IDENTITY THIEFT

UPS/FedEx/USPS Virus - verified IMPORTANT

With the recent cyber-attack on USPS employees NAPS Branch 105 Officers would like to take this opportunity to remind you that spammers are becoming more and more clever in tricking users into thinking their unsolicited email is worth opening. Many of you are aware enough to identify what is real and what is bogus, but there are still people out there still have a difficult time spotting a phishing email.

Currently, there is a scam email going around advising the recipient that the Post Office has attempted to deliver a package unsuccessfully and all you need to do is download the form and take it to your Post Office. The download is a virus. This scam can also appear to be from UPS or Fedex. Read more here: http://www.bbb.org/council/news-events/bbb-scam-alerts/2014/06/scam-alert-fake-usps-emails-carry-a-virus/

If you receive an email from a sender you are not familiar with, do not do business with, asks for personal information such as passwords, accounts numbers or banking information do not click on any links in the email or respond to it. Just delete it.

If you ignore them (delete them) most of the time they will go away because they did not get a response from you.

Use you browser's anti-phishing capabilities to help protect you from phishing websites.

There are many websites to help you learn how to identify spam, here are two:
http://www.ehow.com/how_2003326_identify-email-spam.html
http://www.wikihow.com/Spot-an-Email-Hoax-or-Phishing-Scam

This one will help you understand Identity Theft

http://www.consumer.ftc.gov/features/feature-0014-identity-theft
https://www.fdic.gov/consumers/theft/
http://www.justice.gov/criminal/fraud/websites/idtheft.html
http://www.fbi.gov/about-us/investigate/cyber/identity_theft

There are many no-cost ways to protect yourself: *

- Review your bank and credit card accounts often, daily or weekly, and look for withdrawals or purchases that you did not make.
- Protect your account numbers and passwords. **Never** save passwords on any computer is that not even your own personal computer. That is one of the first places malware will go to get your information.
- Change your passwords monthly and make them strong. Make use of special characters, uppercase and lower case letters and spaces if allowed.
- Do not use the same password for everything. Using multiple passwords for your financial institutions can limit the damage.
- Designate one credit card for online purchases. Credit cards have better protection under federal law than debit cards.
- Always watch for phishing which can be disguised to look like a legitimate business or bank. If you are unsure that it is a phishing attempt, do not click on anything in the email. Rather, contact the institution using their contact information that you know is accurate.
- Take advantage of the annual **free** credit report from each of the 3 credit reporting bureaus: Equifax, Experian and TransUnion. It is recommended that you order one every four months using a different bureau each time. You can order the report directly through each agency, or at annualcreditreport.com. Review the information and be alert to any new accounts that have been opened. New-account frad is more difficult to detect because the thief will not use your address and ou will never see the bills. Remember you do not need to pay for this information. Avoid the many sites that will charge you for this information.
- Use a shredder for sensitive documents such as old bank statement, bills, credit card or any other type of financial applications and anything else that has your personal information on it before recycling it.
- Be smart about using social media. Do not share personal information like you actual birthday or home address. Do not share information that could be used as an answer to security questions, such as your mother's maiden name. Set your privacy levels to high.

- Keep your anti-virus, anti-malware, anti-spyware up to date. There are many internet security packages out there that will update definitions and scan your computer automatically.
- Do not do online banking on an unsecure network at a restaurant, café, or even a library.
- Make sure your home network is secure

*From wsj.com