

# NUIT

Northwestern University  
Information Technology

# NUIT Tech Talk - Computer Security Basics

**March 17, 2009**

**Roger Safian**

**[r-safian@northwestern.edu](mailto:r-safian@northwestern.edu)**



# NUIT

Northwestern University  
Information Technology

# Agenda

- Introduction and brief bio
- Security statistics
- Securing Your Computer
- Things NOT to do
- Online Resources
- Questions



# NUIT

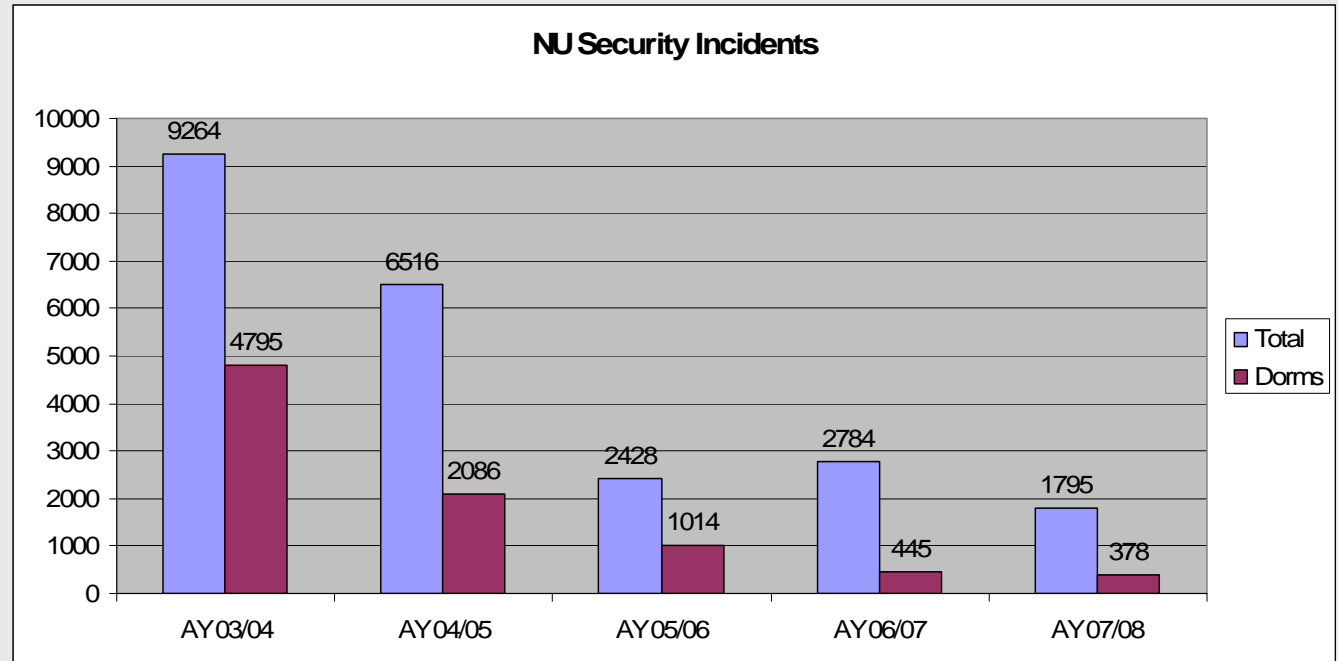
Northwestern University  
Information Technology

