

Protecting Your Data

IS&T Technology Fair
October 10, 2018

Introduction and Agenda

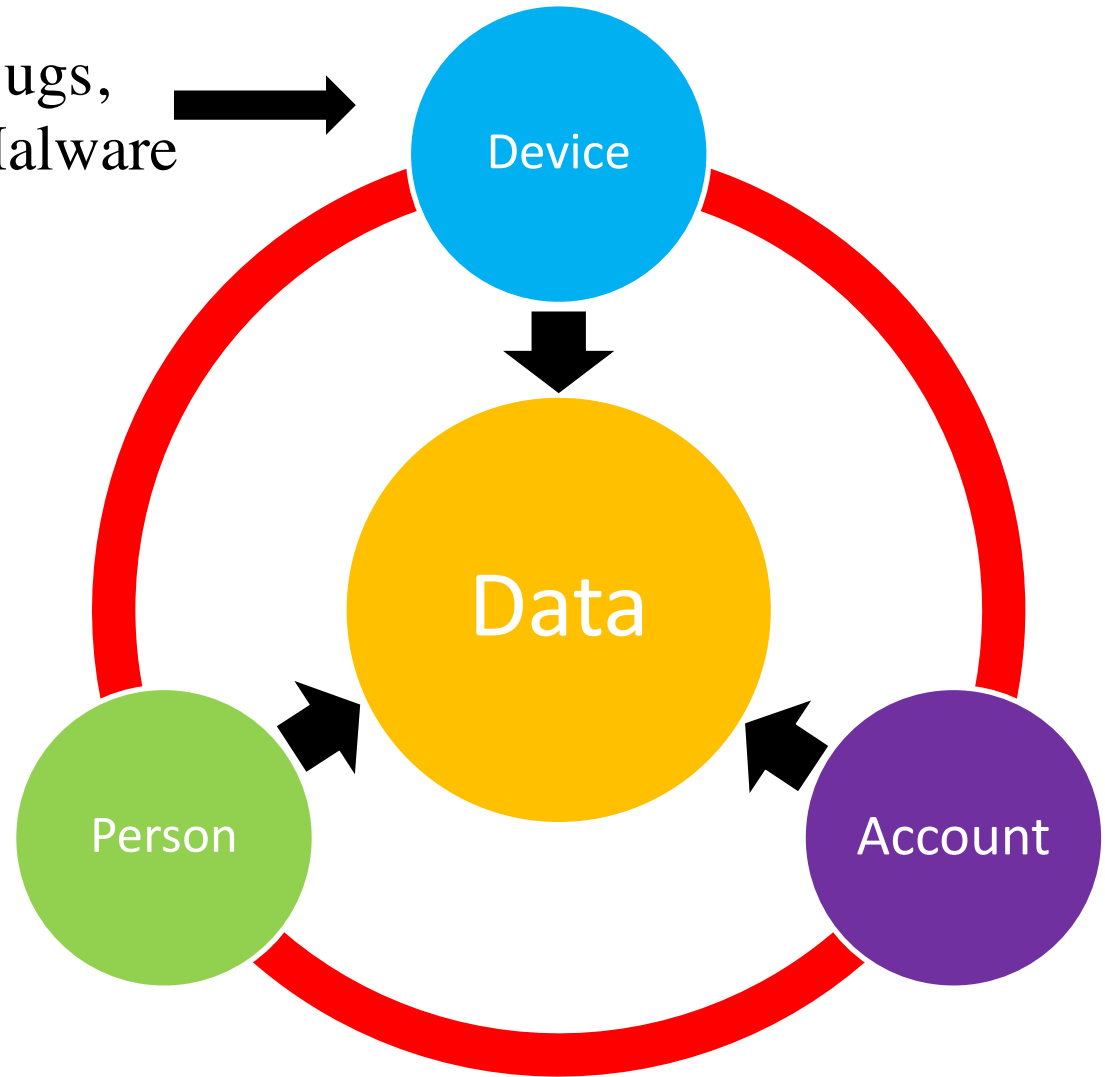


Eric Jacobsen
Director of Information Security
Boston University

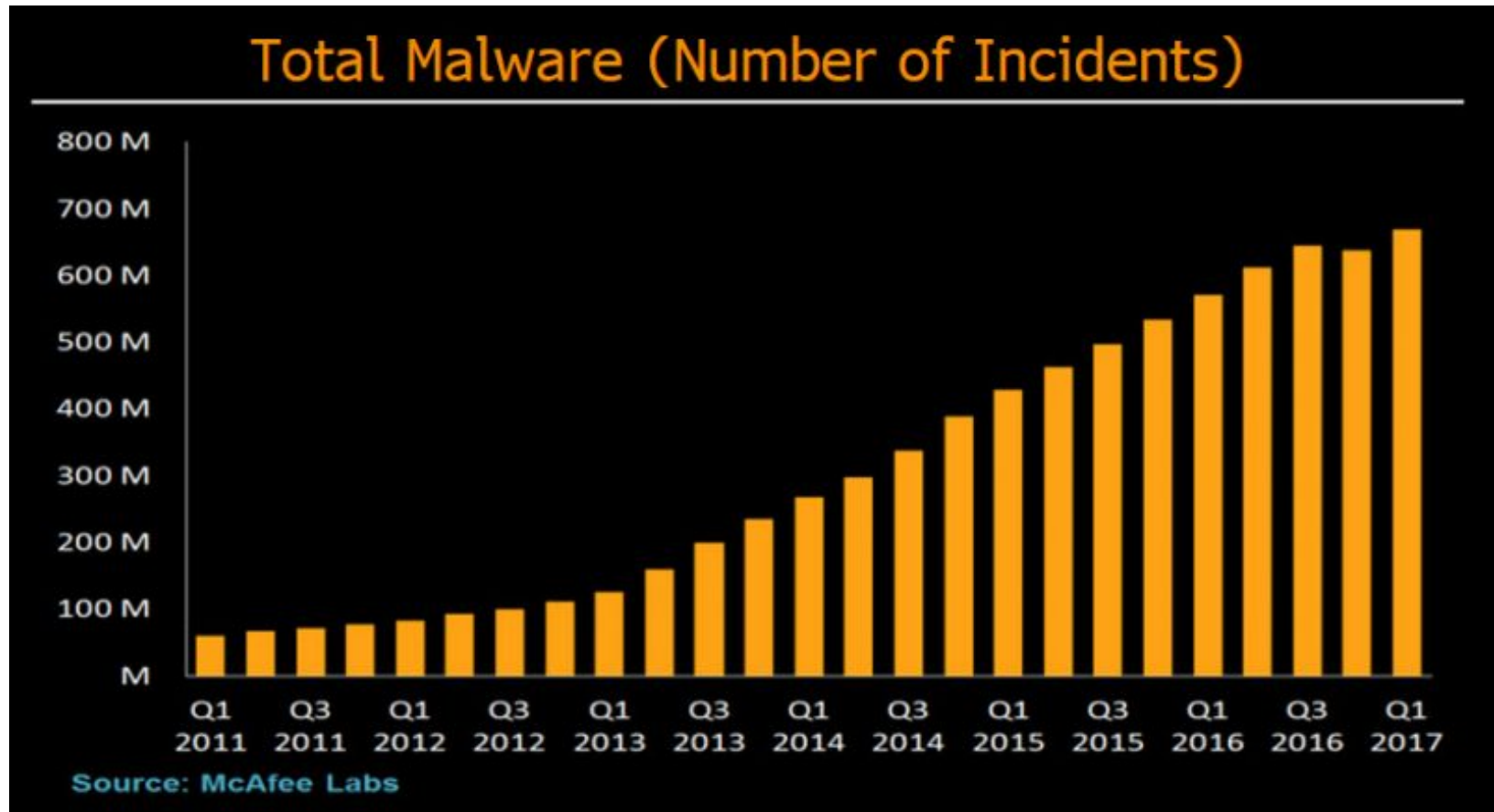
- What are the core challenges to protecting data in 2018?
