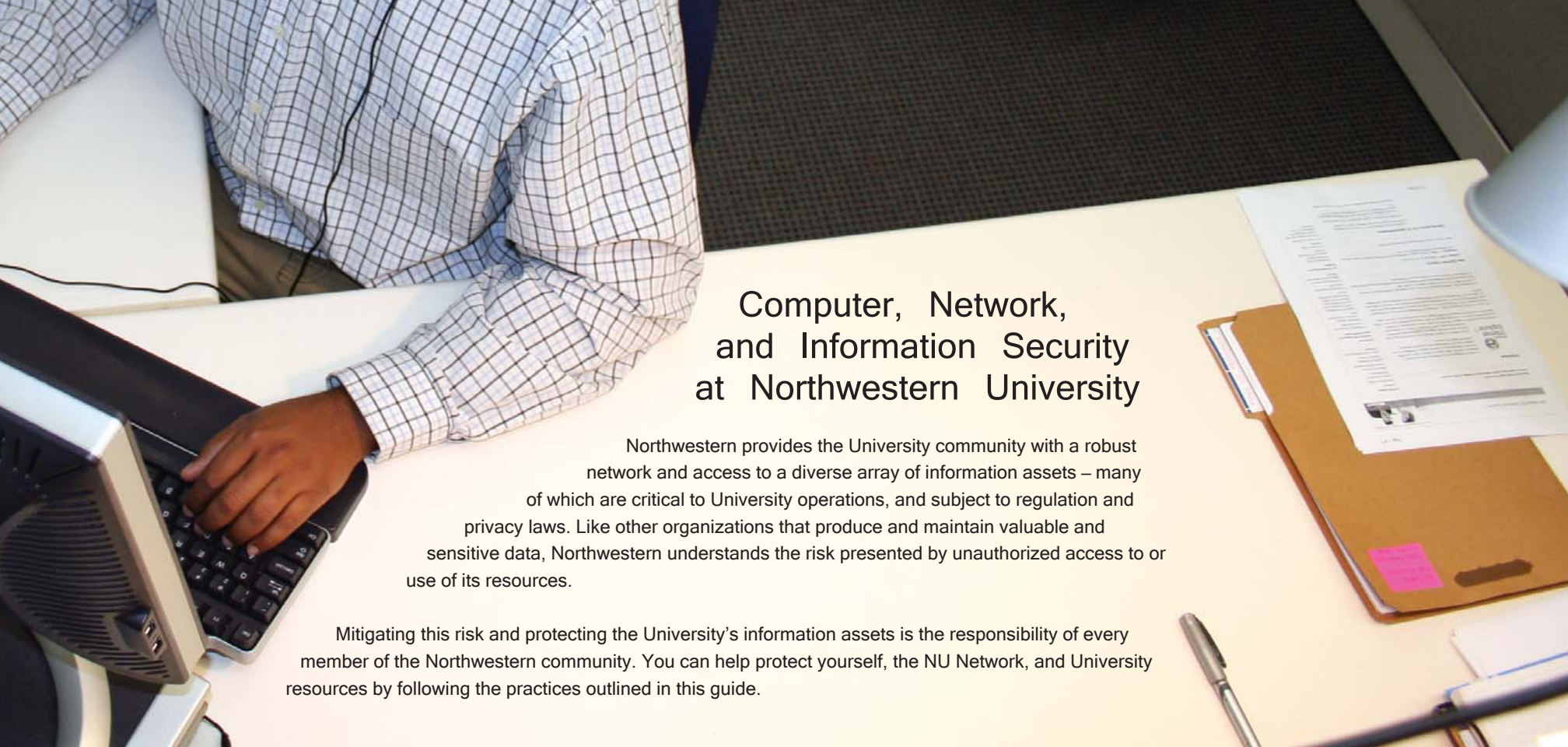




GET SECURE

Your data. Your privacy. Your role.

Northwestern University Information Technology

A high-angle photograph of a person's hands and arms in a light-colored checkered shirt typing on a laptop keyboard. The laptop is on a white desk. To the right of the laptop, there is a clipboard with a white sheet of paper and a pink sticky note. A silver pen lies on the desk below the clipboard. The background is a dark grey carpet.

Computer, Network, and Information Security at Northwestern University

Northwestern provides the University community with a robust network and access to a diverse array of information assets – many of which are critical to University operations, and subject to regulation and privacy laws. Like other organizations that produce and maintain valuable and sensitive data, Northwestern understands the risk presented by unauthorized access to or use of its resources.

Mitigating this risk and protecting the University's information assets is the responsibility of every member of the Northwestern community. You can help protect yourself, the NU Network, and University resources by following the practices outlined in this guide.

WHAT'S AT STAKE?

Northwestern University is committed to upholding the highest standards of information and network security. It is essential that we continue to work responsibly with personally identifiable information, as well as comply with state and federal legislation, program requirements, and University policy. Here are some of the things you can do and the benefits of those actions:

- » Your information – Protecting your personally identifiable information helps keep it private and out of the hands of identity thieves
- » Safety of our constituents – Proper handling of personally identifiable information helps the University comply with federal and state regulations, minimize the risk presented by identity theft, and avoid possible criminal and civil action and penalties
- » Network performance – Keeping your computer secure with anti-virus software, active firewalls, application patches, and an up-to-date operating system helps to keep the NU Network secure and stable
- » Northwestern's reputation – Protecting sensitive data from unauthorized access helps ensure compliance with privacy regulations, avoids adverse publicity, and bolsters the reputation of the University

WHAT'S A SECURITY INCIDENT?

