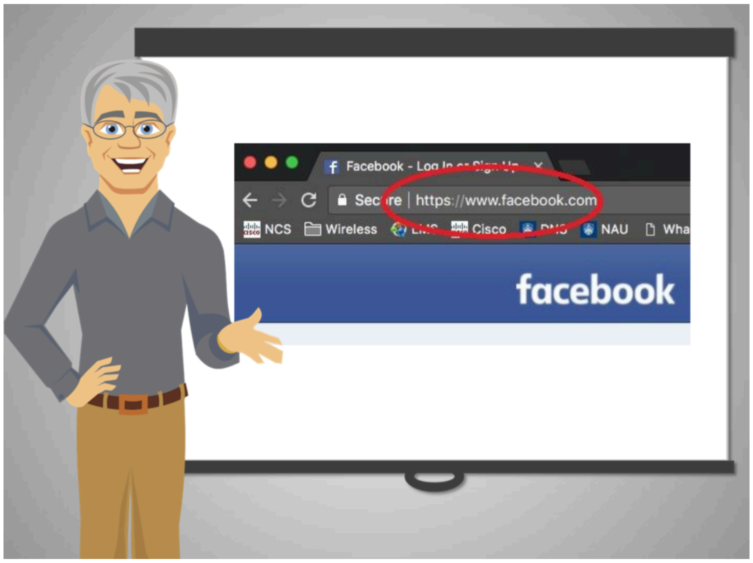
Be Proactive with Security

We just learned all about protecting your computer from malware, but how did Emily get malware in the first place?

Just like you can avoid being pickpocketed in a city by keeping your purse zippered up and not counting your cash in public, you can learn computer safety habits too.

Now, that Emily's computer is clean from malware, let's follow her as she learns more safety behaviors for when she goes online.


Facebook - Log In or Sign Up
Secure | https://www.facebook.com
NCS
Wireless
LMS
Cisco
DNS
NAU
Wha
facebook

Behavior # 1: Always check the website's URL

One indicator of a safe website is a trustworthy address bar. A safe website will always have a reasonable URL that is relevant to the site that you are visiting.

For example, if you are browsing Facebook, the URL should contain some form of "facebook.com"

You can hover over a link in most browsers to see where clicking will take you. The "https" in the beginning of a web address means that any data you send to the website will be secure and safe. Many browsers will also display a lock icon to show that a website is secure. If a website is reliable and represents a good authority, it will usually provide some sort of physical address or phone number that can be easily verifiable.

As a general rule of thumb: if there are any claims that are 'too good to be true', it almost always is. If an email or notice says you just won money or that you must respond immediately to claim it, be very suspicious.

When you're logging in somewhere or submitting secure information, make sure to pay attention to these signs or ask someone before entering personal or financial information.

Congratulations You Won!!!

It is not a joke
You are the 100,000th visitor of the day!

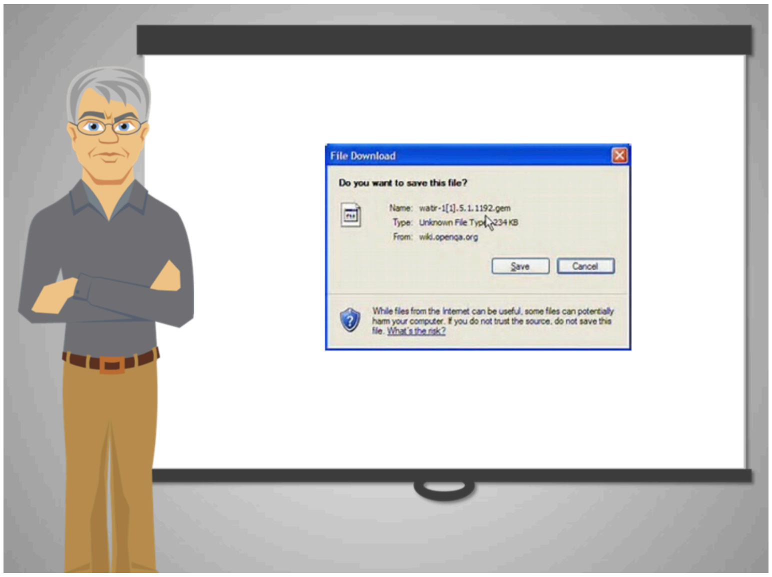
Claim your winnings?

Behavior # 2: Stay away from pop-up windows

Safe and credible websites usually do not appear as pop-ups; pop-up windows should be treated with extreme suspicion and closed as soon as possible.

Be wary of any windows that appear suddenly!
Pop-ups are usually “too good to be true”
Be smart of where you click and browse!

For more tips on avoiding unsafe websites, check out the course Online Scams.



File Download

Do you want to save this file?

Name: watir-1[1].5.1.1192.gem

Type: Unknown File Typ 234 KB

From: wiki.openqa.org

While files from the Internet can be useful, some files can potentially harm your computer. If you do not trust the source, do not save this file. What's the risk?

