ITS INFORMATION TECHNOLOGY SOLUTIONS
An 'Aumakua Hawai'i Company

Dear Valued ITS Clients,

A massive ransomware attack named WannaCry has reached around the world causing significant alarm. The attacks have caused major disruption to hospitals, telecom companies or gas and utilities plants. Among the organizations that took the worst hits is the National Health Service (NHS) in the UK.

WannaCry is a new ransomware variant that takes advantage of a vulnerability in the Windows operating system to encrypt the infected computer's data and hold it hostage until a ransom is paid. In addition, the vulnerability enables WannaCry to quickly spread to other machines in the same environment - all without any human intervention. Microsoft issued a patched to the vulnerability in March 2017, and we have and will continue to verify that systems are up to date with security patches.

The attack is particularly dangerous for businesses because it takes just one employee to become infected for the attack to spread in the entire network, and sometimes even across countries to other subsidiaries, without any user interaction. This happens because the ransomware has a worm component that leverages a recently discovered vulnerability, affecting a wide range of Windows operating systems

WannaCry is spread by a system becoming infected typically through an email **Phishing Scam** trying to trick you into opening an infected attachment, bad link, or any other means of an illegitimate e-mail.

When trying to determine if email is authentic or not, remember one very important detail: *no legitimate company will ever send you email requesting your username, password, or any other personally identifying information.* Also don't open ZIP or attached files that you are not expecting. Call the sender and verify that they sent the attachment prior to opening.

Things to look for to verify if the email is a phishing email:

- Spelling errors and bad grammar
- Odd formatting (e.g., incorrect use of capital letters or punctuation)
- No real person's name included either in the greeting or the signature
- A return or reply-to email address that is spoofed.
- If a password is being requested, you know the email is not legitimate. No legitimate business will ever request your password. Look at what else is being requested as well (e.g., requesting your country or territory is not a legitimate customer service request)
- No mention of a phone number to call or person to contact
- Deleting an account due to lack of response: a legitimate business doesn't follow that kind of practice
- Includes a hyperlink that has an odd looking URL (for instance with a foreign country as the domain, or trying to match a legitimate web address but spelled differently)

Next Steps:

- Avoid opening or clicking on hyperlinks in suspicious emails.
- Call us immediately with any email or system scares that you feel is related to any form of ransomware.
- ITS will continue to monitor and push known Windows Updates to keep you as safe as possible.