CHAPTER 03: PROTECTING YOUR DATA AND PRIVACY

This chapter focuses on your personal devices and your personal data. It includes tips for protecting your devices, creating strong passwords and safely using wireless networks. It also discusses maintaining your data securely.

Your online data is worth something to cyber criminals. This chapter briefly covers authentication techniques to help you maintain your data securely. It also covers ways to enhance the security of your online data with tips about what to do and what not to do online.

Protecting Your Data

Your computing devices store your data and are the portal to your online life. Below is a short list of steps you can take to protect your computing devices from intrusion:

- **Keep the Firewall On** – Whether it is a software firewall or a hardware firewall on a router, the firewall should be turned on and updated to prevent hackers from accessing your personal or company data. Click Windows 7 and 8.1 or Windows 10 to turn on the firewall in the respective version of Windows. Click here to turn on the firewall for Mac OS X devices.
- **Use Antivirus and Antispyware** – Malicious software, such as viruses, Trojan horses, worms, ransomware and spyware, are installed on your computing devices without your permission, in order to gain access to your computer and your data. Viruses can destroy your data, slow down your computer, or take over your computer. One way viruses can take over your computer is by allowing spammers to broadcast emails using your account. Spyware can monitor your online activities, collect your personal information, or produce unwanted pop-up ads on your web browser while you are online. A good rule is to only download software from trusted websites to avoid getting spyware in the first place. Antivirus software is designed to scan your computer and incoming email for viruses and delete them. Sometimes antivirus software also includes antispyware. Keep your software up to date to protect your computer from the newest malicious software.
- **Manage Your Operating System and Browser** – Hackers are always trying to take advantage of vulnerabilities in your operating systems and your web browsers. To protect your computer and your data, set the security settings on your computer and browser at medium or higher. Update your computer's operating system including your web browsers and regularly download and install the latest software patches and security updates from the vendors.
- **Protect All Your Devices** – Your computing devices, whether they are PCs, laptops, tablets, or smartphones, should be password protected to prevent unauthorized access. The stored information should be encrypted, especially for sensitive or confidential data. For mobile devices, only store necessary information, in case these devices are stolen or lost when you are away from your home. If any one of your devices is compromised, the criminals may have access to all your data through your cloud-storage service provider, such as iCloud or Google drive.

IoT devices pose an even greater risk than your other computing devices. While desktop, laptop and mobile platforms receive frequent software updates, most of the IoT devices still have their original firmware. If vulnerabilities are found in the firmware, the IoT device is likely to stay vulnerable. To make the problem worse, IoT devices are often designed to call home and require Internet access. To reach the

Internet, most IoT devices manufacturers rely on the customer's local network. The result is that IoT devices are very likely to be comprised and when they are, they allow access to the customer's local network and data. The best way to protect yourself from this scenario is to have IoT devices using an isolated network, sharing it only with other IoT devices.

Use Wireless Networks Safely

Wireless networks allow Wi-Fi enabled devices, such as laptops and tablets, to connect to the network by way of the network identifier, known as the Service Set Identifier (SSID). To prevent intruders from entering your home wireless network, the pre-set SSID and default password for the browser-based administrative interface should be changed. Hackers will be aware of this kind of default access information. Optionally, the wireless router can also be configured to not broadcast the SSID, which adds an additional barrier to discovering the network. However, this should not be considered adequate security for a wireless network. Furthermore, you should encrypt wireless communication by enabling wireless security and the WPA2 encryption feature on the wireless router. Even with WPA2 encryption enabled, the wireless network can still be vulnerable.

In October 2017, a security flaw in the WPA2 protocol was discovered. This flaw allows an intruder to break the encryption between the wireless router and the wireless client, and allow the intruder to access and manipulate the network traffic. This vulnerability can be exploited using Key Reinstallation Attacks (KRACK). It affects all modern, protected Wi-Fi networks. To mitigate an attacker, a user should update all affected products: wireless routers and any wireless capable devices, such as laptops and mobile devices, as soon as security updates become available. For laptops or other devices with wired NIC, a wired connection could mitigate this vulnerability. Furthermore, you can also use a trusted VPN service to prevent the unauthorized access to your data while you are using the wireless network.

When you are away from home, a public Wi-Fi hot spot allows you to access your online information and surf the Internet. However, it is best to not access or send any sensitive personal information over a public wireless network. Verify whether your computer is configured with file and media sharing and that it requires user authentication with encryption. To prevent someone from intercepting your information (known as "eavesdropping") while using a public wireless network, use encrypted VPN tunnels and services. The VPN service provides you secure access to the Internet, with an encrypted connection between your computer and the VPN service provider's VPN server. With an encrypted VPN tunnel, even if a data transmission is intercepted, it is not decipherable.

Many mobile devices, such as smartphones and tablets, come with the Bluetooth wireless protocol. This capability allows Bluetooth-enabled devices to connect to each other and share information. Unfortunately, Bluetooth can be exploited by hackers to eavesdrop on some devices, establish remote access controls, distribute malware, and drain batteries. To avoid these issues, keep Bluetooth turned off when you are not using it.

