National Fraud Intelligence Bureau

CITY OF LONDON POLICE
National Policing Lead For Fraud

Ransomware Incident
Protect Messaging

14/05/2017

ALERT

Following the ransomware cyber attack on Friday 12 May which affected the NHS and is believed to have affected other organisations globally, the City of London Police's National Fraud Intelligence Bureau has issued an alert urging both individuals and businesses to follow protection advice immediately and in the coming days.

PROTECTION / PREVENTION ADVICE

Key Protect messages for **businesses** to protect themselves from ransomware:

- Install system and application updates on all devices as soon as they become available.
- Install anti-virus software on all devices and keep it updated.
- Create regular backups of your important files to a device that isn't left connected to your network as any malware infection could spread to that too.

The National Cyber Security Centre's technical guidance includes specific software patches to use that will prevent uninfected computers on your network from becoming infected with the "WannaCry" Ransomware:
https://www.ncsc.gov.uk/guidance/ransomware-latest-ncsc-guidance

For additional in-depth technical guidance on how to protect your organisation from ransomware, details can be found here: https://www.ncsc.gov.uk/guidance/protecting-your-organisation-ransomware

Key Protect advice for **individuals** is essentially the same, with one additional point:

- Install system and application updates on all devices as soon as they become available.
- Install anti-virus software on all devices and keep it updated.
- Create regular backups of your important files to a device (such as an external hard drive or memory stick) that isn't left connected to your computer as any malware infection could spread to that too.
- Only install apps from official app stores, such as Google's Play Store, or Apple's App Store as they offer better levels of protection than some 3rd party stores. Jailbreaking, rooting, or disabling any of the default security features of your device will make it more susceptible to malware infections.

Phishing/smishing

Fraudsters may exploit this high profile incident and use it as part of phishing/smishing campaigns. We urge people to be cautious if they receive any unsolicited communications from the NHS. The protect advice for that is the following:

- An email address can be spoofed. Don't open attachments or click on the links within any unsolicited emails you receive, and never respond to emails that ask for your personal or financial details.
- The sender's name and number in a text message can be spoofed, so even if the message appears to be from an organisation you know of, you should still exercise caution, particularly if the texts are asking you to click on a link or call a number.

Don't disclose your personal or financial details during a cold call, and remember that the police and banks will never ring you and ask you to verify your PIN, withdraw your cash, or transfer your money to another "safe" account.

If you have been a victim of fraud or cyber crime, please report it to Action Fraud at http://www.actionfraud.police.uk/

FEEDBACK

The NFIB needs feedback from our readers to evaluate the quality of our products and to inform our priorities. Please would you complete the following NFIB feedback survey through: https://www.surveymonkey.com/r/FeedbackSDU.