The WSU Knowledge Base Wiki

More information about phishing can be found on the WSU Knowledge Base Wiki:

http://learn.winona.edu
http://learn.winona.edu/Phishing

About the WSU Knowledge Base Wiki

You should be able to find answers to most of your WSU campus technology questions on the WSU Knowledge Base Wiki.

Search our growing collection of helpful articles about campus technology. Can't find what you need? Email us at dlc@winona.edu and we will add it. We welcome student, faculty and staff contributions to this site.

How do I protect myself?

- NEVER share your password with spouse, kids or co-workers
- Do Not reuse passwords
- Forward SPAM or phishing schemes to Abuse@winona.edu
- NEVER log onto your computer for someone else to use
- Keep your computer and devices up to date with current operating systems.
- Scan external devices with antivirus software before you transfer files

Contact Us

Technical Support Center
Somsen Hall 207
AskTech@winona.edu
507.457.5240

Malware

Quarantined?

Infected with Malware?
My laptop has been quarantined

If your laptop has been quarantined or riddled with popups we will need to clean out the laptop as soon as possible. We may have your laptop up to 48 hours depending on the severity of the infection.

Why is my laptop quarantined?

Information Technology Services is given the responsibility and authority to quarantine users and computers in the event of an account or computer compromise from MnSCU board policy 5.22-23 and subsequent standards and guidelines.

ITS Staff may quarantine or de-activate a user’s account, computer, or other devices if there is reasonable evidence of:

- University data exposure
- A compromised account
- Malware being detected on a device connected to the university network
- Malware actively attempting to attach itself to a device connected to the university network
- Any user or computer being used to compromise the integrity of other users or resources
- Common scenarios include but are not limited to:
  - Users responding to phishing schemes
  - Unpatched or virus infected computers
  - Large downloads impacting bandwidth availability
  - Internal hacking attempts

How did my laptop become infected with malware?

We cannot tell you exactly how your laptop became infected but the list below is likely.

- Phishing Links - you may have clicked on a malicious link in your e-mail or emailed your password.
- Phishing Picture - you clicked on a malicious or linked picture in your e-mail
- Downloading of games to your laptop
- Downloading FREE software
- Drive-by infection - installs software without your knowledge
  - Drive-by infections are typically carried out by exploiting browser vulnerabilities or security settings on your computer.
- Infected USB memory stick or other external device
  - Malicious programs or malware may be installed on the memory stick and re-download themselves to your computer.
- Peer to Peer sharing of videos, software, etc.
- Ignoring software updates

How long will it take to clean up my laptop?

The process may take up to 48 hours and in some extreme cases longer.

- If the laptop has been quarantined it will be a minimum of 24 hours to run all the utilities necessary to clean it out.
- One other option is just to have it re-imaged. This will erase the entire hard drive. The process will take about 40 minutes and your laptop will be restored to defaults.

NOTE: This option will erase all data, settings and applications. Restoring data requires a full scan and lots of time.

What about my data and files?

Students, faculty and staff are responsible for their own personal files and data. If you have a virus or malware it may not be possible to recover your data.

It is important that you backup your computer on a regular basis as tech support will not back up or assist in backing up of your data due to a virus or quarantined laptop. Backing up infected files will reintroduce problems to a clean machine.