PRESIDENT'S OFFICE
REGIONAL ADMINISTRATION AND LOCAL GOVERNMENT

RANSOMWARE ALERT

Ransomware is a type of malicious software (malware) that gets secretly on your computer or your computer systems. It locks files, usually by encrypting them. They come via emails, remote desktop, accessed over public network or by infected websites that are well crafted to make a person believe the mail, link or attached file is from a trusted source. Clicking on the link causes the malicious software to load on your system and starts encrypting files like Databases, Word, Excel, JPEG, PDF files, etc.

The only way to unlock the files is to pay the criminal sender a ransom (money). They contact you to extort money to "unlock" your company's systems/data. In some cases, after you pay the ransom they don't unlock the files. The encryption cannot be by-passed. It is NOT recommended that a ransom be paid. Once paid you become an ongoing target of these criminals. Proper precautions will reduce risk and allow business to recover from an attack. This issue is both a social engineering attack and a technical attack.

Best Practices to Keep from Getting Infected in the First Place

There are some tips on how to keep your computer from getting infected with ransomware. You don't have to do all of these, but the more you do, the better off you are. The tips are hereunder mentioned:-

i. Keep your operating system up to date.

ii. Know how your applications are updated. Some applications will pop up notifications on your screen, others will notify you via email and still others will only tell you about updates when you use them.

iii. Keep your applications up to date. When new updates come out, especially security updates, apply them. But first, make sure you know the source and how the application is updated – *see item 2.*

iv. If you receive a suspicious email (phishing?), don't click on any links or use the phone numbers in the email.

v. Use anti-virus and anti-malware software and keep it up to date. This should include a good adware filter and a pop-up blocker.

vi. Try not to click on ads for products or companies you don't know. Even better, if you see an appealing ad, go directly to the company's website and see if the offer is there.

vii. Only download and install browser add-ons, plugins, and extensions that come from known, reputable sources.

viii. Take a snapshot of your entire system from time to time, perhaps once a month. This will include data and applications. Store these snapshots on an external drive that is only connected to your computer to do the backup and then is disconnected.

ix. Have a backup of all the files on your computer to a server that is NOT on your network.

If you suspect any virus, please disconnect infected device from the network. This could help minimize the loss of information. Incase you face any problem, please do not hesitate to contact e-Government Security Team (**gicts@ega.go.tz**) or PO-RALG team (dict.staff@tamisemi.go.tz).

Issued By: Directorate of ICT – PO-RALG

21st May, 2018