocks unwanted ads.

In Firefox go to <Tools><Options><Security> and check the boxes for "Warn me when sites try to install add-ons", "Block reported attack sites", "Block reported web forgeries."

In Internet Explorer go to <Tools><Internet Options><Security> and make sure the slider bar is set at least to <Medium-high>.

User Privileges – Consistent with the minimalist philosophy setup User Accounts without Administrator Privileges. This way if your user account is compromised the hacker will be restricted in what they can do.

<Start><Control Panel><User Accounts>
Add User Account as a Standard User

Strong Passwords – Passwords are the keys to the locked doors and windows and they must be protected. Don't share passwords! One of the most common sources of system breaches is a compromised password. The most critical element of password strength is the length of the password. Any eight character password can be cracked with readily available internet tools in a matter of minutes. A twenty character password would take weeks. One technique to lengthen a password without compromising on convenience is called padding where you add characters to the end of an easily remembered password such as $$$$$$$$ or 1234567890. Here is a website that explains the technique in more detail:

GRC's | Password Haystacks: How Well Hidden is Your Needle?

Password managers are a highly recommend tool as they enable you to easily use different passwords on different sites by encrypting all your password in one application requiring you to only memorize one password to access that application. Using the same password for all sites is a poor safety practice. Moreover, Roboform and Lastpass, two examples of password managers, have features that are extremely convenient and actually make accessing password protected websites easier by securely storing the web address, user ID and password and allowing you login with a single click. Finally, there are mobile versions AND all of the passwords can be virtualized and automatically synced

with all devices. Thus, if you change a password using your phone the password will be changed for all devices.

Roboform – Best Password Manager & Form Filler | RoboForm
Lastpass – https://lastpass.com

Finally, you should make use of multifactor authentication which is readily available on commonly used websites such as Facebook, Yahoo Mail and Gmail:

http://www.cnet.com/how-to/how-to-enable-two-factor-authentication-on-popular-sites/

When you enable multifactor authentication you will be required to enter the password AND answer challenge questions or enter a token (six digit code) sent to your phone via text message. Email accounts get hacked frequently, however, one with multifactor authentication is less likely to become compromised.

Interior Security

Data Backup – If you could do only one thing mentioned in this discussion it would be to back up your data in the cloud. The services mentioned below are well worth the cost and operate seamlessly and effectively. Hardware and software can be replaced but your data is critical so make sure you back it up. There are many services and most new computers come with a service pre-loaded however consider using Mozy and Carbonite:

Mozy - https://mozy.com/#slide-5
Carbonite - Carbonite Cloud Backup Services - Online Computer Data Backup

One big advantage of Mozy is you can access your data from all of your devices including your work computer, netbook and home computers. When you work on a file it is saved online and there is no problem with accessing a prior version from a different device. This is consistent with the theme of virtualization and analogous to using iCloud or Gmail for your smartphone.

Finally, if there are multiple users of data such as in a small business, it is highly recommend to have at least two independent backups where the backups are done by different people and each does not have access to the other. This follows the principle that "no one should have all the keys to the Kingdom." Many businesses have been wiped out by a disgruntled employee that is intent on harming the company and deleting all of the data. Having independent backups is a critical control if there are multiple users of the data.

Encryption – Encrypting your data is the second most important protection behind backing up your data. Note: the two most important safeguards are interior defenses

because the perimeter is extremely difficult to guard. We talked about encrypting the data on your smartphone and on your computer. There are built in encryption programs such as Bitlocker which will encrypt your entire hard drive. However, as "leaked" by Edward Snowden, Microsoft has cooperated with Federal Law Enforcement and turned over the encryption key. Bitlocker is still extremely secure. There are alternatives, for example AxCrypt:

Axantum Software AB | AxCrypt | File Encryption Software

This is a free open-source program and encrypts individual files and is a most convenient encryption program. Functionality is as simple as right-clicking on the file and the passphrase can be stored and need only be entered once. Note: if you leave your computer it is recommend not enabling this feature. In that case you would be required to enter the passphrase every time you open a protected file. Entire folders can be selected so it is easy to encrypt or decrypt multiple files at once.

Portable Storage – Flash drives a.k.a. thumb drives are handy (no pun intended) but vulnerable. Make sure all important content on flash drives is encrypted using AxCrypt or something similar. Also be aware of a hacker trick of leaving a flash drive to be found and a curious person inserts the drive into their computer and unknowingly downloads a virus. Don't fall for this and if anyone gives you flash drive, even someone known to you, get in the habit of holding down the left shift key while inserting the drive. This will prevent any auto-executable files on the flash drive from running. Another option is to disable auto-play on your computer.

Human Elements of Security – Awareness and Safe User Practices

Social Engineering – Social engineering are methods hackers use to trick users into revealing sensitive information such as passwords or to unknowingly download a harmful virus. Your best protection is awareness.

Phishing - Protect against phishing which is a technique used by online criminals to trick people into revealing information. Most are fairly easy to recognize as scams but some can emulate notifications from well-known vendors such as Bank of America, UPS, Federal Express, Amazon or Ebay. Examine emails carefully, especially the sender's email address. If the email domain does not match the sender's company it is likely fake. Also examine any links by hovering your mouse over the link to see the linked address. This is not 100% reliable so the best policy is to not click on any links. Instead, open your browser and enter the address manually.

Spearphishing which is also known as pretexting is more insidious. Spearphishing attacks are targeted and the criminal will often glean information from social media sites including names of family or friends to tailor the phishing attack. These can be much more difficult to detect so be careful.

Public Wi-Fi – Public Wi-Fi such as free wireless at airports, hotels and Starbucks is inherently dangerous and should be avoided if possible. Learn how to use your phone as a mobile hotspot by contacting your cellular provider, for example:

> http://www.verizonwireless.com/insiders-guide/tech-smarts/how-to-use-your-smartphone-as-a-mobile-hotspot/

If you must use public Wi-Fi setup a Virtual Private Network (VPN). Here is a link to an example of an application, which also offers a more limited free version:

> Hotspot Shield

Securely Empty the Recycle Bin – Most people don't know this but when you "empty" the recycle bin the file is still intact on your drive and could be easily retrieved. This is analogous to taking the trash out and having a dumpster diver pick out important information. To securely erase files from your system you need to use an eraser (sometimes called a shredder). Here is an example of such an application:

> Eraser (free) Eraser :: Downloads

Malware – Malware includes viruses, spyware and other malicious programs that can be downloaded to aid a hacker or compromise your system. Unfortunately, many of these programs are not detected by antivirus software so you need to be careful.

> Two Email tips:
> 1. Do not open suspicious emails or attachments
> 2. Do not click on links within an email
>
> Scareware - A common ploy is fake antivirus security warnings also called scareware. Everyone on the [COMPANY] network has antivirus software but you should also know what type of antivirus software is protecting your other computers. If a warning pops up react calmly and with caution.
> Ransomware – Is a virus payload that will encrypt your data which will be held for ransom to decrypt. If you backup your data online you can delete the encrypted files, remove the virus and restore your data from the backup.
> How to Remove Browser Pop-ups and Adware. This is both an annoyance and a security problem and it is very good to know if you are being bombarded with browser pop-ups (adware).
> http://malwaretips.com/blogs/remove-adware-popup-ads/