Behavior # 3: Avoid downloading unfamiliar files

Accidentally downloading something is a major cause of installing malware onto someone's computer. Think first, then click. Always ask yourself: Do I actually need to download anything?

Many buttons that look like friendly downloads will cause malware to be installed. If you see something is downloading without your permission, stop the download immediately.

You should not open any files you have downloaded that you are unsure of.

Always check with someone before you run a suspicious program!

When you are ready, click next to continue.

Behavior # 4: Be careful when using public Wi-Fi

An open Wi-Fi hotspot means that you can connect to without having to enter a password. Common places where public Wi-Fi is available are libraries, cafes, restaurants, parks, airports, and other retail stores.

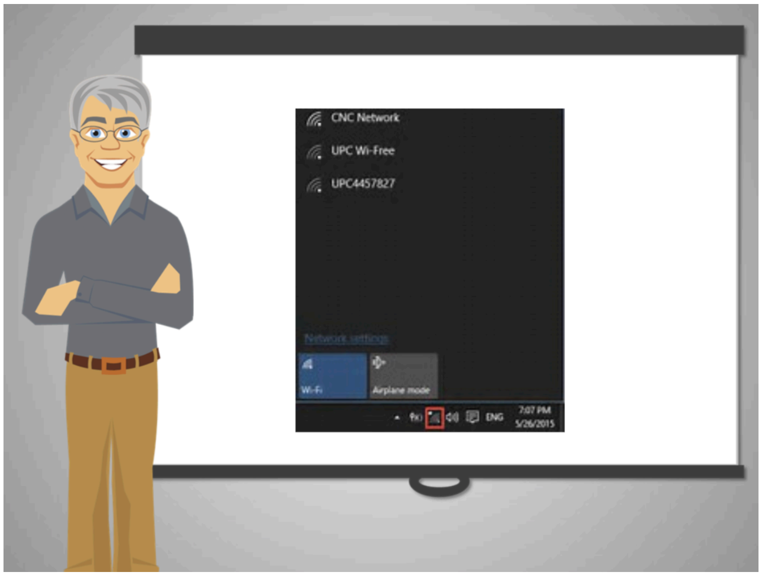
If you are using your credit card online, you should probably use a wired connection or use a desktop computer that has a wired connection.

Whenever you connect to a public Wi-Fi, without using a password, it is possible for other people on the network to see what you are doing and who you are.

Of course, it doesn't always happen, but just like your belongings can be stolen when you are not careful in a public place, people can look at information you submit online in a public network, and they may try to steal your information if you are not careful.

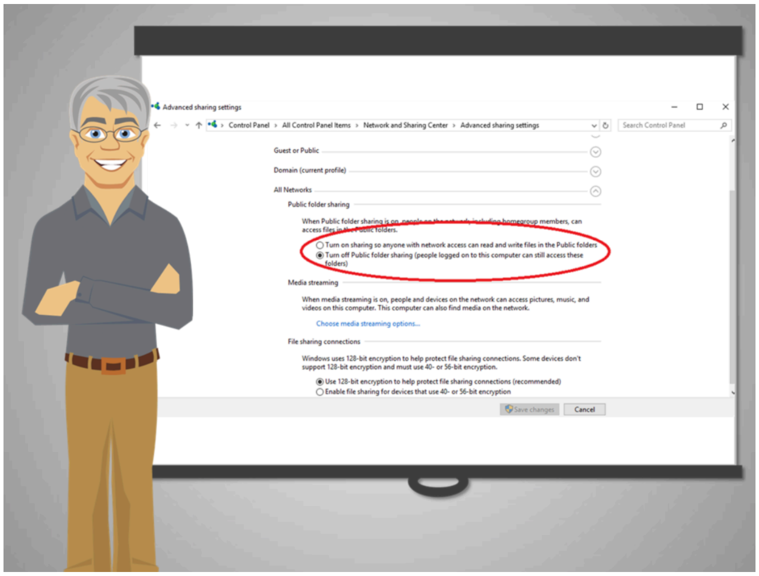
It's always best to be cautious and build good habits to keep yourself safe.

Here is what you can do to be careful when using a public Wi-Fi:



Select a network that is trusted!

Don’t automatically connect to the first Wi-Fi you see and don’t select Wi-Fi names that are suspicious or unexpected. For example, if you are in a library, select the Wi-Fi that seems official. Some people will try to set up public wi-fi’s that are similarly named to the real thing in order to steal your information. If in any doubt, ask someone who would know!


Advanced sharing settings
Control Panel › All Control Panel Items › Network and Sharing Center › Advanced sharing settings
Search Control Panel
Guest or Public
Domain (current profile)
All Networks

Public folder sharing

When Public folder sharing is on, people on the network, including homegroup members, can access files in the Public folders.

○ Turn on sharing so anyone with network access can read and write files in the Public folders
● Turn off Public folder sharing (people logged on to this computer can still access these folders)

Media streaming

When media streaming is on, people and devices on the network can access pictures, music, and videos on this computer. This computer can also find media on the network.

