How can I protect myself from malware (viruses, adware, etc)?
Your computer must have protective software. PCs (Windows) use Microsoft Defender, a built-in virus and threat protection system. More information is at https://www.microsoft.com/en-us/windows/comprehensive-security. For Apple Macintosh computers OSU has a site license for McAfee VirusScan which is available at https://it.okstate.edu/services/software-distribution.html. Please contact your Extension Technology Specialist or departmental IT specialist for more information.

How do I clean my system if it is infected? How do I rebuild my system?
Before attempting to rebuild Windows, upgrade your existing PC or Mac or clean an infected computer, we suggest you contact an IT specialist in DASNR IT or your department. Contact information is available at http://support.dasnr.okstate.edu/contact-us
Antivirus software can assist with malware cleanup; however, many times there are malicious applications other than viruses which need removed.

Can I let a friend use my OSU account password?
It is against OSU policy to use another person's account without proper authorization. Failure to comply may result in suspension of the User ID or other action as outlined in OSU policy or federal/state law.

What is a wireless internet connection?
Most notebook and laptops have built-in wireless network capabilities that enable a connection to the Internet without cable. Wireless access is not offered everywhere. Where offered, it is important that your wireless connection is secure to prevent eavesdropping.

Routers, Hubs, and Switches?
These devices allow multiple computers to connect to a network jack. On the OSU-Stillwater campus, prior approval from the Telecommunications department is required before these devices can be installed.

SECURING YOUR COMPUTER

Security Patches
Downloading and installing the latest security patches and updates for your Microsoft Windows and Apple Macintosh operating system and software programs significantly reduces the chance of your system being compromised. We suggest you enable Automatic Updates. For Windows systems go to https://support.microsoft.com/en-us/help/15081/windows-turn-on-automatic-app-updates.

Firewall
If your computer is connected to the internet, you should have an active and correctly configured firewall. For information on how to configure a firewall in Windows 10 go to https://support.microsoft.com/en-us/help/4028544/windows-10-turn-windows-defender-firewall-on-or-off

Passwords
A password should be at least eight characters in length and include letters (upper and lower case), numbers, and at least one symbol or punctuation.

User Security
Lock your computer when you are away from your desk using a password protected screensaver or by using the operating system's built-in protection. For Windows computers: https://support.microsoft.com/en-us/help/4026828/windows-change-your-screen-saver-settings

Personal Privacy
For more information on FERPA, GLBA, HIPPA, DMCA or the Oklahoma Computer Crimes Act, go to https://security.okstate.edu/ and click on "Policies and Procedures. Also, see https://it.okstate.edu/policies-procedures-and-guidelines/

Security FAQs For Faculty & Staff

DASNR Information Technology

Use of OSU computing systems in any way contrary to applicable Federal or State statutes or the policies of Oklahoma State University is prohibited and will make you subject to University disciplinary actions, including possible immediate termination, and may also subject you to criminal penalties and/or prosecution.

Use of OSU computer systems, authorized or unauthorized, constitutes consent to monitoring. Unauthorized use may subject you to criminal prosecution. Evidence of unauthorized use collected during monitoring may be used for administrative, criminal, or other adverse action. Use of OSU computer systems constitutes consent to monitoring for these purposes.

DASNR Information Technology
http://support.dasnr.okstate.edu
dwayne.hunter@okstate.edu
405.744.5536

OSU Information Security Office
http://security.okstate.edu
abuse@okstate.edu
405.744.1976

What is a computer security incident?
A computer security incident is an instance where a computer has been used as a tool to perform an act that violates university policy or the law.

How do I report a computer crime incident?
If you need to report an incident, please email abuse@okstate.edu or call 405-744-HELP. If the incident is a loss of physical assets or you feel threatened by any form of computer communication, retain as much of the evidence as possible and contact the OSU Police Department directly at 405-744-6523. The OSU Security Office aids the police in many investigations; however, these types of situations fall under police jurisdiction.

