Lecture – Protecting online identity

As the percentage of the population using the internet increases, so do the security risks.

Cyberthreats have become so widespread that the U.S. federal government has implemented a research and development department designed to formulate a plan to develop technology and create policies that minimize the potential risks in cyberspace.

With the rise in use of social media sites and networks, people are making more personal information available to the online world, making it more difficult to protect valuable data. Fortunately, there are a variety of ways to protect your own online identity and personal information.

Here are the top 10 ways you can protect yourself online:

1. Use Strong Passwords

The most common way to protect your online identity is to focus on creating strong passwords. When creating a password, choose something that will not be easily cracked or decoded. Never use a word or number that someone can associate with you such as a first, middle, or last name, a spouse or child's name, address, phone numbers, employers, or other identifying letters or numbers. Mix up the letters and numbers used in your password and use symbols and a combination of upper and lowercase numbers when possible in order to protect yourself from online security breaches. Additionally, it is important to never share your password with anyone. It might be necessary to change your passwords a few times each year.

2. Look for Encryption

Before making any sort of financial transaction online, look for signs that show whether the website is encrypted or not. To do this, look for two things: the trusted security lock symbols and the extra "s" at the end of http in the URL or web address bar. When you are on the page that's asking for your credit card information, the "http" changes to "https" when it is a secure site. At the same time, a lock symbol will also appear on the right side of the address bar or at the bottom left of your browser window. These two signals show that the site is encrypted, which means nobody will be able to see information as it's sent to the website owner. This keeps your name, phone number, address, credit card number and other sensitive information from being seen by anyone else.

3. Install Security Suites

Security suites are security programs that keep dishonest people and programs from infecting your computer and stealing information and data from you. This includes blocking harmful software such as spyware, viruses, and phishing scams that can be installed secretly when you are online. Some of the popular security suites include Norton Antivirus, McAfee Virus Protection, Ad-Aware Pro Security, and AVG Internet Security. Be sure to purchase and install one of these suites to protect your personal information online.

4. Turn on Web Browser Blacklisting

The lack of internet security is partially due to the internet browser being used. Many web browsers have additional security options such as blacklisting. This allows you to set the criteria for sites you will be navigating; only secure, trusted sites will be available to visit.

5. Avoid Phishing Scams

Phishing scams use a variety of methods to obtain your personal information and steal your identity. There are many different phishing scams out there, but they can be avoided by educating yourself on how to recognize them. To avoid being the victim of a phishing scam never open emails or attachments when the sender is unknown and don't click on unsecure links from strange emails. Additionally, avoid anyone offering money, unfamiliar job opportunities or requests for donations to charities as this might be a plot to obtain your personal information and online identity.

6. Get Private Data Protection

Another way to protect your online identity and sensitive information when sharing it online is to get private data protection. This type of security suite will protect any private data that is included in emails, private messenger programs, social media sites, or in various blogs. By employing a private data protection suite, you can further prevent hackers from gathering your personal information.

7. Password-Protect Your Wireless Router

A wireless router that accesses the internet at your home or business should always be password-protected. When you do not have a password on your wireless network, anyone in your range can use and access your internet, even a hacker. A hacker with experience committing cyber crimes will use this to their advantage and steal information from your computer while accessing your router. You should also enable the encryption feature on the wireless router, which scrambles any data you send online to further protect your sensitive data.

8. Hide Your Personal Information

It is possible to accidentally share your personal information with others if you don't set up your web browser properly. Any time you get a new computer or download and install a new browser, you can first configure it. To do this, you will access the "set-up" option on the browser and choose to configure the browser so that it doesn't reveal your name, email address or other information. Be sure to take this extra step when downloading or installing a browser to ensure your privacy and safety.

9. Enable Cookies on Your Web Browser Only When Required

Another option for setting up your browser to protect your online data is by enabling cookies only when required by a website. These cookies are details websites store on your computer, including information about what sites you visit and what you do there. Most of them keep the details to themselves, but this is also a way dishonest people get your information. You want cookies to be enabled, but to limit them only to websites that require it.

10. Protect Your Credit Card Info

Another option for setting up your browser to protect your online data is by enabling cookies only when required by a website. These cookies are details websites store on your computer, including information about what sites you visit and what you do there. Most of them keep the details to themselves, but this is also a way dishonest people get your information. You want cookies to be enabled, but to limit them only to websites that require it.