OFFICE OF NASSAU COUNTY
COMPTROLLER JACK SCHNIRMAN

FACT SHEET

CYBERCRIME PREVENTION TIPS

Scammers love a crisis, and it becomes harder to determine what information is trustworthy. A good rule of thumb is that anything that seems too good to be true is not true. *Stay Vigilant!*

Current Scams

Contact-Tracing Scams: Contact tracing is the process of identifying people who have come into contact with someone who has tested positive for COVID-19, instructing them to quarantine and monitoring their symptoms daily.

🔒 People who have had contact with someone infected with COVID-19 may first get a text message from the health department, telling them that they'll get a call from a specific phone number. The tracer who calls will not ask for personal information. Tracers won't ask for money or for information such as Social Security number, bank account, or credit card number. Anyone who does is a scammer.

According to the Federal Trade Commission, scammers pretending to be contact tracers are taking advantage of how the process works and are sending text messages.

However, messages from scammers are spam text messages that ask to click a link. Unlike a legitimate text message from a health department, which only wants to notify that they'll be calling, this message includes a link to click.

Source: Federal Trade Commission

IRS Scams

IRS Scams: According to the IRS, everyone should be alert for scammers calling, texting and emailing about the coronavirus or COVID-19, including about Economic Impact Payments. These scams can lead to tax-related fraud and identity theft. What you need to know:

🔒 The IRS will not call, email or text you to verify or request your financial, banking or personal information.

🔒 Watch out for websites and social media attempts to request money or personal information. IRS.gov is the official website.

🔒 Don't open unexpected emails that look like they're coming from the IRS or click on any attachments or links. Don't engage potential scammers. Forward suspicious emails to *phishing@irs.gov*.

JUNE 2020

Password Tips

Change passwords often and use a password with additional complexity so hackers have more difficultly cracking your account.

- Don’t use names of people or pets.
- Don’t use lucky numbers such as the birthday for anyone you may know.
- Use a number within the password which will make it more difficult to guess. Examples: Instead of “Tokyo2020” use “T20ok20yo” or rather than “LauraLI66” use “L19uaraLI66.”
- Avoid using the same password for internal and external applications (e.g. Zoom, Google, etc.).

Don't respond to calls, texts, or emails about money from the government

Or from anyone asking for your personal or bank account information. Government agencies, like the IRS will not call, text, or email you about your relief payment.

Hang up on robocalls and research before you donate.

Scammers use illegal sales call to get your money and your personal information. Don't let anyone rush you into making a donation.

Watch out for phishing emails and text messages.

Don't click on links in emails or texts that you didn't expect.

Source: Federal Trade Commission

Tips for Using Zoom, Teams, and Other Conferencing Platforms

Many of us are using Microsoft Teams and Zoom to hold meetings and work collaboratively. These platforms, however, may not always be entirely secure, so it is important to remain vigilant. Here are some safety tips for using Zoom, Microsoft Teams, and other online platforms:

- Make sure that you are communicating with the people you intend. In Teams, it is easy to type a name to start a chat and someone with a similar name from your contact list comes up and is sent a message or is joined to a group in error.
- Be careful with the information shared during these online calls and avoid sharing sensitive documents as attachments. Send emails with attachments before, during, or after the call directly to the participants.
- Monitor who is actually in the session and identify any attendees you do not recognize before starting the meeting. For example, do a roll call to confirm each person who is in the meeting.
- Visual backgrounds are nice to help personalize your session but also be careful where they come from. Only obtain backgrounds from verified sources from the vendor as others may be vulnerable or pose a security risk.