How do I determine whether a computer crime has been committed?
Oklahoma Criminal Statutes cites several acts which constitute computer crime. Some examples include unauthorized access of a computer, using a computer to commit fraud or control monies and threatening and harassing emails. Please view the link below to read the Oklahoma Computer Crime Statutes.
http://www.oscn.net/applications/oscn/deliverdocument.asp?citeID=70183

What is a copyright infringement?
A copyright infringement occurs when media is downloaded, stored, used, copied, and/or shared without legal ownership and without legal permission from the person or entity who created it. Violating a copyright is against OSU policy and Federal/State law. Title 17, Chapter 12, Section 1202, of the United States Code and the DMCA (Digital Millennium Copyright Act) of 1998 criminalizes and heightens the penalties for copyright infringement on the Internet. OSU actively works with commercial companies and Federal/State agencies to reduce copyright violations.

Where can I find applicable computer laws?
For information regarding computer laws refer to the following sites:
Computer Fraud and Abuse Act 1986 (US) 18 USC 1030
http://www.law.cornell.edu/uscode/text/18/1030
Oklahoma Computer Crime Statutes
http://www.oscn.net/applications/oscn/deliverdocument.asp?citeID=70183
The Digital Millennium Copyright Act
http://www.copyright.gov/legislation/dmca.pdf

What OSU policies address appropriate computer use?
OSU's Appropriate Computer Use policy outlines the responsibilities and expectations for institutional users: https://stw.sp.okstate.edu/policies/Shared%20Documents/Appropriate%20Use%20Policy.pdf. For other policies, see https://it.okstate.edu/policies-procedures-and-guidelines/

How should I respond to unsolicited email messages (spam) and what can be done about it?
OSU has two levels of email filtering that helps to minimize spam for @okstate.edu accounts, but when you receive chain mail or unsolicited mailings do not retaliate against the sender. This will only complicate the situation and could make you a party to a policy violation. Instead, consider creating an email rule to block the sender from future messages and consider forwarding the message to abuse@okstate.edu, an account monitored by OSU IT Security.

Am I allowed to experiment with security related software using OSU resources?
OSU Information Technology promotes network security and coordinates responses to unauthorized accesses. This includes working with local supporters, computer users and our Internet Service Provider to protect the campus from network intrusions, denial of service attacks and other unauthorized or inappropriate activities that impair network access. **Under no circumstance** should security-related software tools be used to experiment on OSU resources. Doing so may impair network access or cause problems for the entire OSU community.

What is encryption?
Encryption is the process of obscuring information to make it unreadable without special knowledge. There are many legitimate uses for encryption; however, use of encryption tools for purposes of violating university policy or state and federal law is prohibited.

What can I do if I think my account has been compromised?
Notify the IT Information Security Office at 405-744-4357 or abuse@okstate.edu. Change all of your passwords IMMEDIATELY. Please keep notes and report any unusual behavior or contact.

What activities constitute cracking (commonly known as hacking)?
Cracking includes breaking into computers or computer systems without authorization and copying, altering, deleting or destroying files or creating new files which may be destructive to existing data or to the system. These activities are illegal under the Oklahoma Computer Crimes Act and may constitute a felony.

Scanning/Probing?
Scanning or probing is a technique hackers use to gather as much information as possible about an application and/or a network infrastructure. The hacker looks for vulnerabilities to exploit and when found, uses the vulnerability to gain access to your computer or network. If you detect that someone has attempted to access, scan/probe, or "break into" a computer without authorization, please send the logs of the access attempts to abuse@okstate.edu.
For assistance in obtaining the logs call an IT Specialists in DASNR IT.

How do I report hacker attempts?
Forward the following information to abuse@okstate.edu: date/time of attack, intruder information, intruder's IP, port numbers and logs. Logs are important; submit all logs, e.g. Firewall/Event logs as evidence to assist on the investigation.