Every Day Security

IS&T Technology Fair

October 10, 2018

BOSTON UNIVERSITY

Introduction and Agenda

Tom Grundig
Assistant Director of Information Security
Boston University

- What day-to-day things can I do to make myself and my data safer?

BOSTON UNIVERSITY


7X24 HOURS
PROTECTED BY
ALARM SYSTEM

…nope

…yup

Physical Security

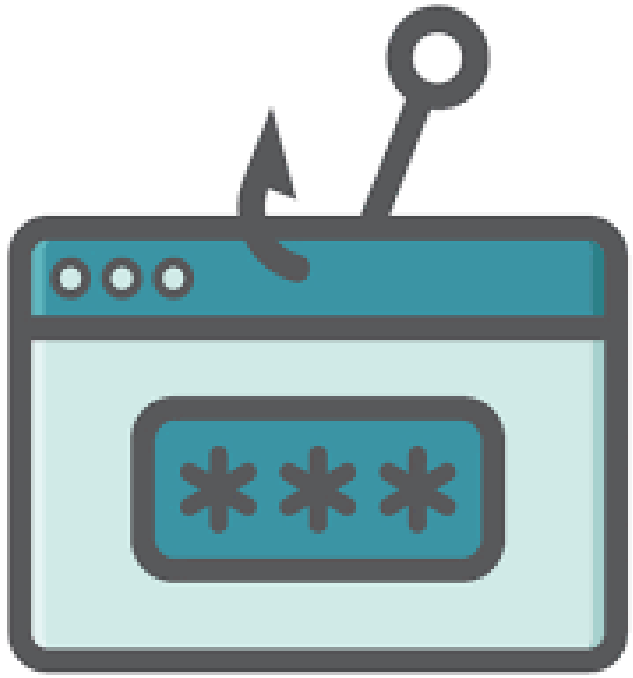
- Don’t let people ‘tailgate’ behind you into a secure area
- Protect your belongings behind locked rooms/drawers
- Lock/password protect your devices
- Set your device/screen to automatically lock when you’re away
- Shred old documents

Protect Your Online Identity

- Use complex passwords/passphrases, UNIQUE for each site (password managers help)
- Do not share passwords with anyone
- Use Multi Factor Authentication
- Close old/unused accounts
- Do not post anything that can allow cyber criminals access to your life

Don’t Get Phished

- Review links before you click!
- Does the email ask you for your password?
- Is the email about a financial account you’re not familiar with?
- Is there an attachment you weren’t expecting?
- Does the email have obvious grammar/spelling mistakes?
- Review your accounts and financial statements



Keep Systems/Software Updated

- Configure Operating System to automatically download and install updates/patches
- Keep software up to date (Office, Adobe, Java, Flash etc.)
- Keep mobile devices and apps updated
- Keep Internet-enabled devices updated (security cameras, thermostats, appliances etc.)

Antivirus Software

- Always install and enable AV software
  - Yes even on a mac
  - Yes even on a mobile device
- Keep AV software up to date

Safe Surfing

- Be wary of public/non-secured Wi-Fi
- Use VPN
- Shop from trusted sites
- Check the web browser address bar…is the page secure?

Disk Encryption

- Use Native Operating System full disk encryption
  - Microsoft – Bitlocker
  - Mac – FileVault
- Don’t store your sensitive data unencrypted.
- If you have a BU owned Windows or Mac system, IS&T will help you encrypt your hard drive, as well as manage your key.
- For student and personal machines, IS&T can provide easy to follow instructions on how to encrypt your own devices.

Multi-Factor Authentication

- For BU systems, Duo can be used on several services, such as Shibboleth, Windows RDP, Unix SSH, Web Apps; let us know and we'll see if we can help.
- Enable it wherever you can! (social accounts, personal email, banking accounts etc.)
- Duo mobile app can be used to manage MFA keys for personal accounts as well (i.e. Facebook, AWS, Gmail)

Back-Up Your Data

- Backup data on a regular, reoccurring basis
- BU systems are eligible for backup and restore services provided by IS&T through CrashPlan.
  - Any files you choose to back up will be encrypted and securely stored on a server that is off campus (in the cloud). You can restore them yourself without having to contact IS&T.
- Students or BU community members interested in backing up a personal computer can take advantage of our 25% BU discount for personal licenses.

CRASHPLAN™

Secure Media Destruction

- When Internal, Confidential, or Restricted Use data is no longer required for business purposes, it must be disposed of securely—in a way that prevents it from being read or used again.
- IS&T offers a service where we will have your media physically shredded and recycled, free of charge.

If something bad does happen…

BU Information Security

(Cyber) Incident Response Team

- 617-358-1100
- irt@bu.edu

We're here to help!

Questions