NEW YORK STATE OF OPPORTUNITY. | Office of Information Technology Services

Cyber Security Dos and Don'ts

Cyber security is the shared responsibility of every agency employee and business unit. YOU play a key role in properly safeguarding and using private, sensitive information and state resources. The following Dos and Don'ts help remind us all of actions we must take to remain vigilant.

- DO use hard-to-guess passwords or passphrases. A password should have a minimum of 10 characters using uppercase letters, lowercase letters, numbers and special characters. To make it easy for you to remember but hard for an attacker to guess, create an acronym. For example, pick a phrase that is meaningful to you, such as "My son's birthday is 12 December, 2004." Using that phrase as your guide, you might use **Msbi12/Dec,4** for your password.

- DO use different passwords for different accounts. If one password gets hacked, your other accounts are not compromised.

- DO keep your passwords or passphrases confidential. DON'T share them with others or write them down. You are responsible for all activities associated with your credentials.

- DON'T leave sensitive information lying around the office. DON'T leave printouts or portable media containing private information on your desk. Lock them in a drawer to reduce the risk of unauthorized disclosure.

- DON'T post any private or sensitive information, such as credit card numbers, passwords or other private information, on public sites, including social media sites, and DON'T send it through email unless authorized to do so. DO use privacy settings on social media sites to restrict access to your personal information.

- DO pay attention to phishing traps in email and watch for telltale signs of a scam. DON'T open mail or attachments from an untrusted source. If you receive a suspicious email, the best thing to do is to delete the message, and report it to your manager and Information Security Officer (ISO)/designated security representative.

- DON'T click on links from an unknown or untrusted source. Cyber attackers often use them to trick you into visiting malicious sites and downloading malware that can be used to steal data and damage networks.

- DON'T be tricked into giving away confidential information. It's easy for an unauthorized person to call and pretend to be an employee or business partner. DON'T respond to phone calls or emails requesting confidential data.

- DO destroy information properly when it is no longer needed. Place paper in designated confidential destruction bins throughout the office or use a crosscut shredder. For all electronic storage media, consult with IT.

- DO be aware of your surroundings when printing, copying, faxing or discussing sensitive information. Pick up information from printers, copiers or faxes in a timely manner.

- DON'T install unauthorized programs on your work computer. Malicious applications often pose as legitimate software. Contact your IT support staff to verify if an application may be installed.

Enterprise Information Security Office
Website: www.its.ny.gov/eiso
Phone: 518-242-5200 | Email: eiso@its.ny.gov

- DON'T plug in portable devices without permission from your agency management. These devices may be compromised with code just waiting to launch as soon as you plug them into a computer.

- DO lock your computer and mobile phone when not in use. This protects data from unauthorized access and use.

- DON'T leave devices unattended. Keep all mobile devices, such as laptops and cell phones physically secured. If a device is lost or stolen, report it immediately to your manager and ISO/designated security representative.

- DO remember that wireless is inherently insecure. Avoid using public Wi-Fi hotspots. When you must, use agency provided virtual private network software to protect the data and the device.

- DON'T leave wireless or Bluetooth turned on when not in use. Only do so when planning to use and only in a safe environment.

- DO familiarize yourself with your responsibilities under the NYS Acceptable Use of IT Resources Policy (http://www.its.ny.gov/document/acceptable-use-information-technology-it-resources-policy). Review and follow NYS Information Security Policies and related standards (http://its.ny.gov/eiso/policies/security).

- DO report all suspicious activity and cyber incidents to your manager and ISO/designated security representative. Challenge strangers whom you may encounter in the office. Keep all areas containing sensitive information physically secured, and allow access by authorized individuals only. Part of your job is making sure NYS data is properly safeguarded, and is not damaged, lost or stolen.

The New York State Office of Information Technology Services Enterprise Information Security Office is dedicated to protecting privacy; safeguarding the State's information assets and infrastructure; identifying and mitigating vulnerabilities; detecting, responding and recovering from cyber incidents; and promoting cyber awareness and education. We stand ready to assist and support you in your cyber security risk management efforts.

Remember - cyber security is everyone's responsibility!

Enterprise Information Security Office
Website: www.its.ny.gov/eiso
Phone: 518-242-5200 | Email: eiso@its.ny.gov