

Security Tips

When you are at work

1. Visit the NSU Policies and Forms pages:
<http://www.nsu.edu/policies>
<http://www.nsu.edu/forms>
<http://www.nsu.edu/oit/policies>
2. Always logoff or lock your PC when you leave and set a password protected screen saver.
3. Encrypt or password-protect sensitive files and use USB key encryption software.
4. Use strong passwords, use different passwords on each system and never share your password with anyone. Strong passwords have a minimum of 8 characters and a combination of upper and lower case letters, numbers and symbols.
5. Never open a file or click on a link in an email if you do not know or trust the sender.

For your personal computer

6. Keep your operating system up to date. Visit <http://windowsupdate.microsoft.com>
7. Use your operating system's built-in or third party firewall. For a free third party firewall, visit <http://www.zonelabs.com>
8. Use antivirus software (AV) and keep it up to date. For free AV software visit <http://free.grisoft.com> or <http://www.avast.com>
9. Use Anti-Spyware products. Visit www.lavasoftusa.com (*Ad-Aware*)
www.safer-networking.org (*Spybot S&D*)
<http://www.microsoft.com/athome/security>
10. Do not post personal information on public websites where anyone can access it.
11. Use wireless encryption on your home network.

Information Security

- The Information Technology Security Team provides guidance and support in several key areas of information security, ranging from network and computer security to physical access control systems. The team develops and implements global security policies, standards, guidelines and procedures ensuring the ongoing maintenance of the security architecture for application, data, infrastructure and network.
- The campus-wide firewall, Virtual Private Network (VPN), wireless and wired authentication, Intrusion Detection and Prevention (IPS/IDS) systems, antivirus software, computer and network monitoring, and investigation of security breaches are just a few of the team's responsibilities.
- The IT security team provides information security training to University departments and activities for the purpose of educating departments and group members on issues pertaining to information security.
- Security is based on Confidentiality, Integrity and Availability (the CIA triad). The Information Security Team strives in establishing the perfect balance within the CIA triad while at the same time empowering the end user and carrying forward the academic mission of the University.

Test Your Knowledge

- Do you know a legitimate URL when you see it? Test yourself online at <http://security.nsu.edu> while playing the Anti-Phishing Phil game. Phishing is one of the predominant ways criminals use to steal your identity.
- Take the on-line security awareness quiz at <http://security.nsu.edu> and learn about the policy on Acceptable Use of Technological Resources. Remember to print your certificate upon completion.

Frequently Asked Questions

Q. How can I do my work from home?

A. Faculty and Staff have the option to use VPN services from anywhere they have an Internet connection to their PC. Go to <https://spartanet.nsu.edu> for more info.

Q. What is NSU doing to make my Internet experience a safe and enjoyable one?

A. NSU uses a combination of an intrusion prevention system, a network firewall, anti-virus software, and other security tools to prevent attacks to your PC.

Q. Does the security team work with local and state authorities?

A. The security team will work with local, state and federal authorities as well as the internal and state audit department as needed.

Q. What should I do if my computer is infected with viruses, spyware or malware?

A. Contact helpdesk@nsu.edu or call 823-8678.

Q. What should I do if I believe someone has gained unauthorized access to my PC?

A. Report the incident to your supervisor and contact the Information Security Officer.

Q. Can I safely report security incidents to the security team?

A. Confidentiality is our guiding principle. You should report all security incidents you observe to the Information Security Officer.

Q. What constitutes a security incident?

A. A violation of university IT policies and/or a physical or computer breach is considered a security incident.

MEET THE SECURITY TEAM

Andrea Di Fabio

Information Security Officer

High Performance Computing Coordinator

adifabio@nsu.edu 757.823.2896

Ronald A. King

Information Security Engineer

raking@nsu.edu 757.823.3918

Office: *MCAR Suite 401*

Web: <http://security.nsu.edu>

E-mail: security@nsu.edu

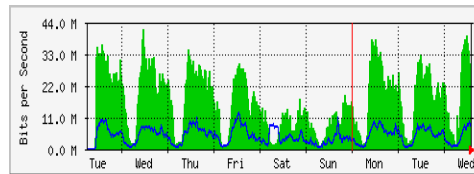
This Brochure is published by the
Office of Information Technology
with assistance from the
Technology Advisory Group (TAG)
and the Technology Systems
Support Team (TSST)

NSU SECURITY TOOLS

Intrusion Prevention

We employ a wide variety of specialized hardware, servers and software to detect and stop malicious network traffic and to spot security violations.

Internet Bandwidth

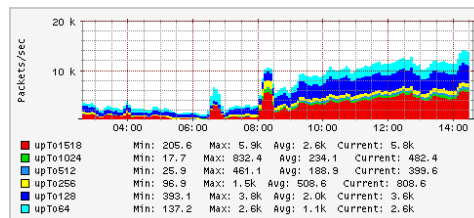


We constantly measure our total bandwidth to the Internet for capacity planning and to detect unusual traffic.

System Logging

We log, correlate and retain all security events such as logon/logoff times, system/data access and modification for forensic purposes and analysis.

Network Monitoring



We monitor network traffic and classify it by protocols. We prioritize business traffic and look for anomalies.



INFORMATION SECURITY

2008 – 2009

**Office of Information
Technology**

Norfolk State University

700 Park Ave.

Norfolk, VA 23504