3.1.2 Protecting Computing Devices

Firewall turned on,

firewall (either a software firewall or a hardware firewall on a router) to protect your device from unauthorized access. constantly update firewall to prevent hackers from accessing your personal or organization data.

Antivirus software,

always use antivirus software to provide another layer of protection. This software, which often includes antispyware, is designed to scan your computer and incoming email for viruses and delete them. Keeping your software up to date will protect your computer from any new malicious software that emerges.

Manage OS and browser

Hackers are always trying to take advantage of vulnerabilities that may exist in your operating system. Therefore, to protect your computer and your data, you should set the security settings on your computer and browser to medium level or higher. You should also regularly update your computer's operating system, including your web browser, and download and install the latest software patches and security updates from the vendors.

Password Protection,

All of your computing devices, including PCs, laptops, tablets and smartphones, should be password protected to prevent unauthorized access. sensitive or confidential data, should be encrypted. You should only store necessary information on your mobile device, in case it is stolen or lost.

IoT devices pose an even greater risk than your other computing devices. While desktop, laptop and mobile platforms receive frequent software updates, most IoT devices have their original software. If vulnerabilities are found in the software. And to make the problem worse, IoT devices require Internet access, most often relying on your local network. The best way to protect yourself from this scenario is to set up any IoT devices on an isolated network.

3.1.3 Wireless Network Security at Home

you should encrypt wireless communication by enabling wireless security and the WPA2 encryption feature on your wireless router. But be aware, even with WPA2 encryption enabled, a wireless network can still be vulnerable.

3.1.4 Public wifi Risks

it is best not to access or send any personal information when using public Wi-Fi.

always verify that your device isn't configured with file and media sharing and that it requires user authentication with encryption.

an encrypted VPN service to prevent others from intercepting your information (known as 'eavesdropping') over a public wireless network. This service gives you secure access to the Internet, by encrypting the connection between your device and the VPN server. Even if hackers intercept a data transmission in an encrypted VPN tunnel, they will not be able to decipher it.

3.1.6 Strong Password

use special characters "!@$#%", dont use account names, atleast 10 characters

3.1.7 Passphrase

pass phrase is more strong than a password, as it is longer and easier to remember, takes long time to brute force.

tips: choose statement, add symbols, longer = better, avoid common statements.

3.2.1 Encryption

Encryption is the process of converting information into a form in which unauthorized parties cannot read it. Authorized person with the secret key or password can decrypt the data and access it in its original form.

3.2.2 how to encrypt?

Software programs are used to encrypt files, folders and even entire drives. Encrypting File System (EFS) is a Windows feature that can encrypt data. It is directly linked to a specific user account and only the user that encrypts the data will be able to access it after it has been encrypted using EFS.

Steps:

select files-->properties-->advance-->"encrypt contents to secure data"-->done

see the files/folders that are encrypted appear green color

3.2.3 back up data

Having a backup may prevent the loss of irreplaceable data. 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.

storing options: Home, secondary location(usb,NAS,HDD), the cloud.

3.2.5 how to permanently delete data?

To erase data so that it is no longer recoverable, it must be overwritten with ones and zeroes multiple times, using tools specifically designed to do just that. SDelete from Microsoft, shred for Linux and Secure Empty Trash for Mac OS X. The only way to be certain that data or files are not recoverable is to physically destroy the hard drive or storage device.

3.3.1 Terms of Service

When signing up, you are prompted to sign a service agreement with the provider. You don't think too much about it and agree to all the terms without reading them.

TOS :a legally binding contract that governs the rules of the relationship between you, the service provider and others who use the service.

3.3.2 Understand the term

Terms of Service will include a number of sections, from user rights and responsibilities to disclaimers and account modification terms.

The data use policy outlines how the service provider will collect, use and share your data.

The privacy settings allow you to control who sees information about you and who can access your profile or account data.

The security policy outlines what the company is doing to secure the data it obtains from you.

3.3.6 consider the following before sign up

- Have you read the Terms of Service?
- What are your rights regarding your data?
- Can you request a copy of your data?
- What can the provider do with the data you upload?
- What happens to your data when you close your account?

3.3.7 protect your data

To protect your data and safeguard your account, you should:

always read the Terms of Service when registering for a new service and decide whether the service is worth waiving your rights to your data for

select your privacy settings rather than accepting the default

limit the group of people you share content with

review the service provider's security policy to understand what they are doing to protect your data

change your passwords periodically, use a complex password and two factor authentication to secure your account.

3.4.1 Two Factor Authentication

Two factor authentication to add an extra layer of security for account logins. Two factor authentication requires a second token to verify your identity.

Such as:

physical object such as a credit card, mobile phone or fob

biometric scan such as a fingerprint or facial and voice recognition

verification code sent via SMS or email.

hackers can still gain access to online accounts through phishing attacks, malware and social engineering.

3.4.2 Open Authorization

Open authorization (OAuth) is an open standard protocol that allows you to use your credentials to access third-party applications without exposing your password.

3.4.4 Spoof

Spoof is when an attacker impersonates a legitimate person, for example a spoofed email sent by attacker impersonating company boss will make the employees believe that their boss sent a legit attachment, but when they open attachment the malware script executes and infects the computer.

3.4.5 Email and Web browser privacy

These problems can be minimized by enabling the in-private browsing mode on your web browser.

When private mode is enabled, cookies are disabled. Therefore, any temporary internet files are removed and your browsing history is deleted when you close the window or program. This may help to prevent others from gathering information about your online activities. Even with private browsing enabled and cookies disabled, companies are constantly developing new ways of fingerprinting users in order to track their online behavior.

3.6 Quiz 100% (12/12)