Boston University Security Awareness

What you need to know to keep information safe and secure

BOSTON UNIVERSITY

Introduction

- Welcome to Boston University's Security Awareness training.
- Depending on your reading speed, this presentation will take approximately 8 minutes to complete.
- This training is meant to familiarize you with common computer security concerns.
- As well as addressing security pitfalls, we will also discuss methods of avoiding problems which could expose critical University data.
- These strategies will also allow you to better protect your own personal information in your day-to-day computing.

Introduction

- This training is intentionally general in nature. Directions on how to implement specific security changes will be covered in later trainings.
- Your BU workstation's security settings may be determined by whoever provides your desktop or network support.
- Any questions on changing the settings on a workstation at BU should be directed to the appropriate support personnel.

BOSTON UNIVERSITY

Why be concerned?

- Think about everything you use your computer for:
  - Banking
  - Shopping
  - Paying Bills
- Then consider how much of your personal information is involved in those transactions; social security number, name, address, medical information, etc.
- Now imagine the amount of personal information, sensitive information, Boston University collects on students, faculty, and staff.

BOSTON UNIVERSITY

What can you do?

- There are simple steps we can all take to insure University information is not compromised.
- Three factors are of primary importance:
  - Confidentiality - Protecting information from unauthorized disclosure.
  - Integrity - Protecting information from unauthorized modifications, and ensuring the information is accurate and complete.
  - Availability - Ensuring information is available when needed.

BOSTON UNIVERSITY

How are we threatened?

- Unfortunately the severity and range of threats to information security are increasing every day. Some threats to be aware of include:
  - Viruses - Small pieces of malicious software which “infect” your computer.
  - Spyware - Software which collects information from your computer which can be used to exploit your system.
  - Operating System Holes - Weaknesses in the operating system which may or may not be known to the manufacturer.
  - Weak Passwords - Simple passwords which can be guessed or cracked.
  - Social Engineering - Seemingly innocent schemes which trick you into voluntarily divulging sensitive information.

Viruses

- Just like with biological viruses, the simplest way to avoid a computer virus is prevention.
- Computer viruses are designed to be destructive. To destroy files or systems or to create more widespread mayhem across the larger network.
  - Boston University has free anti-virus software available for download at http://www.bu.edu/tech/desktop/virus-protection-security/
  - As long as you have properly installed and updated anti-virus software you will greatly reduce your risk of infection.

Viruses

- You should also take a few common sense steps to keep from getting infected:
  - Don’t open email attachments you don’t recognize. Email from unknown senders frequently contains viruses.
  - Don’t load data storage devices on your work system from untrusted sources, or even from your own home computer, unless you know they’re clean of viruses.

Spyware

- Spyware has become a greater threat than viruses in recent years.
  - Spyware is less obvious in its impact on your system, and does not necessarily adversely affect your performance. Rather, it is designed to collect information about you or your system and send it to someone who can use the information to attack your system or break into accounts you might have on other systems.
  - Boston University has free anti-spyware software available for download at http://www.bu.edu/tech/desktop/virus-protection-security/spyware/preventing/

Spyware

- If you have properly installed and updated anti-spyware software you will greatly reduce your risk of exposure.

Operating System Holes

- Making a perfect piece of software is nearly impossible. No matter how hard Microsoft or Apple might try there are still going to be things they miss.
- Sometimes this leads to holes in how the software functions and these holes can be utilized to attack your system.
- When manufacturers become aware of security holes they will release patches to fix them. Most systems have an automated method for downloading and installing such updates.
- Whether you do it manually or automatically you need to keep your software updated with the latest patches.

Avoid Weak Passwords

- A weak password contains
  - less than eight characters
  - common usage words such as:
    - Names of family members, pets, friends, co-workers, fantasy characters, etc.
    - Computer terms and names, commands, sites, companies, hardware, software.
    - "Boston University", “Boston", or unit names.
    - Any of the above spelled backwards.
    - Any of the above preceded or followed by a digit (e.g., secret1, 1secret)

Avoid Weak Passwords

- words found in a dictionary (English or foreign)
- Birthdays, addresses, and phone numbers.
- Word or number patterns like aaabbb, qwerty, zyxwvuts, 123321, etc.

