HM Government of Gibraltar

JOINT PRESS RELEASE

No: 301/2017

Date: 15th May 2017

Statement on Wannacry Ransomware attack

Authorities in Gibraltar continue to closely monitor events surrounding Friday's global ransomware cyber attack that targeted organisations and individuals in various countries, in particular, those targeting various sectors across the United Kingdom, where agencies continue to work and cooperate closely to investigate the attacks and restore services to those affected areas.

All Government IT Systems have been unaffected by Friday's attack, and there have as yet been no reports of any Gibraltar-based systems having been affected by this latest attack, which is said to have exploited a vulnerability in Windows operating systems. Although a patch for this vulnerability is said to have been released by Microsoft in March of this year, many systems may not have had this update installed.

The Royal Gibraltar Police and HMGoG's Information, Technology & Logistics Department (ITLD) continue to communicate with each other regularly, and have already reached out to local industry partners through the issuing of preventative advice.

Attacks of this nature, particularly on critical services, can have a significant impact on individuals, therefore it is important for organisations and individuals alike to ensure that they:

1) Do not click on links or open any attachments received in unsolicited emails or SMS messages.
(Remember that fraudsters can 'spoof' an email address to make it appear like one used by someone you trust. If in doubt, always check the email header (or contact the person separately).

2) Always install software updates as soon as they become available, no matter how inconvenient this might sometimes seem.
Whether an update is for the operating system (ie Windows) or an application, an update can contain fixes for critical security vulnerabilities.

3) Create regular backups of your important files to an external hard drive, memory stick or online storage provider. Note that it is important that the device you backup to is not left in an insecure location, or linked to the same network your main machines are connected to.

There are various online resources that provide useful advice on how to protect your data, devices, what to do if/when infected with ransomware and access to unlocking tools.

Once such resource is the “No More Ransomware” project, a free online resource developed by the European Cybercrime Centre and industry partners, and which can be found at: https://www.nomoreransom.org/

Further updates and advice on these attacks may also be issued from time to time in the form of press notices or via social media channels:

HM Government of Gibraltar:
Twitter @GibraltarGov Facebook: www.facebook.com/gibraltargovernment

Royal Gibraltar Police:
Twitter @rgpolice Facebook: www.facebook.com/royalgibpolice