



# Ministry of Technology, Communication and Innovation

## IT Security Unit

### IT Security Awareness

## Rogueware

*"Know how to recognize it"*

August 2015

Issue 02

### What is Rogueware ?

Rogueware, also known as fake security software or scareware, is a form of software that **scares** a user into thinking that his computer has been infected when in reality his computer is in good working condition. It aims at causing shock, anxiety or at frightening unsuspecting computer users by making them believe that their computers are under attack.

It is designed to **trick** victims into purchasing and downloading useless and potentially dangerous software.

### Why is Rogueware created ?

- ▶ To **install malware** on your computer
- ▶ To **scare** you into paying for more fake products
- ▶ To **slow** your computer and **corrupt** your files
- ▶ To **raid** your bank account
- ▶ To **disable** windows updates
- ▶ To **steal** your identity

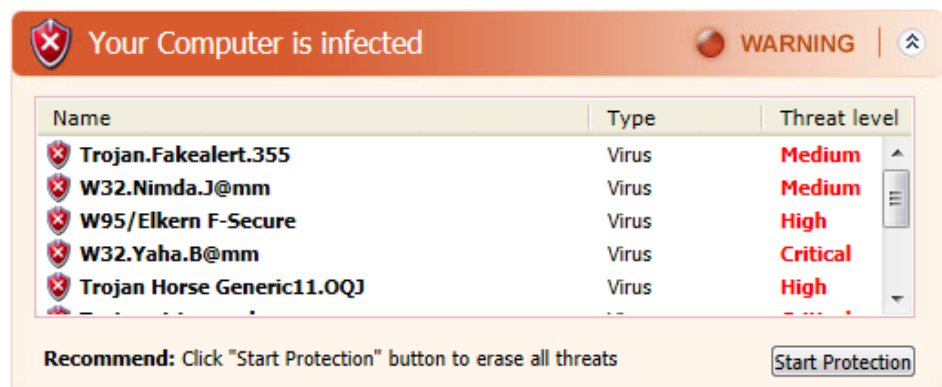


**If you suspect your computer has been infected by Rogueware, contact your IT technical team.**

<http://mtci.govmu.org>

### How does Rogueware operate?

As illustrated below, Rogueware is a malicious software (malware) that pretends to be a well-known, commonly used program, (for example, an antivirus):



This means that the software appears to be beneficial from a security perspective but when installed may:

- provide limited or no security
- bombard the user with alarming warnings or threatening messages
- attempt to lure users into participating in fraudulent transactions
- display unwanted advertisements on the user's screen
- generate erroneous or misleading alerts
- cause the computer to run slower than usual
- show constant pop-ups with the browser redirecting to non-desirable websites




### Protect yourself from Rogueware

- ✓ Avoid clicking on pop-up messages prompting you to immediately download an antivirus software
- ✓ Use up to date and reliable antivirus software from trusted companies to protect your computer against infection
- ✓ Ensure that pop-up blocker is configured in order to prevent 'pop-ups' from sites you do not wish to access
- ✓ Exercise caution when you click links in email and surf on the internet
- ✓ Refrain from disclosing any personal information when prompted to do so
- ✓ Use a standard user account instead of an administrator account
- ✓ Be mindful of emotionally charged alerts and warnings

# Rogueware: Preying on people's fear




Rogueware **operates** by displaying popup messages indicating that your computer is infected and pretends to be a well-known software



To **protect** yourself from rogueware, use an updated and reliable antivirus software and do not click on suspicious links

Rogueware is **created** to install malware on your computer and to scare you into paying for false security check



A relatively large number of computers in the world are infected by rogueware.

