10 Ways To Not Get Hacked

Explanation:

In this current Computer Age, you hear more and more of Cyber-Attacks against Governments, Companies, and frankly anyone connected to a computer. Which includes sharing personal or finical information along with downloading and installing unknown infectious software. However, there are common everyday steps you can take to help prevent you from being an easy target, whether you're at work or at home.

Instructions:

Things to look for:

1. **Take time to Recognize Phishing Emails:**
    - Many times attackers spread Malware though email attachments. Remember, hackers are trying to get you to **respond quickly**, so do the following:

    A. If you see this **Orange** GoTriangle banner **carefully check their email address**.

    CAUTION: This email originated from outside GoTriangle. Do not click links or open attachments unless you recognize the sender and know the content is safe.

    B. Don't completely ignore spelling, punctuation, and grammatical errors.

    C. Always ask the question **"DOES THIS EMAIL MAKE SENSE"** ***For Example, would the CEO ask me for a quick favor or purchase him a gift card.***

    D. If you're in doubt, feel free to call them or their company and verify before taking any further suggested actions. **Remember, if the senders email was hacked someone else may be replying to your email. So use the phone number off their website and not the phone number listed on the email.**

2. **Install and Update your Antivirus Software:**
    - Software manufacturers are constantly patching holes and back doors within software, in an effort to stop criminals from gaining access to your computer. However, this will only work if you consistently update the Antivirus and Software on your computer.

3. **Use 2 Factor Authentication (2FA):**
    - Where possible enable 2FA, this will allow you to receive a confirmation code on your cell phone in order to confirm your identity. **For example, even if your computer was hacked, the Hacker will not have access to your cell phone.**

4. **Do Not use same password everywhere:**
    - For obvious reasons, if the hacker gets into one account, then they'll have access to other more important accounts. **So use Unique Passwords for each login.**

5. **Do Not 'Save Passwords' in Browsers:**
    - When you're on the Internet you leave a digital trail that can be easily followed by hackers, for that reason it's best to **NOT** allow your browser to store your passwords. Since this information is stored on the computer, you can be sure the Hackers malicious software can find it.

6. **Be careful with how much info you post online:**
    - Criminals are constantly monitoring Social Media, **"It's their Job**". The more you post the more they know, such as when you're on vacation and what's in your home.

7. **Stay away from FREE software sites:**
    - Oftentimes hackers will imbed malicious software in FREE programs just for that reason. ***"Everyone wants something for FREE"***

8. **Avoid Pop-Ups:**
    - **NEVER – Click Here to WIN your Prize.** If you receive a pop-up, **just close it**, usually by clicking the **X** in the Upper-Right corner.

9. **Be careful when sharing personal information:**
    - Legitimate baking institutions will **NEVER** ask for your Account Information, in an unsolicited email or phone call. For example, if you bank at Wells Fargo but receive an email from Chase Bank **"Don't Click any Account Links"**. Instead, call the bank with a known working number **NOT** the number provided in the possibly fraudulent email.

10. **Be Cautions about Downloading Anything from the Internet:**
    - When in doubt, **"Don't Click to Find Out"** Don't let your Curiosity get the best of you.