Use Strong Passwords

- A strong password contains
  - Both upper and lower case characters (e.g., a-z, A-Z)
  - Digits, punctuation characters, and letters (0-9, !@#$%^&*()_+|~-=\`{}[]:";'<>?,./)
  - At least eight alphanumeric characters long
  - No words in any language, slang, dialect, jargon, etc.
  - No personal information, names of family members, etc.

Use Strong Passwords

- Try to create passwords that can be easily remembered.
- One way to do this is create a password based on a song title, affirmation, or other phrase. For example, the phrase might be: "This May Be One Way To Remember" and the password could be: "TmB1w2R!" or "Tmb1W>r~" or some other variation.

Social Engineering

- Social Engineering describes the non-technical methods used to learn sensitive information about a user or system. Examples include:
  - FREE! Websites – sites which offer a “special deal” to you
    - You create an account and password to get it. Sometimes they even send you the item.
    - But what they also give you is a piece of spyware which sits on your computer and tracks the websites you go to.
    - Then those sites are sent to the attacker. They try the same username and password you gave them when you created an account on their site to try and gain entry to your banking, or 401k plan, etc.

Social Engineering

- Since people often use the same username and passwords this sort of ruse works a lot of the time.
- To avoid this problem use different usernames and passwords on all your online accounts.

- NEVER use your work username and password for personal accounts.
- Someone calls and asks you for information.
  - Ask them for their name, company and phone number.
  - In almost every case, the caller will disconnect when asked questions or placed on hold.
  - Or if someone you do business with calls you, look up their official number and call them back.
- If you are unsure whether an email request is legitimate, try to verify it by contacting the company directly.

Our Environment

- Without some understanding about the University environment it is difficult to work effectively to help reduce security threats.
- We should focus on several factors to help us better determine what we can do to secure our data:
  - What are the systems used for? While we want to have the most secure solutions possible, we also want them to be appropriate to the sensitivity of the data and the level of exposure.
  - Who is supposed to have access; to what, and why? Often people are granted more access than they need.
  - If someone asks you for access to information, make sure you confirm that they should have it.

Our Environment

- Once we understand how the environment is supposed to be, we will better be able to identify when there has been a potential security incident.

Security Incidents

- Examples of security incidents include:
  - An account password is compromised either through guessing or being cracked.
  - There is a hacking attempt made against your system; some attempt to force entry or exploit a vulnerability.
  - Computer files go missing.
  - There are unexplained changes to system data or your configurations.
  - You become infected by a virus.
  - Your laptop, workstation, PDA, or other electronic system is stolen.
  - An unauthorized user attempts to access your system.

Security Incidents

- If you suspect a problem, contact the IS&T Incident Response Team (IRT). You can report a suspected issue to them via the web at http://www.bu.edu/tech/security/incidents/reporting/ or by calling their hotline at 617-638-1100.

Security Tips – Email Attachments

- You should never open an attachment unless you can answer “YES” to all three of the following conditions:
  - I know who sent me the file.
  - I am expecting this file or similar ones to be sent to me.
  - I know my anti-virus software is up-to-date.

Security Tips – Physical Security

- Remember to always log out if you are going to step away from your computer for any length of time, or you are finished using it.
- Always enable a password-protected screen saver on your computer.
- Consider using a boot password for your computer.
- Be aware of who has keys to your workplace and who has physical access to your office.
- Shred documents containing sensitive information.
- Make sure your data is being backed up daily.

Security Tips – Firewalls

- A firewall is a piece of software or hardware which acts as a protective barrier between your computer and potentially harmful content on the Internet.
- Firewalls help guard computers against hackers as well as many computer viruses and worms by only allowing traffic that you need reach your computer.
- If your operating system has a built-in firewall be sure it's enabled. B.U. Linux, Apple OS X, and Microsoft Windows XP sp2 all have their own firewalls.
- Go to: http://www.bu.edu/tech/desktop/virus-protection-security/safe-computing/firewall/ for more information.

Boston University Contacts

- **IT Help Center** - can answer most personal computing support and network connectivity questions. http://www.bu.edu/tech/desktop/support/help-center/
- We also offer a network-based file-backup service for departmental servers and individual workstations. http://www.bu.edu/tech/infrastructure/backup-restore/
- **IS&T Information Security** - can answer your computer security related questions, and address University administrative data access & concerns. http://www.bu.edu/tech/security/

BOSTON UNIVERSITY