# Ransomware

## The Biggest Threat to Your Data in 2016

Malware is far from a new problem but the inexorable rise of Ransomware has taken many by surprise. The Health IT industry made headlines when MedStar Health was hit and its data was breached by Ransomware. The threat of Ransomware has now become so great, that the US and Canada issued joint security alerts.

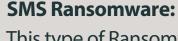




## What is Ransomware?

Ransomware is malicious software designed to block access to your computer until a sum of money is paid. Hackers can demand hundreds or thousands of dollars, just so you can retrieve your own data.

# Types of Ransomware



This type of Ransomware locks your computer and displays a ransom message with a code. To unlock your computer, you are instructed to send the code via text message to a premium-rate SMS number to receive the corresponding code to unlock it.



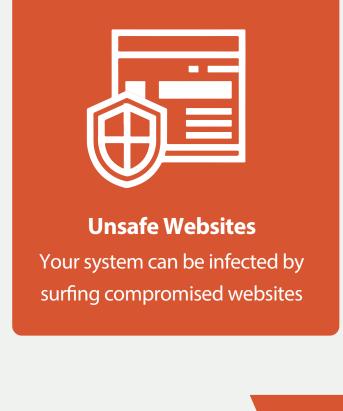
encrypt your personal files and folders using complex encryption algorithms to make your computer's data unusable. The malware author then demands that you pay for the decryption key using one of the online payment systems mentioned above.

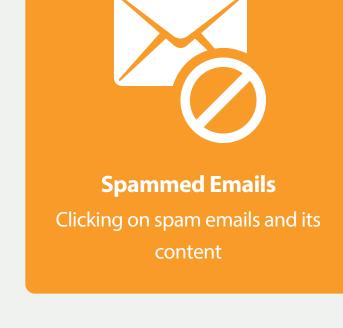


### This variant of Ransomware also

locks your computer, but it displays a more intimidating ransom message which appears to be from your local law enforcement agency. Unlike SMS Ransomware, this particular kind instructs you to pay through an online payment.

## How does the Malware Attack? You can be infected when you unknowingly download Ransomware from:







How to Avoid Infection?

### Create a backup and store it offline. Remember that Ransomware may search for documents on any connected drives or shares, so backing up to a system that is directly

Always Have a Backup

connected or uses a shared volume could result in the backed up files being encrypted as well.





#### security are functional and up-to-date in your system in order to filter out currently-known

variants of Ransomware.

**Separate System Admin Accounts** 

# network shares, USB sticks, etc.

Always use high quality anti-malware on



Consider locking down your

infection by the malware or

**Execution Restriction** 

Limit the areas in which executables

Ransomware.

computer with a security policy by

# knowing it's safe.

**System Lockdown** 

#### using the best security software to privileges, and they should use a lock down Windows to prevent separate administrator account when

performing tasks requiring their privileges. **Sandboxing** Run your e-mail client inside a

sandbox to further protect and scan

against a Ransomware infection.

System Administrators should never

give normal user accounts extended



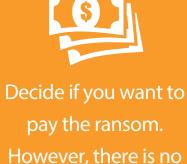
### (.exe files) are allowed to be run and limit the damage caused by malware.





disconnect it from

the network



will unlock your data

guarantee criminals



and restore your

system