Dos and don'ts

Best practices for protecting against ransomware

- Keep security software up to date.
- Keep operating system and other software updated as updates include patches for newly discovered security vulnerabilities.
- E-mail is one of the main infection gateways.
- Be wary of unexpected e-mails especially if they contain links and/or attachments.
- Be extremely wary of any Microsoft Office e-mail attachment that advises you to enable macros to view its content.
- Organisations that have been breached should immediately isolate infected computers to stop the spread of the virus. Patch systems using the Microsoft security update or do virtual patching.
- Organisations not attacked should also immediately patch their systems and update security software.
- Backing up important data is the single most effective way of combating ransomware infection.
- Organisations should ensure that back-ups are protected or stored off-line so that attackers can't delete them.
- Using cloud services could help mitigate ransomware infection as many services retain previous versions of files, allowing you to "roll back" to the unencrypted form.

Source: Symantec, Trend Micro

Businesses can refer to SingCert's advisory on WannaCry at www.csa.gov.sg/singcert; or seek help from SingCERT through singcert@csa.gov.sg or call 6323 5052.