Choose media streaming options...

File sharing connections

Windows uses 128-bit encryption to help protect file sharing connections. Some devices don't support 128-bit encryption and must use 40- or 56-bit encryption.

● Use 128-bit encryption to help protect file sharing connections (recommended)
○ Enable file sharing for devices that use 40- or 56-bit encryption

Check if the file sharing option is turned off – Most devices have an option to turn sharing off, because with sharing turned on, you allow anyone to freely roam your device and take whatever they like from you.

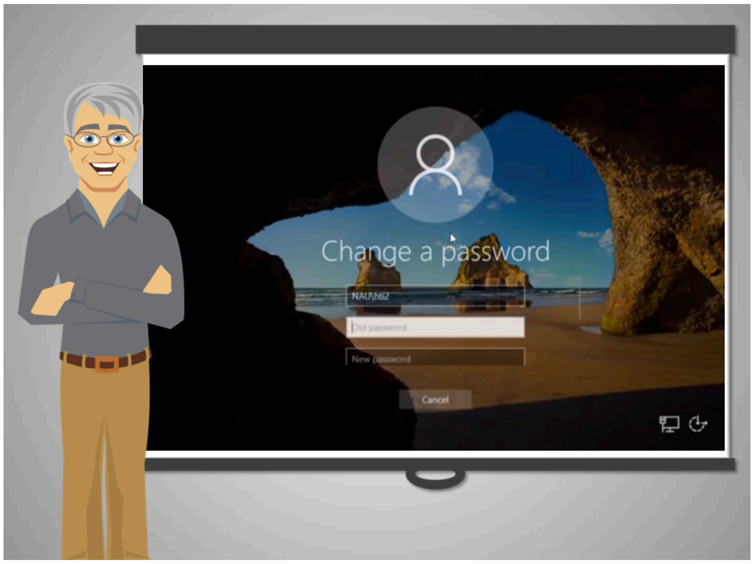
Secure
https://

Check for HTTPS; this will help indicate that people on the same network will not be able to intercept your data. Remember, if you're logging in somewhere, make sure that there's https in the address bar, and then it's a safe website!

Name
Second name
Initials
Address
Tel
Email

Never submit personal information when using a public Wi-Fi. Public Wi-Fi is good for browsing, but not for submitting personal or financial information.

If you are planning to check your bank account or look at other sensitive information, it is best to do it in a private network.



Change a password

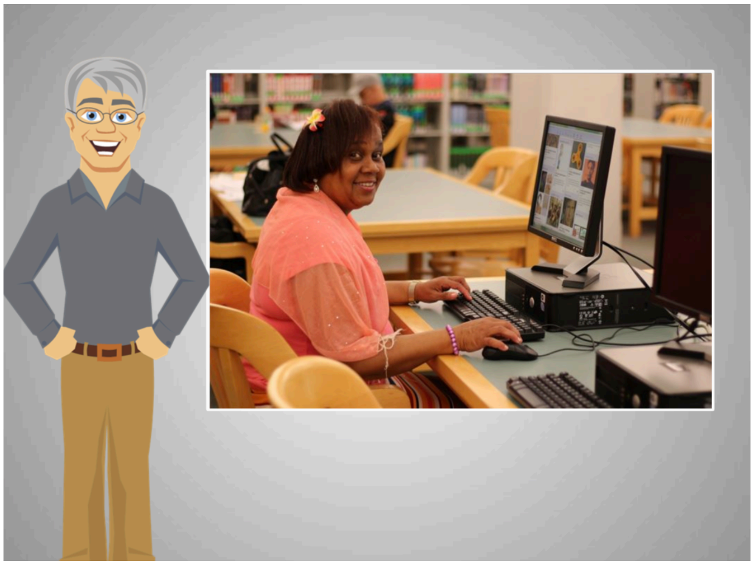
NAU\hti2

Behavior # 5: Password protect your personal computer.

In case someone access your computer without your consent, the password will prevent them from getting access to the data stored in it.

To add or change your password, open the Control Panel from the Start menu and then choose the User Accounts icon. Then choose either Create a Password or Change Your/My Password to add or update a password on your account. Follow the directions on the screen for entering or deleting your password.

This process may not be as easy the first time you do it. Ask a trusted friend to help you if following the directions on the screen gets confusing to you. Write down the password and keep it in a safe place in case you forget it.



Emily’s computer was slow as a consequence of not updating her software, not using protective software or navigating insecure websites.

Now Emily knows it and you do too:

Be careful of anyone asking for sensitive information – always verify!
Stay sharp with emails, popups, and suspicious websites
Update software, check identities, verify URLs, read carefully, know the signs!

Now that Emily’s computer problem is fixed, she is ready to be back online and using her computer to make her life easier and more fun.

Built by Microsoft

Microsoft

DIGITALLEARN.ORG
A PLA INITIATIVE