An information security incident is any known or suspected event or circumstance that results in the unauthorized release or exposure of sensitive information beyond the University's sphere of control. Anyone with knowledge or a reasonable suspicion of an incident is instructed to make an immediate report to their management, local technical support staff, and NUIT's Network Operations Center at 847-467-NNOC (6662) or e-mail security@northwestern.edu.

What Does A Security Incident Look Like?

Incidents occur in many forms; here are a few examples:

- » The theft or physical loss of computer equipment known to hold files containing Social Security Numbers or other sensitive data
- » An unencrypted list of alumni contributors is e-mailed to an unauthorized recipient
- » A server known to hold sensitive data is accessed or otherwise compromised by an unauthorized party
- » Printed copies of student loan applications are discovered in a publicly accessible dumpster
- » A firewall is accessed by an unauthorized entity
- » A network outage is attributed to the activities of an unauthorized entity
- » An outside entity is subjected to a DDoS (Distributed Denial of Service) attack originating from within the University network



SECURE YOUR COMPUTER

START NOW

A computer must be secured before it connects to the Internet. An unprotected computer can be taken over in a matter of minutes and often without any outward sign of the compromise. Follow these steps to help ensure your system is secure.

SECURE PASSWORDS

Strong, effective passphrases/ passwords are simple and very important defenses for your computers and the NU Network. Best practices for passphrases/ passwords include:

- » Make them hard to crack by using an abbreviated phrase with characters and numbers
- » Do not share them with others
- » Change them immediately if you suspect a problem
- » Use different administrator and user passwords, where possible
- » Use them with your NetID at Northwestern only, not for outside applications
- » Password-protect all machines in your area

PROTECTIVE PROGRAMS

Viruses, spyware, and other malware can cause computer malfunction or allow hackers to steal data. Once a virus is on your machine, it can infect other computers on the NU Network, so protective programs are essential:

- » Symantec AntiVirus – Available free for download from NUIT; set it for regular scanning and automatic updates
- » Spyware – NUIT recommends free Spybot - Search & Destroy to regularly scan for spyware
- » Firewall – Prevent unauthorized connections to your computer
- » Find full instructions and downloads:
www.it.northwestern.edu/security

SECURE SETTINGS

Security flaws can exist in any operating system or software program, and these exploitable holes must be fixed with small programs called patches, issued by the manufacturer. To make sure your computer is always up-do-date with security patches:

- » Enable operating system Automatic Updates – Instructions available on the NUIT Web site
- » Update software when prompted, especially AntiVirus
- » Find full instructions and downloads:
www.it.northwestern.edu/security

SMART HABITS

A good way to defend yourself and the University from security incidents is to use smart security habits. Keep the following tips in mind to guard against cybercrime:

- » Do not open unexpected attachments
- » Be skeptical, and use caution when downloading anything
- » Turn your computer off or to hibernate mode if not in use
- » If you suspect a security incident, report it immediately to NUIT's Network Operations Center at 847-467-NNOC (6662)



SECURE
YOUR
WORKING
ENVIRONMENT

PROTECTED DATA

Treat all sensitive data as a highly valuable asset, and minimize the chance that it is released to unauthorized users:

- » Identify sensitive data inputs, locations, and sensitivity
- » Do not use Social Security Numbers as an identifier, use employee or student ID numbers instead
- » Encrypt private data sent across the network; see your local technical support staff for details
- » Save sensitive data files to a network drive, not a work or personal computer
- » Allow access to sensitive data to only those who “need to know”

CAREFUL DISPOSAL

When you no longer need sensitive data, it is better to dispose of it than continue to account for it. Ensure data cannot be recreated, and follow careful disposal best practices:

- » Only store necessary data
- » Shred papers containing sensitive data
- » Follow the Disposal of Northwestern University Computers Policy:
www.it.northwestern.edu/policies/disposal.html
- » Sanitize hard drives of disposed computers to remove sensitive data
- » Dispose computers through University Services' Computer and Peripherals Recycling Program

SAFE CONNECTIONS

Sensitive data is more easily stolen when it is being shared between users, so take note of the connection you use. Unapproved wireless networks, e-mail, and public computers are particularly vulnerable to security breaches.

- » Use only Northwestern-approved networks and wireless access points
- » Do not e-mail private data, as messages can be intercepted
- » Use Virtual Private Network (VPN) when off campus for a secure connection

BE PREPARED

In the event of a disaster or a security incident, do you know what to do? These events occur unexpectedly, so find out in advance how to respond:

- » Report any known or suspected security incident to your management, your local technical support staff and NUIT's Network Operations Center at 847-467-NNOC (6662); you can also send an e-mail to security@northwestern.edu
- » Learn about your school or department's business continuity plans from your dean or department chair
- » Make regular system backups and test your system restore function; check with your technical support staff for details



NORTHWESTERN
UNIVERSITY

Northwestern University Information Technology
1800 Sherman Avenue
Evanston, Illinois 60201

www.it.northwestern.edu

Produced by NUIT Communications.

© 2007 Northwestern University Information Technology. All rights reserved.



SECURITY RESOURCES

Report suspected computer, network,
and information security incidents

NUIT Network Operations Center
847-467-NNOC (6662)
security@northwestern.edu

Contact NUIT Information Security

NUIT Information Systems and
Security/Compliance (ISS/C)
security@northwestern.edu

Report crimes or emergencies

University Police
911 on campus

Recycle computer hardware

University Services
847-491-7569
univsvcs@northwestern.edu

Find out more

www.it.northwestern.edu/security