First Response: Checklist

This document is for the user or owner of a UW computer which has been involved in a cyber incident (for example, a malware infection or unauthorized third-party access).

For more detail and explanations, see the First Response Guide.

As you work through the following steps, **record your observations and actions, and what time they occurred.**

1. **Disconnect the device from the network if it is not a critical service.**
    - If it has a wired internet connection, unplug the network cable.
    - For wireless devices, turn off the wireless adaptor if that's possible, or disconnect from the wireless network.

2. **Preserve state. If at all possible, don't touch anything else.**
    - It's important to not do anything that would make it difficult to determine who did what.
    - Don't log off or power down the device.
    - Don't use the computer; use a different computer until you hear from us.
    - Don't log into a compromised device for any reason.
    - Don't do your own forensics.

3. **Preserve evidence.**
    - If you have logs in a central location, save them immediately.
    - Do not log into a compromised device to retrieve logs.

- **Contact the Office of the CISO and your IT support staff by telephone.**
    - If you get voicemail, leave a detailed message and then email ciso@uw.edu to let us know.
    - If applicable, please write down everything you observed and what you did and make a note of what time you did it. Answer the following questions, if possible.
        - How did you discover the problem and when?
        - What programs were open?
        - What were you doing immediately before the incident?
        - Were there any recent changes in hardware, software, or work habits (such as working remotely), or peripheral devices added?
        - Did you notice anything else that may be important or unusual?
    - The forensics team will need as much information as possible to understand who did what and when. If changes or actions are unavoidable, it's critical for us to know when they occurred.
        - Did you fail over a server?
        - Did you reset a password or disable an account?
        - Did you power off or log into or out of a computer?
        - What time did any of those actions occur? What time were logs saved, and from where?

The Office of the CISO wishes to do everything possible to avoid interrupting your workflow while preserving the evidence needed to protect UW data. If your department has IT support, we will be working with them to guide their response, but the information provided here may help to provide context for what we may be asking.