'Tis the Season for HOLIDAY SCAMS

Here are some tips on how to be Cyber Smart when shopping online during this holiday season

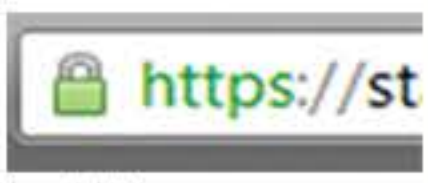
Click Cautiously

Cyber criminals can attack your computer through links and email attachments. Don't click on anything from unknown senders and when receiving e-greeting cards, coupons, or other mail from friends and family, verify that they've sent it before opening!

Review New Websites Before Shopping

It's easy for cyber criminals to create fake online stores with too good to be true deals in order to obtain your credit card information. Do a web search and check for reviews for new online stores.

Remember, secure websites are indicated with a lock symbol in the browser window and/or a "https" in the URL.



Watch Out For Fake Shipping Notices

Phishing attacks can also come through fake shipping notices. Official shipping notices from carriers such as FedEx and UPS come with tracking numbers that **you can enter into the website instead of clicking on links within the email.**

Restrict Your Exposure To Credit Card Theft

If possible, use only one credit card with little or no balance for all your online purchases. At the end, you'll only have one credit card balance to pay off and only one card will be exposed.

Use Different E-mail Accounts

Your emails and passwords for your bank accounts should be different from your personal shopping accounts. Using a variety of logins ensures that if one is compromised, all won't be in jeopardy. **Also, avoid using your Hostos email address.**

What To Do If...

YOUR CREDIT CARD HAS BEEN COMPROMISED

- Contact the credit card company
- Monitor your accounts
- File a police report with the FTC (Federal Trade Commision)

YOU'VE ACCIDENTALLY CLICKED ON A PHISHING LINK

- Update your Anti-virus protection **(Free McAfee software is available through CUNY Portal)**
- Perform a computer Scan
- Change your account logins and passwords

YOUR IDENTITY HAS BEEN STOLEN

- Place a fraud alert with the credit bureau agencies
- Monitor your credit reports
- Contact any company that might have been affected (i.e. Social Security Administration, IRS, etc.)

CONTACT THE IT SERVICE DESK (X6646) IMMEDIATELY IF YOUR WORKSTATION PC HAS BEEN COMPROMISED

Stay Away From Pop-Ups

Don't click on pop-ups, no matter how rewarding or authentic they may seem. Turn on the option for blocking pop-ups on your browser. If you run into a pop-up, don't click the "Ok/Cancel" buttons. Instead, close the window by clicking the "x" in the top right corner or press **"Alt + F4"** on a PC or **"Command + W"** on a Mac.

Back Up Your Data Often

In the event of a ransomware attack, you will need to restore your computer files from a back-up that is not connected to your computer such as an external hard drive.

Phishing - An attempt to obtain personal, financial or other confidential information from someone, usually through an email that appears to be from a legitamate source but contains a link to a fake or replicated website

Ransomware - A type of malicious software designed to block access to a computer system until a sum of money is paid to the hacker.

For more information on how to stay Cyber Smart, visit, www.Hostos.cuny.edu/IT

Hostos Community College