UT ARLINGTON

Information Security Office

# An Introduction on How to Better Protect Your Computer and Sensitive Data

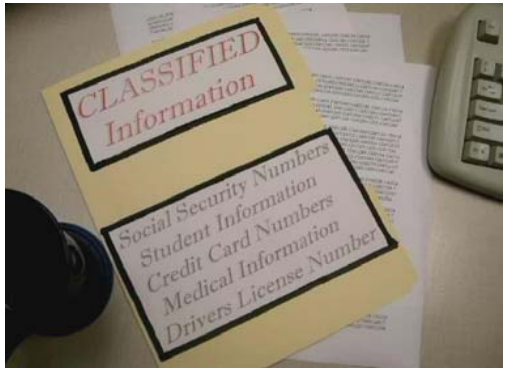

# Common Security Problems

- Computer users who fail to use “strong” passwords
- Constant attacks by viruses, worms, key loggers and bots
- Unauthorized software downloads containing viruses
- Email scams targeting sensitive information (phishing)
- Social engineering attempts (persons posing as staff)

# Computing Policy & Laws

All UT Arlington Faculty and Staff should be familiar with:

- Family Educational Rights and Privacy Act (FERPA)
- Health Insurance Portability & Accountability Act (HIPAA)
- Texas Administrative Code (TAC 202)
- UT Arlington / UT System Computing Policy (UTS 165)
- Policy, Law and Procedures listed at: www.uta.edu/security




# Sensitive Information Protected by FERPA

Sensitive information may include SSN, Drivers License, credit & debit card numbers, photographs, passwords, email address, student & staff directory information (address, phone numbers, date & place of birth, major, classification, participation in officially recognized activities and sports, dates of attendance, weight and height of members of athletic teams, enrollment status, degrees and awards received and most recent previous school attended).

Student directory information may be flagged at the request of the student as confidential and must not be disclosed.


# Protecting Sensitive Information

- Unless required for your job, all social security numbers should be replaced with UTA ID Numbers (a.k.a. EmplID)
- Never store sensitive information on your computer / laptop
- Keep all sensitive documents organized and under lock & key
- Dispose of documents / media containing sensitive information when no longer used. UT Arlington staff must consult records retention policy: www3.uta.edu/policy/retention/home.htm


# *Use A Strong Password As Your First Line of Defense*

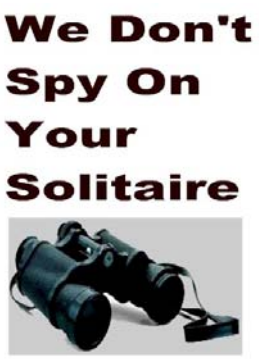
- Select a password that is a minimum of eight characters
- Use symbols ($,%,*), numbers, UPPER / lower case letters
- Example of a strong password: Y3!!0W*Tz
- Never write down your password, if so lock it up
- Never share or grant access to your computer / password


# Security Best Practices

- Never open attachments or click on links from strangers
- Never respond to “phishing” emails asking for personal info
- Beware of “malicious” software and internet downloads
- Use an anti-virus program, confirm definitions are updated
- Update patches when released to avoid “Zero Day Exploits”


# Security Best Practices

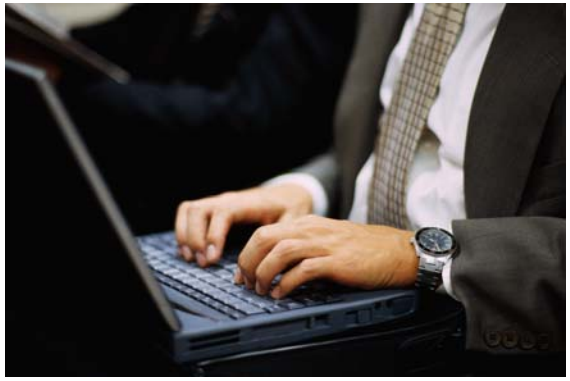
- By default staff computers have security settings enabled
- You should also protect your personal computer / laptop
- Confirm that your system firewall is enabled
- Confirm that your antivirus is set to auto update definitions
- Confirm that patches for your operating system and installed software programs are constantly updated


# *Network Monitoring Helps Protect Users*

UT Arlington Information Security Office has network monitoring software and hardware in place to monitor inbound and outbound network communications, watching the UT Arlington Network for potential threats.

However, persons using any UT Arlington computing resources should not have any reasonable expectation of privacy. All criminal and legal matters will be handled by the UT Arlington Police and Legal Department.



# Beware of Potential Threats
# Key Loggers

- A key logger is a program that can be installed remotely or manually on your computer or laptop (usually a payload of a computer virus or bot infection)
- Criminals use key loggers to record your passwords, credit card numbers, financial information and websites visited
- Some anti-virus programs can detect key loggers (spyware)

# *Beware of Potential Threats Bot Networks*

- A bot network is malicious code that is secretly installed on your computer or laptop via computer exploit, rootkit or virus
- Bot Networks can be used for denial of service attacks against other computer systems crashing their networks
- Bot Networks can be used to access your sensitive data so that it can be sold on the internet or used for identity fraud

# Beware of Potential Threats Password Crackers

- Password crackers were once used by system admins to help users who had forgotten passwords, they are now often used as a tool by criminals to break into computers
- Simple passwords can be “cracked” in seconds. Use a “strong password” or “pass phrase” for better security


# *Beware of Potential Threats*
# *Social Engineering*

Persons conducting a “Social Engineering Attempt” are trying to gain access to information or areas by pretending to be someone that they are not. Examples of threats include:

- Imposters posing as tech support asking for passwords
- Emails asking for sensitive information (a.k.a. “phishing”)
- Phone calls from persons posing as employees / officials
- Pretending loss of access cards or keys to “borrow” yours
- Social networking sites or surveys asking for information

**Always report suspicious persons to authorities!**

# *Have Questions? Contact Us!*

For more help with technical issues first contact the UTA Helpdesk: 817-272-2208 helpdesk@uta.edu

For information about UTA computing resources visit the OIT website: www.uta.edu/oit

For information about UTA computing security visit the security website: www.uta.edu/security

If you are aware of a suspected computer crime contact the UT Arlington Police x3381