St George's, University of London
Anti-Malware Policy

1. Introduction

1.1 The University is obliged to make sure its IT systems and other facilities are secure and not subject to improper use. This Policy sets out the responsibilities of all users, including users of privately-owned devices that connect to the University IT facilities, in relation to malicious software. These measures do not guarantee security, but they will help to significantly reduce the risk of widespread virus infection at the University.

1.2 The word 'malware' is used collectively to denote many types of malicious software, including viruses, ransomware, worms, trojans, macros, mail bombs and rootkits. A virus is a piece of self-replicating computer program code that is designed to destroy or damage digital information, or to steal user or business data.

1.3 There are many potential sources of malicious software, including websites, social media, USB memory sticks, unsolicited CDs, electronic mail, and software or documents copied over networks such as the campus network or the internet.

1.4 A malware infection is costly to the University and often time-consuming for individuals. This may be through the loss of data or access to IT systems, staff time to recover a system, or the delay or loss of important work. Additionally, malicious software can spread from an infected system and can lead to severe disruption to IT services and possible reputational damage or even fines. Malicious software is a constantly evolving threat and the University therefore applies controls to protect our systems and information from all forms of malware.

2. Scams and Hoaxes

2.1 There are many types of scams or hoaxes; many perform what is known as "social engineering" via to frighten the recipient into a reactive action without thinking of the consequences. It is important to remember, that e-mail is NOT an urgent medium and has no guaranteed delivery. If an email threatens repercussions if an instant response isn't forthcoming it should be considered a scam.

2.2 Many spam emails are sent with dire warnings about messages with topical subjects or attachments. The receiver is often asked to forward the email to all colleagues and friends around the globe. If you are unsure whether an email you receive is a hoax or scam, you can check it at www.snopes.com. Do not forward these messages on. If you receive such a message, just delete it.

2.3 Some websites you visit will suggest your PC or tablet is infected with a new virus and hence you need to run / install / purchase their anti-virus software. Do not click this message. Instead, check that you have the latest signatures and updates in your existing anti-virus software and then run a manual scan.

2.4 If you download a fake anti-virus application, or think that your device has a virus, please report this to the helpdesk or to local IT staff as soon as possible, because it will be much easier to remove if reported promptly.

3. Scope

3.1 This Policy applies to all users, including Halls of Residence users, guests and other users of privately-owned devices that connect to the University IT facilities. By following this Policy, users will help to protect themselves and other University users against malicious software. The University IT Regulations, on which this Policy expands, require everyone to take the practical steps needed to keep this protection active and up to date. If in doubt, contact itav@sgul.ac.uk

4. Purpose

4.1 The objectives of this document are:

- To set out user responsibilities about malicious software prevention
- To set out the rules governing the application and use of malicious software prevention systems at the University

5. Policy

General

- All personal computers, devices and servers connected to the University network must run a supported version of the Operating System and installed applications with the latest available patches applied.
- All personal computers and servers that are connected to the University network or otherwise using the IT facilities must run up-to-date anti-malware product that continually monitors for malicious software (viruses, worms, etc.).
- Anti-malware must be configured for on-access scanning, including the downloading or opening of files, folders on removable or remote storage, and web page scanning.
- Anti-malware protection software must be configured to run regular (at least daily) scans.
- The University's IT Regulations prohibit any activity intended to create and / or distribute malicious code (viruses, worms, etc) on the University network or IT facilities. However, when requested to do so by IT staff in order to aid investigations, users may send suspected malware using a method that does not allow the malware to propagate / spread.
- The University reserves the right to disconnect any device from the network if an infection is found or suspected. The device will be disconnected until the infection is removed and suitable preventative tools have been installed on the device.
- If you suspect that a device is infected with a virus, report the incident to the helpdesk and / or to local IT staff as soon as possible.

In addition to the above, specifics for SGUL Managed devices

- SGUL IT managed desktops will have ESET Endpoint Security for Windows, deployed part of the imaging process.
- SGUL IT managed servers will have ESET File Server Security deployed.
- Deployment, Updates and Policies for the ESET product are centrally manged via the ESET Protect Management portal.

- The Endpoint security software will be configured to prevent users from accessing known malicious web sites
- The Endpoint security software will be configured to perform HIPS and IPS checks
- Users will be unable to uninstall or disable anti-virus software.
- If users experience difficulties with a recommended anti-virus product, requests for technical support may be made via itav@sgul.ac.uk

Email:

- SGUL's anti-virus and spam gateway product will scan emails for malicious attachments and quarantine if found to be suspicious.
- SGUL's anti-virus and spam gateway product will scan emails for malicious attachments and silently delete if known to be fraudulent or dangerous.
- Email attachments will be scanned on access by the Endpoint security application.
- SGUL's anti-virus and spam gateway product will scan emails for malicious URL's and phishing and quarantine if found to be suspicious.
- SGUL's anti-virus and spam gateway product will scan emails for malicious URL's and phishing attempts and silently delete if known to be fraudulent or dangerous