London

27 July 2020

Ransomware Warning

Some of you may have read reports that there has been a new round of ransomware doing the rounds at present, with some very high profile companies such as Garmin being hit and taking their systems down for an undisclosed period of time.

For those of you that are unfamiliar with what ransomware is, after gaining access to a computer system through a vulnerability or social engineering, the attacker uses ransomware to encrypt important files. Then, they demand payment (usually in Bitcoin) to provide the decryption key. Some ransomware campaigns do actually live up to their end of the bargain if paid, but others are just a scam to milk victims for as much money as possible. While individuals are sometimes hit for a “small” amount of money in ransom, businesses can be asked to pay much larger sums to regain access to their data.

Whist we do everything we can do to ensure security within our systems at Colart (such as Multi Factor Authentication and Intrusion Prevention Systems) occasionally things will slip through the net. As such we all need to be on our guard and take every precaution as to not compromise personnel and company data.

There are a few tips to ensure that we remain vigilant and on our guard against these types of attacks as below:

- Ensure both Colart and personnel accounts use MFA (multi factor authentication).
- Do not open an email or a link/attachment from an unknown sender (or a colleague) if it does not look legit (this goes for both business and personal email).
- If it looks like you have been compromised, remove the battery/power from your device and contact Tech Support immediately.
- To ensure that no loss of data occurs, ensure you save your files to OneDrive or other network and cloud storage where possible.

If you think you have been compromised or have any questions regarding any of the above then feel free to get in touch with members of the Tech Team.

Stuart Cooney – Head of Global Infrastructure