This checklist is intended for University-owned desktops or laptops compromised by malware. If a server is compromised or this is a different type of incident (e.g., stolen computer), contact security@oit.umass.edu. If your department’s computers are maintained by IT LAN Support, complete these items in collaboration with your LAN Support contact.

For assistance with any of the items below, email security@oit.umass.edu.

☐ Keep detailed notes
You may have to provide details about the incident, including how you responded, to other staff, management, University Legal Counsel, or Internal Audit.

☐ Minimize system changes
Changes can destroy valuable data related to the incident. Do not power off, run anti-virus software, or attempt to back up data.

☐ Gather volatile information while the system is running (optional)
Document any open network connections, running processes, logged-in users, and connected drives. Capture an image of the computer’s memory.

☐ Shut the system down & preserve hard drive data
Make sure the system is shut down before completing the next steps.
Option 1: Get a forensically-sound copy of the hard drive
Keep this information until the incident is resolved. Preserve an MD5 hash of the original drive(s) and image(s).
Option 2: Connect the hard drive to a write blocker
Write blockers enable you to acquire information from a drive without damaging its contents.

☐ Run Identity Finder & a malware detection scan
With the write blocker in place or after you saved a forensically-sound copy of the affected drives:
• Run Identity Finder to identify and locate sensitive data.
• Complete a malware/virus detection scan using your preferred anti-virus/anti-malware application.
• Gather any other information relevant to this incident.

☐ Provide IT with a status report
Contact IT if Identity Finder finds any personally identifiable information, IT first contacted you about this incident, or you cannot rule out the presence of sensitive data. Email security@oit.umass.edu the following:
• Incident history
  (date, time, symptoms, first response)
• Identity Finder & malware scan results
• Host name
• IP Address
• MAC Address
• Building & room number
• Your email & campus telephone number

If the device contains personally identifiable information, IT will need the hard drive(s) (or the forensically-sound copies) for in-depth analysis. Note: If the malware scan results may be useful to other campus IT Administrators, please forward OIT this information.