Use Unique Passwords for Each Online Account

You probably have more than one online account, and each account should have a unique password. That is a lot of passwords to remember. However, the consequence of not using strong and unique passwords leaves you and your data vulnerable to cyber criminals. Using the same password for all your online accounts is like using the same key for all your locked doors, if an attacker was to get your key, he would have the ability to access everything you own. If criminals get your password through phishing for

example, they will try to get into your other online accounts. If you only use one password for all accounts, they can get into all your accounts, steal or erase all your data, or decide to impersonate you.

We use so many online accounts that need passwords that is becomes too much to remember. One solution to avoid reusing passwords or using weak passwords is to use a password manager. A password manager stores and encrypts all of your different and complex passwords. The manager can then help you to log into your online accounts automatically. You only need to remember your master password to access the password manager and manage all of your accounts and passwords.

Tips for choosing a good password:

- Do not use dictionary words or names in any languages
- Do not use common misspellings of dictionary words
- Do not use computer names or account names
- If possible use special characters, such as ! @ # $ % ^ & * ( )
- Use a password with ten or more characters

Use Passphrase Rather Than a Password

To prevent unauthorized physical access to your computing devices, use passphrases, rather than passwords. It is easier to create a long passphrase than a password, because it is generally in the form of a sentence rather than a word. The longer length makes passphrases less vulnerable to dictionary or brute force attacks. Furthermore, a passphrase maybe easier to remember, especially if you are required to change your password frequently. Here are some tips in choosing good passwords or passphrases:

Tips in choosing a good passphrase:

- Choose a meaningful statement to you
- Add special characters, such as ! @ # $ % ^ & * ( )
- The longer the better
- Avoid common or famous statements, for example, lyrics from a popular song

Recently, United States National Institute for Standards and Technology (NIST) published improved password requirements. NIST standards are intended for government application but can also serve as a standard for others as well. The new guidelines aim to provide better user experience and put the burden of user verification on the providers.

Summary of the new guidelines:

- 8 characters minimum in length, but no more than 64 characters
- No common, easily guessed passwords, such as password, abc123
- No composition rules, such as having to include lowercase and uppercase letters and numbers
- Improve typing accuracy by allowing the user to see the password while typing
- All printing characters and spaces are allowed
- No password hints
- No periodical or arbitrary password expiration
- No knowledge-based authentication, such as information from shared secret questions, marketing data, transaction history

Even with access to your computers and network devices secured, it is also important to protect and preserve your data.

Encrypt Your Data

Your data should always be encrypted. You may think you have no secrets and nothing to hide so why use encryption? Maybe you think that nobody wants your data. Most likely, this is probably not true.

Are you ready to show all of your photos and documents to strangers? Are you ready to share financial information stored on your computer to your friends? Do you want to give out your emails and account passwords to the general public?

This can be even more troublesome if a malicious application infects your computer or mobile device and steals potentially valuable information, such as account numbers and passwords, and other official documents. That kind of information can lead to identity theft, fraud, or ransom. Criminals may decide to simply encrypt your data and make it unusable until you pay the ransom.

What is encryption? Encryption is the process of converting the information into a form where an unauthorized party cannot read it. Only a trusted, authorized person with the secret key or password can decrypt the data and access it in its original form. The encryption itself does not prevent someone from intercepting the data. Encryption can only prevent an unauthorized person from viewing or accessing the content.

Software programs are used to encrypt files, folders, and even entire drives.

Encrypting File System (EFS) is a Windows feature that can encrypt data. EFS is directly linked to a specific user account. Only the user that encrypted the data will be able to access it after it has been encrypted using EFS. To encrypt data using EFS in all Windows versions, follow these steps:

Step 1. Select one or more files or folders.

Step 2. Right-click the selected data **>Properties**.

Step 3. Click **Advanced…**

Step 4. Select the **Encrypt contents to secure data** check box.

Step 5. Files and folders that have been encrypted with EFS are displayed in green, as shown in the figure.

Back Up Your Data

Your hard drive may fail. Your laptop could be lost. Your smart phone stolen. Maybe you erased the original version of an important document. Having a backup may prevent the loss of irreplaceable data, such as family photos. To back up data properly, you will need an additional storage location for the data and you must copy the data to that location regularly and automatically.

The additional location for your backed up files can be on your home network, secondary location, or in the cloud. By storing the backup of the data locally, you have total control of the data. You can decide to copy all of your data to a network attached storage device (NAS), a simple external hard drive, or maybe select only a few important folders for backup on thumb drives, CDs/DVDs, or even tapes. In that scenario, you are the owner and you are totally responsible for the cost and maintenance of the storage device equipment. If you subscribe to a cloud storage service, the cost depends on the amount storage space

needed. With a cloud storage service like Amazon Web Services (AWS), you have access to your backup data as long as you have access to your account. When you subscribe to online storage services, you may need to be more selective about the data being backed up due to the cost of the storage and the constant online data transfers. One of the benefits of storing a backup at an alternate location is that it is safe in the event of fire, theft or other catastrophes other than storage device failure.

