Jersey Financial Services Commission

Press Statement **15 May 2017**

JFSC issues guidance on WannaCry cyber attack

The Jersey Financial Services Commission (JFSC) is aware of the recent ransomware campaign relating to version 2 of the "WannaCry" malware which experts are describing as "the biggest ransomware outbreak in history", affecting more than 200,000 victims in over 150 different countries.

The JFSC has been working over the weekend to assess the threat, further reviewing its own systems' security measures, while liaising with partner organisations and using intelligence to constantly assess the risk posed.

The JFSC has been informed of further variants of the malware entering circulation, distributed by phishing emails. Companies can undertake the following simple steps to help protect their organisation:

- Keep your organisation's **security software patches** up-to-date
- Use **proper antivirus software** services
- Most importantly for ransomware, **back up the data** that matters to you and test the backups. You should then be able to recover your data without paying a ransom
- **Do not download files or programs** from unknown websites or sources. Even if you know the source, get authorisation from your IT department before downloading software to the company network
- **Think before you click – exert extreme caution** regarding emails, links or untrustworthy websites that may allow dangerous viruses or malware onto the network
- **Given the nature of ransomware, we suggest that you report but do not forward any suspicious emails**
- **Avoid attachments**, as viruses can be embedded in files. Take extra care when opening these files and only open them if you know they are genuine
- **Report anything suspicious** whether it is an email, link or website
- Phishing emails are designed to look like authentic messages to lure you into clicking them. Trust your instincts. If an email seems suspicious or isn't quite right, even if it's from someone you know, do not open it and report it
- Accidents happen - if you do open an email or click a link you think is suspicious, inform your security team or IT immediately
- **Be alert. Think before you click.**

Emma Martin
Head of Communications
T + 44(0)1534 822166
E e.martin@jerseyfsc.org

For further guidance and the most up-to-date advice on how to protect your business against ransomware and other cyber threats, please visit the National Cyber Security Centre (NCSC) website as follows:

Ransomware: latest NCSC Guidance

https://www.ncsc.gov.uk/guidance/ransomware-latest-ncsc-guidance

NCSC, latest statement on international ransomware cyber attack
https://www.ncsc.gov.uk/news/latest-statement-international-ransomware-cyber-attack-0

Ends.