OFFICE OF
INFORMATION TECHNOLOGY
STEVENSON UNIVERSITY

Stevenson University Information Security Incident Response Playbook: User Reports Desktop/Laptop Malware

Last Updated: January 10, 2025

OFFICE OF INFORMATION TECHNOLOGY
STEVENSON UNIVERSITY

Information Security Incident Response Playbook:

User Reports Desktop/Laptop Malware

1. Purpose: This playbook describes the steps that should be taken if anyone reports a possible malware issue on a computer to the Office of Information Technology, including a helpdesk ticket, phone call or in person.
2. Procedure
    a. Initial triage questions and actions:
        i. Is the computer currently running?
        ii. What network is the computer connected to?
            1. If desktop that only has Ethernet wired connection – have user disconnect.
            2. If using WiFi connection
                a. See if user can identify the network (Stevenson, SUConnect, Admin, etc.)
                b. Try to have user disable WiFi
        iii. What windows, pop-ups or messages can be seen?
            1. Get as many details as possible.
            2. If user has mobile device, have them take a picture of the screen.
        iv. Are there any other unusual behaviors on the computer?
            1. Files not accessible or filenames being changed/encrypted
            2. Mouse or keyboard not working
            3. Sounds
        v. What was the user doing on the computer **immediately prior to the detection?**
            1. Using email (ask if they recall any subject lines, recipients, name of attachments)
            2. Browsing websites (ask if they recall what sites)
            3. Opening files from a server (what was the name of the server or drive letter)
            4. Installing a browser extension or toolbar:
                a. What browser are they using (Chrome, Edge, Safari, Firefox, etc)?
        vi. What was the name or type of extension or toolbar?
        vii. Did the user take any actions **after** the detection?
            1. Entering information to any box/window such as username and password, cell number, etc.
            2. Restarting the computer.
            3. Going to any other websites to search for information about the behavior.
            4. Attempting to install any software, such as a virus cleaner.
    b. Open or update helpdesk ticket.
        i. Make sure Request Type is “Virus/Spyware Infection”
        ii. Include all information gathered during triage.
        iii. Add any additional technical information easily available including:
            1. Name of computer
            2. Location, especially for laptop
            3. Mobile number for user
    c. Conduct initial response activities.
        i. Run malware scanner
            1. Forticlient EMS
            2. MalwareBytes
            3. CCleaner
            4. Microsoft Defender (M365\Intune)
        ii. Contact Chief Information officer for further steps