Deleting Your Data Permanently

When you move a file to the recycle bin or trash and delete it permanently, the file is only inaccessible from the operating system. Anyone with the right forensic tools can still recover the file due to a magnetic trace left on the hard drive.

In order to erase data so that it is no longer recoverable, the data must be overwritten with ones and zeroes multiple times. To prevent the recovery of deleted files, you may need to use tools specifically designed to do just that. The program SDelete from Microsoft (for Vista and higher), claims to have the ability to remove sensitive files completely. Shred for Linux and Secure Empty Trash for Mac OSX are some tools that claim to provide a similar service.

The only way to be certain that data or files are not recoverable is to physically destroy the hard drive or storage device. It has been the folly of many criminals in thinking their files were impenetrable or irrecoverable.

Besides storing data on your local hard drives, your data may also be stored online in the cloud. Those copies will also need to be deleted. Take a moment to ask yourself, “Where do I save my data? Is it backed up somewhere? Is it encrypted? When you need to delete your data or get rid of a hard drive or computer, ask yourself, “Have I safeguarded the data to keep it from falling into the wrong hands?”

Safeguarding Your Online Privacy

Popular online services, such as Google, Facebook, Twitter, LinkedIn, Apple and Microsoft, use two factor authentication to add an extra layer of security for account logins. Besides the username and password, or personal identification number (PIN) or pattern, two factor authentication requires a second token, such as a:

- **Physical object** - credit card, ATM card, phone, or fob
- **Biometric scan** - fingerprint, palm print, as well as facial or voice recognition

Even with two factor authentication, hackers can still gain access to your online accounts through attacks such as phishing attacks, malware, and social engineering.

OAuth 2.0

Open Authorization (OAuth) is an open standard protocol that allows an end user’s credentials to access third party applications without exposing the user’s password. OAuth acts as the middle man to decide whether to allow end users access to third party applications. For example, say you want to access web application XYZ, and you do not have a user account for accessing this web application. However, XYZ has the option to allow you to log in using the credentials from a social media website ABC. So you access the website using the social media login.

For this to work, the application 'XYZ' is registered with 'ABC' and is an approved application. When you access XYZ, you use your user credentials for ABC. Then XYZ requests an access token from ABC on your behalf. Now you have access to XYZ. XYZ knows nothing about you and your user credentials, and this interaction is totally seamless for the user. Using secret tokens prevents a malicious application from getting your information and your data.

Do Not Share Too Much on Social Media

If you want to keep your privacy on social media, share as little information as possible. You should not share information like your birth date, email address, or your phone number on your profile. The people who need to know your personal information probably already know it. Do not fill out your social media profile completely, only provide the minimum required information. Furthermore, check your social media settings to allow only people you know to see your activities or engage in your conversations.

The more personal information you share online, the easier it is for someone to create a profile about you and take advantage of you offline.

Have you ever forgotten the username and password for an online account? Security questions like "What is your mother's maiden name?" or "In what city were you born?" are supposed to help keep your account safe from intruders. However, anyone who wants to access your accounts can search for the answers on the Internet. You can answer these questions with false information, as long as you can remember the false answers. If you have a problem remembering them, you can use password manager to manage them for you.

Email and Web Browser Privacy

Every day, millions of email messages are used to communicate with friends and conduct business. Email is a convenient way to communicate with each other quickly. When you send an email, it is similar to sending a message using a postcard. The postcard message is transmitted in plain sight of anyone who has access to look, and the email message is transmitted in plain text, and is readable by anyone who has access. These communications are also passed among different servers while in route to the destination. Even when you erase your email messages, the messages can be archived on the mail servers for some time.

Anyone with physical access to your computer, or your router, can view which websites you have visited using web browser history, cache, and possibly log files. This problem can be minimized by enabling the in-private browsing mode on the web browser. Most of the popular web browsers have their own name for private browser mode:

- **Microsoft Edge**: InPrivate
- **Google Chrome**: Incognito
- **Mozilla Firefox**: Private tab / private window
- **Safari**: Private: Private browsing

With private mode enabled, cookies are disabled, and temporary Internet files and browsing history are removed after closing the window or program.

Keeping your Internet browsing history private may prevent others from gathering information about your online activities and enticing you to buy something with targeted ads. Even with private browsing enabled and cookies disabled, companies are developing different ways of fingerprinting users in order to gather information and track user behavior. For example, the intermediary devices, such as routers, can have information about a user's web surfing history.

Ultimately, it is your responsibility to safeguard your data, your identity, and your computing devices. When you send an email, should you include your medical records? The next time you browse the Internet, is your transmission secure? Just a few simple precautions may save you problems later.

Summary

This chapter focused on your personal devices, your personal data. It included tips for protecting your devices, creating strong passwords and safely using wireless networks. It covered data backups, data storage and deleting your data permanently.

Authentication techniques were discussed to help you maintain your data securely. It briefly covered how easy it is to share too much information on social media and how to avoid this security risk.