## About Me

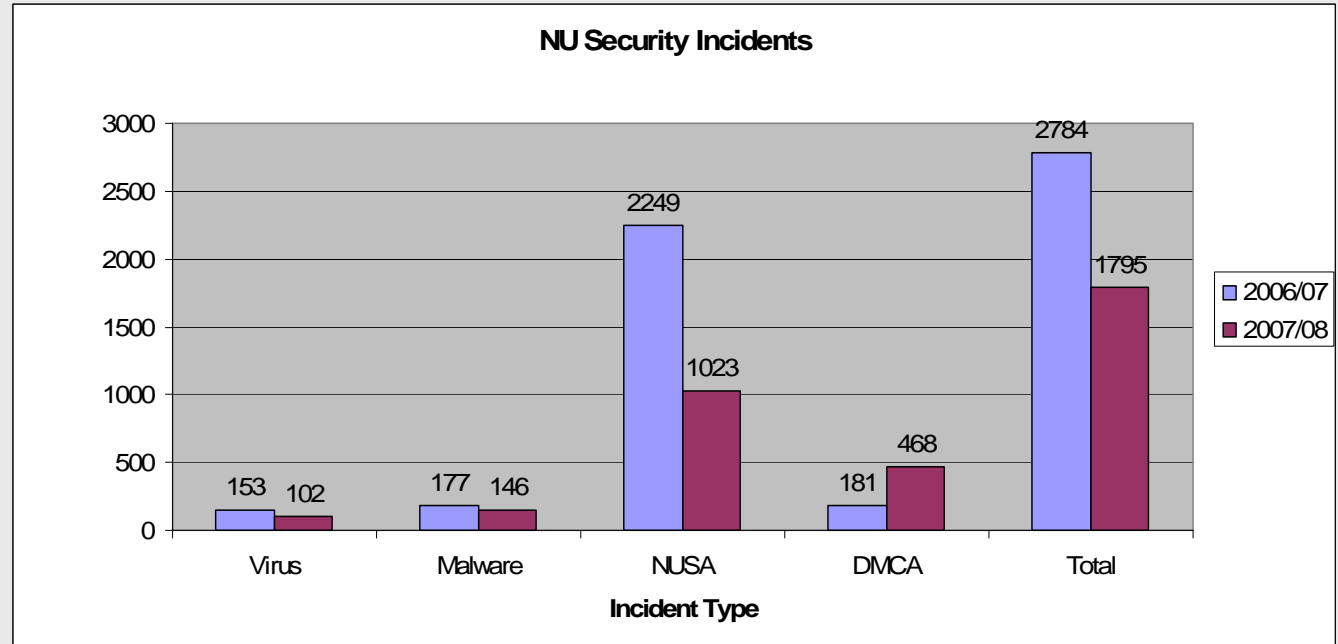
- NUIT – Senior Data Security Analyst
  - Information & Systems Security/Compliance
  - 20+ years at Northwestern
- NU-CERT
  - Incident Response Team
- FIRST
  - NU's representative
  - Former Steering Committee member
- CIC/Big Ten Security Working Group
  - Former chair



# Security Statistics



# Security Statistics (cont'd)



## Why These Incidents Occur?

- Weak Passphrases
  - All machines and accounts need passphrases
  - Use rules similar to the NetID rules
- Opening viral attachments
  - Don't open unexpected attachments
  - Only open specific types of extensions
  - Make sure to look at the LAST extension

# Why These Incidents Occur (cont'd)

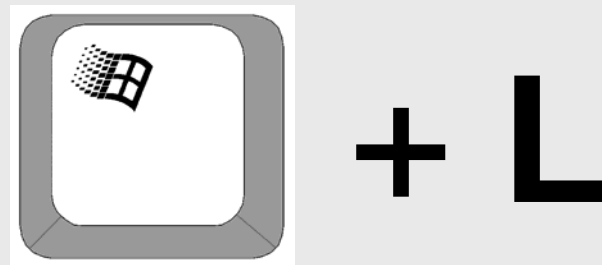
- Updates not applied
  - Ensure Windows update runs automatically
  - Don't forget about layered products
    - Anti-viral
    - Web Browser
- Network use
  - Instant Message
  - P2P
  - Be careful when clicking on links

## Ground Rules

- Microsoft focused
- In your department
  - Check with your department tech support
  - Report anything that seems unusual
- At home
  - You are the tech support
  - Know what your family does online
  - **Never** share your NetID or passphrase

# Turn Your Computer Off

- If your computer is off, it can't be compromised
  - You save energy as well
- Lock computer when you leave
  - *Hold down the **Windows Key** and press **L***



