MICHIGAN STATE
UNIVERSITY

Keep it Safe

Stop Assuming. Start Securing.

Protect your information
and the information of others.
computing.msu.edu/secureIT

Mitigating risk and protecting information a

**Protect yourself and the information you have beer
by following the safe computing practices outlined**

computing.msu.ed

Protect Yourself

Safeguard Passwords
When it comes to passwords, you can never be too protective. Be sure to guard passwords as you do money, use different passwords for different accounts, change passwords often, don't share passwords, and use strong passwords. Methods for creating strong passwords are listed at computing.msu.edu/securelT.

Protect Personal Information
Personal information should never be shared nor sent through e-mail, especially:

- Social Security numbers
- Passwords
- Credit card numbers
- Bank account numbers
- Driver's license numbers
- Names, addresses, phone numbers in conjunction with other personal data
- Health and financial information
- Student educational records

Criminals use personal information to facilitate identity theft.

Remember:
Encrypt private data sent across networks or stored on a laptop or desktop machine. It is best to store private data on a secure server, not personal computers or portable storage devices. Visit computing.msu.edu/securelT for information about encrypting data.

Allow access to sensitive data on a "need to know" basis only. When leaving your computer, even for a moment, lock it. Ensure that your screen saver is set to require a password before the desktop can be reactivated.

When sensitive data is no longer needed, get rid of it. Shred papers with sensitive data and sanitize hard drives when disposing or transferring computers.

Educate yourself about the most common tactics used to get personal information, like phishing.

ssets is everyone's responsibility.

n entrusted with
here.

u/secureIT

Protect Your Computer

Always Use Anti-virus and Anti-spyware Software

Anti-virus software protects your system from viruses, worms, and other malicious software.

Schedule software to check for updated virus information on a daily basis, and run periodic virus scans on your system.

Spyware is malicious software that spies on you as you use your computer. It then transmits that information to a third party. Spyware can capture your keystrokes as you enter your user names, passwords, and credit card numbers.

Failure to use anti-spyware *and* anti-virus applications can lead to repeated infections which could precipitate poor computer performance, identity theft, and costly repairs.

Turn on a Personal Firewall

A personal firewall provides an essential layer of protection to your computer. Firewalls come in two forms: hardware and software. A hardware firewall is a separate physical device that blocks unwanted traffic before it reaches your computer. Software firewalls are particularly beneficial for laptops since they are installed on the computer, protecting it when used at different locations, like coffee shops and other public areas.

Apply Software Updates

Operating systems and most software applications frequently release updates to download and install. It is important to install these updates as soon as they become available. They often includes patches to security holes which may make your system vulnerable to viruses or other exploits.

Terms to Know

- ✓ **Phishing**: an attempt to criminally and fraudulently acquire sensitive information, such as account information, passwords, and credit card details, by masquerading as a trustworthy entity in an electronic communication.

- ✓ **Malware**: software designed to infiltrate or damage a computer system without the owner's informed consent. Malware includes computer viruses, worms, trojan horses, most rootkits, spyware, dishonest adware, and other malicious and unwanted software.
  Types of malware include:
  Virus: a computer program that can copy itself and infect a computer without permission or knowledge of the user.
  Spyware: computer software installed surreptitiously on a personal computer to intercept or take partial control over the computer. Spyware can collect personal information, Internet surfing habit, sites visited, and can change computer settings, resulting in slow connection speeds and loss of programs or Internet access.
  Keylogging: one of the most dangerous forms of spyware, keylogging programs capture keystrokes, mouse clicks, files opened and closed, sites visited, and more as a person uses their computer.

- ✓ **Spam**: Electronic junk mail or junk news group postings.

- ✓ **Identity Theft**: a crime where a criminal assumes someone else's identity in order to profit by fraudulent means.

MICHIGAN STATE UNIVERSITY

SECURE IT

computing.msu.edu/secureIT
ATS Help Desk (517) 432-6200