Preventing Virus infections & Intrusion

Important Notice

Hackers and scammers are constantly coming up with new ways to scam your employees and company. Up until recently, such threats were directed primarily at large corporations. Recently, these attackers have concentrated on smaller and more vulnerable businesses. These attacks range from email theft and wire transfer requests, to ransom of network data from infections such as the cryptolocker virus.

the wire transfer scam that attackers have been using is discussed here - http://consumerist.com/2015/03/10/scammers-are-taking-more-money-with-fake-boss-wire-transfer-schemes/

concerning the invasive computer threat known as “CryptoLocker.” - http://www.pandasecurity.com/mediacenter/malware/cryptolocker/

CryptoLocker hijacks users’ documents and asks them to pay a ransom, usually caught by opening an email zip file attachment.

"What can you do to Protect your company and yourself from these threats"?

- Keep an eye on who is emailing you - At first glance, samsmith@computerware.com and Samsmith@computeware.com look alike (the second address is missing an “r”). Fraudsters register alternate domain names that look plausible enough, hoping to fool you into sending them large sums of money via wire transfer or information we do not share outside the company.

- Do not open any attachments or links that you are not expecting, even if the email is from someone you may know. It is not unusual for these emails to come from an acquaintance whose system is already infected – as a result, their system will send out malicious links to everyone in their address book. If you suspect that may be the case, call them and verify they intended to send you that message.

- Do not visit websites on office system that are not specifically work related – many websites may seem harmless but contain malicious code that can cause infection. This includes YouTube, twitter, Facebook, etc., if you need to connect to these sites please do it on your own phones.

The most efficient way to protect yourself and your data is to be aware, check email addresses carefully, be cautious about opening any attachments, and make sure local files are directed to your server for backup.

If you become infected, immediately disconnect from the network or turn off the machine and call Andrew Jerez. at extension 143. If you are not certain if an attachment or email is safe, call Andrew Jerez, and he will test it for you.

Keep your computer and email passwords in a secure place, do not put on sticky note attached to your monitor. Never send anybody your passwords on an email. Don’t share your password with anybody, if you suspect somebody may have it immediately have Andrew Jerez change it for you.

Below is a list of the DOs and DON’Ts of safe computing:

DON'T open attachments you weren't expecting.

DON'T click on links you are uncertain about.

DON'T reply to junk email, even if trying to unsubscribe, that email from a relative in a foreign country trying to send you 10 million dollars does not exist.

DON'T visit non-work related websites.

DON'T connect to unsecured Wi-Fi hotspots, if we give you access to our wireless please follow all these don’ts.

DON'T download questionable files.

DO check the email address of people sending you email.

DO call the sender by phone if you received a questionable email from them.

DO shut down your computer nightly.

DO use complex passwords on all accounts.

DO contact your IT or computer specilist if you have any questions.