NASSAU COUNTY

SPiN

A Crime Prevention Partnership

SECURITY / POLICE INFORMATION NETWORK

THOMAS R. SUOZZI
County Executive

JAMES H. LAWRENCE
Commissioner

USE STRONG PASSWORDS TO HELP PROTECT YOUR INFORMATION

- Using passwords that have at least eight characters and include numerals and symbols.
- Avoiding common words: some hackers use programs that can try every word in the dictionary.
- Not using your personal information, your login name, or adjacent keys on the keyboard as passwords.
- Changing your passwords regularly (at minimum, every 90 days).
- Using a different password for each online account you access (or at least a variety of passwords with difficulty based on the value of the information contained in each.

BACK UP IMPORTANT FILES

No system is completely secure. If you have important files stored on your computer, copy them onto a removable disc, and store them in a secure place in a different building than your computer. If a different location isn't practical, consider encryption software. Encryption software scrambles a message or a file in a way that can be reversed only with a specific password. Also, make sure you keep your original software start-up disks handy and accessible for use in the event of a system crash.

ANTI-VIRUS SOFTWARE

Anti-virus software protects your computer from viruses that can destroy your data, slow your computer's performance, cause a crash, or even allow spammers to send email through your account. It works by scanning your computer and your incoming email for viruses, and then deleting them.

To be effective, your anti-virus software should update routinely with antidotes to the latest "bugs" circulating through the Internet. Most commercial anti-virus software includes a feature to download updates automatically when you are on the Internet.

PHISHING – BAIT OR PREY

"Phishers" send spam or pop-up messages claiming to be from a business or organization that you might deal with for example, an Internet service provider (ISP), bank, online payment service, or even a government agency. The message usually says that you need to "update" or "validate" your account information. It might threaten some dire consequence if you don't respond. The message directs you to a website that looks just like a legitimate organization's, but isn't. What is the purpose of the bogus site? To trick you into divulging your personal information so the operators can steal your identity and run up bills or commit crimes in your name.

Don't take the bait: don't open unsolicited or unknown email messages; don't open attachments from people you don't know or don't expect; and never reply to or click on links in email or pop-ups that ask for personal information. Legitimate companies don't ask for this information via email. If you are directed to a website to update your information, verify that the site is legitimate by calling the company directly, using contact information from your account statements. Or open a new browser window and type the URL into the address field, watching that the actual URL of the site you visit doesn't change and is still the one you intended to visit.