Computing Virus and Malware Landing Page

Overview

Just like you, your computers can get sick when they catch viruses and malware that are designed to harm and/or steal your information. They can even use your compromised computer as a foothold to attack others. Your best defense is to be aware of the risks and install protective software, such as Sophos anti-virus and CrowdStrike Falcon endpoint protection, threat intelligence, and services focused on preventing damage from targeted attacks.

- How can I reduce the risk of malware infecting my computer?
- How can I find out about the latest virus threats at MIT?
- For more information on how to classify and secure your data, see Information Protection @ MIT.

How to

Set up Sophos Anti-virus Protection

- Obtain Sophos
- Sophos Links

Set up Crowdstrike

- Obtain Crowdstrike Falcon
- CrowdStrike Falcon - Installation Instructions

Tell if your Computer has a Virus/Malware

- Does my computer have malware on it?

Recover from a Virus/Malware

- How do I remove malware and recover from a system compromise?
- I received a UDP reflection attack notice
Email Risks and Responses

Identify Risky Emails

- What is a phishing email?
- What is CryptoLocker Ransomware?
- What is a Nigerian 419 scam?

Phishing

- Examples of phishing emails that appear to come from MIT
- Is there a list of phishing reply email addresses?
- Reporting Phishing Email

SPAM

- IS&T's SPAM Filtering Service
- Can something be done to stop the spammers?
- How do spammers get my email address?
- I'm getting spam from MIT. Now what?

Misc

- How to verify if an email originated from someone at MIT
- Email address forged by spammers or virus

FAQ's

- Virus Protection at MIT - Virus Protection Tips
- Can I run two virus protection software applications on my machine? Won't this be safer?

Have Questions or Still Need Help?

- Contact the IS&T Service Desk