What is Ransomware?

Ransomware generally presents users with an ultimatum: pay a fee to unlock and reclaim personal data, or don't pay the fee and lose the data indefinitely. Ransomware is able to automatically corrupt and delete files in the event that monetary compensation is not received, leaving most users with little time to resolve the problem through alternate means.

How to deal with Ransomware:

- Do not pay the ransom. It only encourages and funds these attackers. Even if the ransom is paid, there is no guarantee that you will be able to regain access to your files.
- Be sure you are backing up your data on a regular basis. If you do become a victim of a ransomware attack, you will be able to restore any impacted files from a known good backup. Restoration of your files from a backup is the fastest way to regain access to your data.
- Do not provide personal information when answering an email, unsolicited phone call, text message or instant message. Phishers will try to trick employees into installing malware, or gain intelligence for attacks by claiming to be from IT. Be sure to contact your IT department if you or your coworkers receive suspicious calls.
- Use reputable internet security software and a firewall. Maintaining a strong firewall and keeping your security software up to date are critical. It's important to use antivirus software from a reputable company because of fake software out there.
- Employ content scanning and filtering on your mail servers. Inbound e-mails should be scanned for known threats and should block any attachment types that could pose a threat.
- Make sure that all systems and software are up-to-date with relevant patches. Exploit kits hosted on compromised websites are commonly used to spread malware. Regular patching of vulnerable software is necessary to help prevent infection.
- If traveling, alert your IT department beforehand, especially if you're going to be using public wireless Internet. Make sure you use a trustworthy Virtual Private Network (VPN) when accessing public Wi-Fi like Norton WiFi Privacy.

Source: What you need to know about the Petya ransomware