Security Update: Think before you download

There's a free app you've wanted to get or a cool game your child wants to download. Think before you download anything! According to the latest cybersecurity report from Microsoft, "deceptive downloads" are currently the top online threat.

Deceptive downloads are actually legitimate programs (such as apps, games, music or software) that criminals have tampered with to include malicious items.

Here's how it works. Your friend sends you a link to a great game for you to try. You install the game, not knowing that you are also installing malware. This malicious software might access your personal information on your computer or device or even hijack your computer and use it for cybercrime. Unfortunately, it could be months or even years before you notice your system has malware.

Tips to avoid deceptive downloads?

- Think before you click a link and only download software from websites you trust.

- Turn on automatic updating so that you're always using the latest, most secure versions of the software installed on your computer.

- Make sure you're using antivirus software and that it is current.

- While there are no guarantees that a website or link is safe, there are some questions to ask before accessing the site:

    - Did you get the link in an unsolicited email? If you don't recognize the sender, don't open the email or click on the link.

    - Did you read the link? If the link is misspelled or isn't what you'd expect it to be, don't click it.

    - Does the link begin with https? If it doesn't begin with https, don't enter credentials or other personal information.

    - Is there a lock icon in the address bar (typically this indicates a more secure connection)? If so, click the lock and review the security certificate for the site.

    - Does your browser display a certificate warning message when you click on the link? If it does, don't click on the link.

Happy surfing.