# Passphrases

- NU NetID Passphrase
  - Be cr34t1v3 (creative)
    - Fth,oM (From the halls of Montezuma)
  - Longer is better
    - NUIT is working to extend the length of passphrases
  - Never share your passphrase
- Windows Passphrase
  - Separate accounts; separate passphrases
  - Change regularly

# Software Updates & Patches

- Windows Update
  - Should be set to run automatically
  - Check manually as well
- Other software
  - E-mail software
  - Web browser
  - Microsoft Office
  - Antivirus software
  - Instant Messenger

# Firewall Protection

- Standard with Windows XP SP 2
  - And many other products/operating systems
- Always keep your firewall active
- Combine with hardware firewall if possible
- Zone Alarm is free for home use
  - <http://www.zonealarm.com/>
  - Search for “free Zone Alarm”

# Antivirus Software

- Never open unexpected files
- Keep up to date
  - Set to auto-update
  - Get updates from Symantec
    - <http://www.it.northwestern.edu/transitions/2008/savswitchtool.html>
- Run regular scans (weekly or more)
  - Try from Safe Mode (reboot, *hold F8*)
- Delete files from quarantine

# Instant Messenger

- Malware spreads via buddy lists
  - Often done without the knowledge of the infected user.
- Verify that a link was sent to you
  - Ask the sender if they sent you a link
- Be very cautious about installing extra plugins to your client

# Spyware

- Disable ActiveX and Javascript
  - Tools > Internet Options > Security
- Be careful when downloading programs
- Use a spyware removal program
  - More than one is better
  - Spyware – Search & Destroy:
    - <http://www.safer-networking.org/en/>

# Junk E-mail (Spam)

- Never reply to remove
- Use junk e-mail filters
- E-mail Defense System (EDS)
  - Filters some junk e-mail and viruses at server level; only for central mail servers
    - Only monitors the alias Not the actual mailbox

# Phishing Scams

- Phishing: Fraudulently attempting to obtain personal information
  - Typically through email
- Never give your personal information in response to a unexpected request
- Use out-of-band communication to verify
- Double-check embedded URLs

# Copyright Violation

- Peer-to-peer (P2P) software **is legal**
- Violation of copyright **is illegal**
- Malware targets P2P software
- Be aware of what your children and household members are doing
  - It's you who gets sued
    - And pays any penalty

## Recommendations

- Windows update set to automatic
- Anti-Virus software up to date
- Strong Windows passphrase
  - 15 characters is the “sweet spot”
- File sharing is OFF
- Firewall is ON
- System Restore is OFF
- Guest account is disabled

## Things NOT To Do

- Turn off automatic updates
- Turn off firewall
- Turn off Anti-Virus software
- Uninstall Service Packs or Hotfixes
- Relying on browser X as “secure”
- Not checking that the admin account has a strong passphrase

## Things NOT To Do (cont'd)

- Rebuilding a machine, while it's on the network
- Put infected machine on the network to download updates and fixes
- Install a firewall to limit malware already on an infected machine
- Knowingly working with pirated software

# Online Resources

## NUIT Web info

- Computer and Network Security
  - <http://www.it.northwestern.edu/security/index.html>
- Reporting a Security Incident
  - <http://www.it.northwestern.edu/security/help.html>
- Secure the Work Environment
  - <http://www.it.northwestern.edu/security/working.html>
- Incident Response Protocol
  - <http://www.it.northwestern.edu/policies/incident.html>

## Contact Information

- Roger Safian
  - (847) 491-4058
  - [security@northwestern.edu](mailto:security@northwestern.edu)
  - [r-safian@northwestern.edu](mailto:r-safian@northwestern.edu)
- NUIT Support Center
  - (847) 491-**HELP** (4357)
  - [consultant@northwestern.edu](mailto:consultant@northwestern.edu)
- Northwestern Network Operations Center
  - (847) 467-6662 (staffed 24 hours per day)

# NUIT

Northwestern University  
Information Technology

# Questions?



NORTHWESTERN  
UNIVERSITY