BOSTON UNIVERSITY
SECURITY 101

PROTECT YOUR ONLINE ACCOUNTS

- **USE PASSPHRASES** A passphrase is a sentence rather than a collection of random characters, for instance it can be something like: IloveB0st0nintheFall! (note use of zeroes in the word "Boston", uppercase and special character to fulfill complexity requirements)
- **DON'T REUSE YOUR PASSWORDS** Using the same password across multiple accounts leaves these accounts vulnerable. When one of them is breached , all of them can be breached. Use unique passwords for your accounts, especially your most important accounts like your BU account, banking account or personal email.
- **CONSIDER A PASSWORD MANAGER** In order to aid you in your quest to create a unique password for each of your online accounts, consider using a password manager.
- **ENABLE TWO-FACTOR (2FA) OR MULTI-FACTOR AUTHENTICATION (MFA)** One of the best ways to secure any account, password manager or not, is to enable MFA. Whenever it is available use it for your online accounts. At BU we use DUO 2FA to protect your accounts. Using the Duo App is the most secure and cost effective method.
- **CHANGE YOUR PASSWORDS PERIODICALLY** Visit the Terrier Cybersecurity Checkup cybercheckup.bu.edu to see your BU password age then decide if it's time to change your password. For all other accounts, set a time frame and update as often as necessary.
- **CHANGE YOUR PASSWORD IMMEDIATELY** If you've clicked on a suspicious link or inadvertently handed over your password https://www.bu.edu/tech/services/security/iam/authentication/kerberos/kerberos/

PROTECT YOURSELF FROM MALWARE

- **MALWARE IS SOFTWARE** designed by cyber attackers with the intention of gaining access or causing damage to a computer or network. Malware is a contraction for “malicious software.” Examples of common malware includes viruses, worms, Trojan viruses, spyware, adware, and ransomware.
- **MOST MALWARE** is distributed via email in the form of a bad attachment or hyperlink. It can also be distributed by SMS/text.
- **AVOID ATTACHMENTS** with suspicious extensions, such as .exe, .scr, .vbs, .hta, .reg or .bat.
- **HOVER OVER LINKS** or display them (if you're using a smartphone) before you click. Verify they go where they say they are going.
- **DOWNLOAD CROWDSTRIKE** for your laptop or desktop at bu.edu/tech/crowdstrike This software is free of charge for all faculty, staff and students. Crowdstrike replaces McAfee Antivirus, offering next generation protection.

PROTECT PRIVACY AND DATA

- **DON'T COLLECT DATA** you don't need.
- **ELIMINATE DATA** you no longer need. Delete files and shred documents with sensitive information. BU Information Security holds a document and hard drive shredding event Spring and Fall on campus, take advantage and clear out old files and dispose of electronics safely and securely.
- **REVIEW THE BU DATA MANAGEMENT POLICY** If you're handling data at BU, make sure you review our the Data Protection Standards which details the classifications of data, who and how data should be handled and in order to keep privacy and integrity intact.

BU INFORMATION SECURITY
CONTACT: buinfosec@bu.edu
VISIT: bu.edu/infosec

BOSTON UNIVERSITY
SECURITY 101

TO REPORT A SENSITIVE DATA INCIDENT OR BREACH

Call our 24 hour hotline at 617-358-1100

Or visit www.bu.edu/contact and select one of the following topics:
1: Information Security & Business Continuity
2: Cybersecurity Incident Response
3: Sensitive Data Incident Response

IDENTIFY AND REPORT PHISHING

- **LOOK OUT FOR THE WARNING SIGNS** There are several warning signs you've received a phish in your inbox:
  - **URGENCY** Cyber criminals want you to take action without thinking. Therefore they create a sense of urgency and call to action when crafting their scams
  - **REQUESTS FOR PERSONAL INFORMATION** Be wary of requests for your information. A legitimate organization will never ask you for your password or other personal information
  - **TIMELINESS & CONTEXT** *Timing is everything*. If an email seems untimely and out of context, stop, think, and ask "*why am I receiving this email right now?*"
  - **SENDER INFORMATION** Verify the sender by verifying the "*From:*" is a legitimate address. Valid BU emails will ONLY come from a '*username@bu.edu*' address.
  - **POOR GRAMMAR** Awkward wording or misspellings within an email from a reputable source, or even a colleague or friend, is often an indicator you may have received a phishing email
  - **HYPERLINKS** Remember, never click on links before verifying they go where they say they're going.
  - **ATTACHMENTS** Verify ANY attachments you receive before opening them. Check the sender information is correct and known to you or reach out directly to the person or organization sending the email

TO REPORT A PHISHING EMAIL

If you received a phishing message, particularly one falsely claiming to be from BU, forward it to **abuse@bu.edu** along with the message headers and then delete it

INSTRUCTIONS ON INCLUDING HEADERS

www.bu.edu/tech/services/cccs/email/office-365-outlook/management/headers

BU PHISHING GUIDE

Visit this guide for a quick overview of phishing and the warning signs

www.bu.edu/tech/support/information-security/security-for-everyone/phishing

BOSTON UNIVERSITY PHISH BOWL

Here you can find a list of the latest phishing scams reported by the BU community.

www.bu.edu/infosec/phishbowl

ADDITIONAL BU RESOURCES & POLICIES

TERRIER CYBERSECURITY CHECKUP

Visit the Terrier Cybersecurity Checkup and view your BU password's age, breaches your BU account has been associated with, and devices attributed with your DUO 2FA account at BU.

cybercheckup.bu.edu

BOSTON UNIVERSITY
SECURITY 101

SECURING YOUR MOBILE DEVICE

www.bu.edu/tech/support/information-security/securing-your-devices

REGISTER YOUR LAPTOP

www.bu.edu/police/crime-prevention/laptop-registration-with-stop

DUO TWO FACTOR-AUTHENTICATION

www.bu.edu/tech/support/duo

DATA LIFECYCLE MANAGEMENT POLICY

www.bu.edu/policies/data-lifecycle-management-policy

DATA ACCESS MANAGEMENT POLICY

www.bu.edu/policies/1-2-b-data-access-management-policy

HOW TO: SAFELY DISPOSE MEDIA

www.bu.edu/policies/record-retention

RECORD RETENTION POLICY

www.bu.edu/policies/record-retention

ACCESS TO ELECTRONIC INFORMATION POLICY

www.bu.edu/policies/electronic-information-access

DATA CLASSIFICATION POLICY

www.bu.edu/policies/data-classification-policy

MINIMUM SECURITY STANDARDS

www.bu.edu/policies/minimum-security-standards/123

BU INFORMATION SECURITY
CONTACT: buinfosec@bu.edu
VISIT: bu.edu/infosec