

CITYWIDE INFORMATION SECURITY AWARENESS NEWSLETTER

News from DoITT's Information Security Team

INSIDE THIS ISSUE: October is National Cyber Security Awareness Month



- [National Cyber Security Awareness Month](#)
- [Use Strong Passwords](#)
- [Dispose of Information Properly](#)
- [Beware of Phishing Emails](#)
- [Protect Mobile Devices](#)
- [Resources for More Information](#)

NATIONAL CYBER SECURITY AWARENESS MONTH

October is National Cyber Security Awareness Month — a good time to summarize common themes and review key ways in which we can easily improve our level of safety and online security.

In knowing how to use strong passwords, how to securely dispose of information, how to be watchful for phishing scams, and how to protect our mobile devices, we can take significant steps in protecting ourselves and our families in this rapidly changing world of cyber-security.

Several of these topics have been covered in this year's Security Awareness Newsletters - this issue serves as a handy reminder of the steps we can take to protect ourselves.

USE STRONG PASSWORDS

1. Make your passwords long and complex. The longer and more "complex" your passwords are, the more difficult they will be to guess. Passwords including at least one character from each of the following categories are more complex than those containing only letters and/or numbers:

Alphabetic characters: Aa, Bb...Zz

Numeric characters: 0 1 2 3 4 5 6 7 8 9

Special characters: { } [] , . < > ; : ` " ? / | \ ` ~ ! @ # \$ % ^ & * () _ - + =

2. Avoid dictionary words. Your passwords will be stronger if you avoid using words which can be found in a dictionary. Also avoid common phrases, names of people, friends, family, pets, places, sports teams, hobbies, sequences and repeated characters. For example, fido123, nygiants and Betty222 are weak passwords.
3. If you must write down a password, you should store and protect the document on which it is written appropriately to prevent disclosure to anyone other than yourself.

4. Never share passwords and never send them in email. Sharing passwords can open the door to potentially significant loss of information, assets, privacy, accountability, and reputation.

DISPOSE OF INFORMATION PROPERLY

1. When the time comes to retire a computer, laptop, mobile phone, USB thumb drive, or other portable device, be sure to permanently wipe any sensitive data from the device's internal memory and hard drives.
2. Remove SIM cards from mobile phones.
3. Shred any media (print-outs, credit cards, CDs, DVDs, etc.) containing personal or sensitive information.

BEWARE OF PHISHING EMAILS

1. Avoid giving out personal information on social networking sites such as Facebook and LinkedIn and set your privacy and security settings at the most restrictive levels for these sites. This limits the information scammers can gather about you (which can be used against you in a phishing attack).
2. Open web pages from bookmarks which you have personally set or, even better, by typing in their URLs.
3. Since email addresses can be "spoofed" (faked) you should be cautious with all emails you receive, including those which appear to be from friends and "trusted entities." Ask yourself whether the email is really from whom it appears to be and if you are unsure, contact the sender by telephone to verify the message. Do not respond to unsolicited emails requesting personal information nor to those which ask you to "verify your information" or "confirm your user-id and password."
4. Be cautious with links contained in emails, even from friends and sources you normally trust. Do not open any attachments contained in suspicious emails and do not respond to unsolicited pop-ups.
5. Do not participate in chain-letters (chain emails).
6. If an email appears to be a phishing attack, do not respond to it and, except for reporting it, do not forward it. Instructions for reporting phishing attacks to the Federal Trade Commission are available at this link:

[Reporting spam to the Federal Trade Commission](#)

PROTECT MOBILE DEVICES

1. Use your phone's password lock feature. Enable the option on your phone which will automatically lock the device after it has been idle for a pre-set time period. Use a password or pin which is difficult to guess and change it periodically.
2. Avoid storing passwords for online accounts. If your phone remembers passwords for websites you visit often (a.k.a. auto-fill), turn this feature off. This is particularly important for your online accounts which contain personal or financial data. The convenience is probably not worth the risk.
3. Use Wi-Fi with caution. Turn Wi-Fi service on your phone off when you are not using it. This lowers the risk of connecting to an insecure or suspect network and saves battery life. If you do not recognize a Wi-Fi access point or if you are not sure whether it is secure, don't connect to it.
4. Keep the software on your phone up-to-date. Periodically check your phone provider's website for updates and apply any available software and security patches.
5. Be careful with apps. Do research on apps that you install on your smartphone. Apps are great, especially when they're free, but can come with the hidden price of malware, spyware, and other security issues. A bit of due diligence in checking reviews on an app can save a lot of time and trouble in the long run.

6. Take advantage of the mobile security applications and services which are available for your phone. Software applications and services (e.g., remote-wipe) are available to guard the data on your mobile phone from many known security threats. Consult your mobile phone provider for more information and consider utilizing these offerings which can significantly improve the security of your mobile device.
7. Avoid "jailbreaking" or "rooting" your phone. If you feel inclined to customize your phone by tampering with its operating system in order to circumvent vendor restrictions, remember that this will usually void the vendor's warranty and disable the phone's security features.
8. Backup your data. As always, this simple measure is essential if you want to avoid losing your data if your phone is lost, stolen, or broken.

RESOURCES FOR MORE INFORMATION

NY State Division of Homeland Security

[October Cyber Security Awareness Month](#)

NY State Division of Homeland Security

[Kids Safe Online NYS Poster Contest](#)

April 2011 Security Awareness Newsletter

[Security Tips for Personal Smartphone Users](#)

May 2011 Security Awareness Newsletter

[Phishing and Identity Theft Alert](#)

June 2011 Security Awareness Newsletter

[Spear Phishing Alert](#)

Sept 2011 Security Awareness Newsletter

[Phishing Alerts - Fake Traffic Tickets](#)

Citywide Information Security Policies and Standards are available at:

<http://cityshare.nycnet/infosec>

Please report security violations, issues, and questions to the Citywide Service Desk at:

(212) NYC-HELP or (212) 692-4357

PLEASE DO NOT REPLY TO THIS MESSAGE