Ransomware: What is it? And how it can affect your Firm?

Ransomware is a type of malware that infects a device and locks the user out of it. This prevents users from accessing any of the local files stored on the hard drive. The only way to recover these files is to pay the ransom demanded by the hackers or unencrypt the files. Law enforcement agencies suggest that you never pay money to ransomware hackers due to the fact that they may not actually follow through and decrypt the files for you.

There are three types of ransomware:

- **Screen locker ransomware** locks the user out of their physical device by taking them to a page that often claims to be part of a law enforcement agency. They require you to pay a "fine" to unlock your computer. This is the least damaging type of ransomware, as there is no actual encryption on the device.
- **Locker ransomware** encrypts the whole hard drive of the computer, which essentially locks the user out of their system. This is extremely damaging as all of the files held on the hard drive become virtually unusable.
- **Crypto ransomware** will only encrypt specific files that seem to be important. These may be word documents, PDF's and image files. This leaves the system usable, but locks the user out of all of the files.

The reason that ransomware is so dangerous is because once the files have been encrypted, decrypting them is next to impossible. No security updates or system restore will allow you to get them back.

How do you get ransomware?

There are several ways that Ransomware can infect your device. The most common method that is through opening malicious emails that contain infected attachments, such as word documents or PDF's.

In other cases, simply navigating to certain webpages can cause advertisements to trigger that redirect you to a site that can infect your computer. This happens with little to no interaction from the user, and this redirection can occur even from legitimate sites.

These sites contain exploit kits that attempt to use vulnerabilities in web browsers and other software to install.

info@i-worx.ca – 604 639 6300 – unit 201 – 1520 Barrow St - North Vancouver – V7M 1A5

www.i-worx.ca

How can you recover data that has been encrypted by ransomware?

Firstly, do not pay the cyber criminals that are holding your data hostage. They may likely take the money and leave your data encrypted, or use those funds to victimize other people.

Once the data has been encrypted, it is nearly impossible to unencrypt it without the specific key. The best way to make sure that you don't face ransomware is to have anti-virus and anti-malware software installed on your machine.

There are some decryption software's out there that can decrypt the data on your hard drive, but you need to be certain that the decryption tool matches the specific type of malware on your machine. If they are not the same, you risk encrypting your data even further.

The best way to make sure that your data is not affected is by having back up of your machine. That way, even if your data is encrypted then you can just restore from your backup, and be up and running in no time.

How do you protect yourself from Ransomware?

The best way to protect yourself from ransomware is to prevent it from happening in the first place. To do this, you should utilize an anti-virus and anti-malware software, update your computer often, and also to back up your files and data often. This includes the operating system, as well as software and web browsers; this ensures you have the best level of protection against external threats. Also having backups is integral to protect yourself should you be infected, this allows you to restore systems to before the infection, and minimize downtime.

If you are looking to have an easy and secure IT solution, then i-worx hosted desktops may be right for you.

We offer hourly backups, enterprise level security, and anti-virus and anti-malware all built into our hosted desktops. Secure yourself against the worst, and save money in the process.

info@i-worx.ca – 604 639 6300 – unit 201 – 1520 Barrow St - North Vancouver – V7M 1A5

www.i-worx.ca