Week 2: Cybersecurity Awareness Month - Staying Safe Online

The overwhelming consensus in material about online safety is that scammers and hackers “take advantage of your kindness.”

Think about that. It is difficult to imagine an audience more helpful and kind than the SSNDs. We educate and we serve. It is integral to who we are. Unfortunately, that innate desire to be responsive makes us more susceptible to scams.

Before we launch into what to do to stay safe online, and what to do if you fail to stay safe, consider your *approach* when using the internet.

1. **Trust your instincts.** If you feel pressured or uncomfortable by anything you encounter online, disengage.
2. **Be suspicious** of those contacting you whether it is through a pop-up, ad, or email.
3. **Bring your skeptic.** You are not obliged to engage, respond, or be friendly. Mistrust anything that sounds urgent.

Below is a sample list of situations you could encounter online.

Pop-up Ads – Pretend to be from a notable company such as Apple or Microsoft and notify you that something is wrong with your device or offer an opportunity.
Tech scams – Claim to be tech support and that an issue has been found with your computer and that you should call for help or download software.
Charity scams – Seek your money to help a worthy cause.
Government scams- Claim to be employees of an entity that demands payment or information.
Links – Often appear in an email from an organization or a person who wants to share information with you.

DON’T CLICK THAT SUSPICIOUS LINK!

Your gut instincts are your best defense against phishing.

CYBERSECURITY AWARENESS MONTH

And if you find yourself in these situations.

- Do not click on ads. Go to the official webpage of the store/vendor instead.
- The IT Department of SSND connects with you via the phone, our help desk email address [helpdesk@ssndcp.org], our Connections newsletter or CP Announcements. Period.
- Avoid charity scams by seeking out the organization yourself to donate. Double-check email addresses to verify the sender.

- Do not download attachments or click on links unless you know the person and/or are expecting something.
- No reputable organization will use threats or demand immediate payment.
- Verify any site, service, or company, especially when you provide information. If in doubt, **call the source**.

Even if you have done your best to ensure your online usage is secure, you can be hacked or tricked. If you suspect this is the case:

1. Turn off your computer.
2. Call the SSND help desk immediately at 1-800-373-7521.
3. Call the SSND finance team if you have shared personal information.
4. Change passwords to your accounts if you are able.

Finally, a couple of helpful reminders about online security.

Panda is our security software and if a box presents and wants you to restart your computer, do not put it off indefinitely. This update protects your computer.

Know that the SSND IT team is here to help you. **Please use us!** We would much rather offer help *before* anything happens, than after when the damage is done. Call 1-800-373-7521 or email us at helpdesk@ssndcp.org.