RANSOMWARE FACT SHEET

It says a lot about the brashness of criminals when even law enforcement agencies become their victims. That's exactly what happened in late February when a police department in Illinois paid a $500 ransom to unlock a department computer after it was infected by ransomware.

Ransomware is a type of malware that prevents or limits users from accessing their systems. It forces its victims to pay a ransom through certain online payment methods in order to grant access to their systems, or to get their data back. No device is safe. Ransomware targets desktop computers, file servers, smartphones and laptops. Several examples of ransomware have become very well known because of their reach and cost to those infected.

CRYPTOLOCKER Renders data files unusable unless the victim pays for a key to unlock infected files. It's usually triggered when a user downloads an attachment or clicks on a link in a email disguised to look like it's coming from a friend or business partner.

CRYPTOWALL Incorporates data-theft malware, which allows the virus to steal potentially valuable data from infected systems, whether or not the victim pays the ransom.

TORRENTLOCKER First appearing in August 2014, it's made from components of CryptoLocker and CryptoWall. It's typically distributed via emails that pretend to be shipping notifications, driving or speeding violations, or other corporate/government correspondence.

CRYPTOFORTRESS Making headlines in February 2015, it looks similar to TorrentLocker. It encrypts files with a 2048-bit RSA-AES encryption routine. This type of encryption would take a standard desktop computer 6.4 quadrillion years to decrypt.

PACMAN Debuted in early 2015. It uses very convincing Dropbox links to fool victims. Its first targets were Danish chiropractors who received emails with the subject line, "Possible new patient." The email contained Dropbox links to MRI and CT scans, which launched the ransomware.

PREVENTION STARTS WITH PEOPLE

When it comes to preventing any virus, including ransomware, your first step should be to reduce the potential for human error. It helps to know what to watch out for:

- Avoid sites that offer pirated or free software, music, movies or TV shows.
- Watch out for emails claiming to be from banks or government agencies.
- Don't click on a link or attachment in an email or text message if you don't know the source.

ROLL BACK THE CLOCK ON RANSOMWARE

If your files are being held hostage, Carbonite can help. Both Carbonite Pro for workstations and Carbonite Server Backup enable you to roll back to a time before your files were infected, so you can restore an uncorrupted version of the file. The key is making sure you're backing up regularly and using Carbonite before you become a target.