- How do these risks show up at BU?
- What can you do to help?
- What is BU doing to protect you?



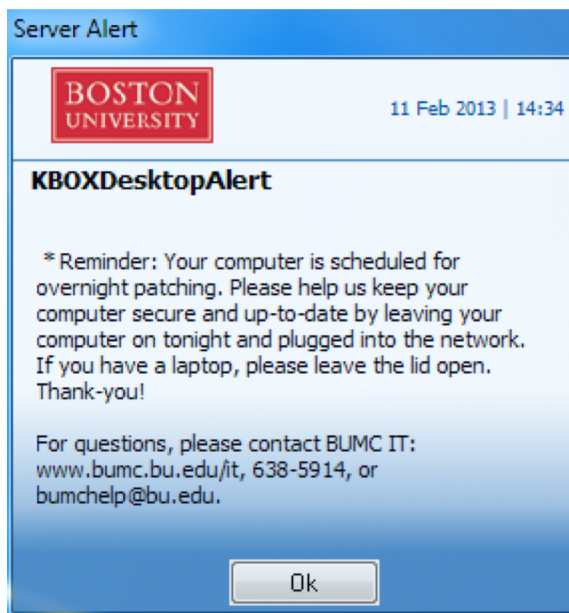
Attack Bugs,
Install Malware



Attacking the Device



How can you help with this?



How can you help with this?



How can you help with this?



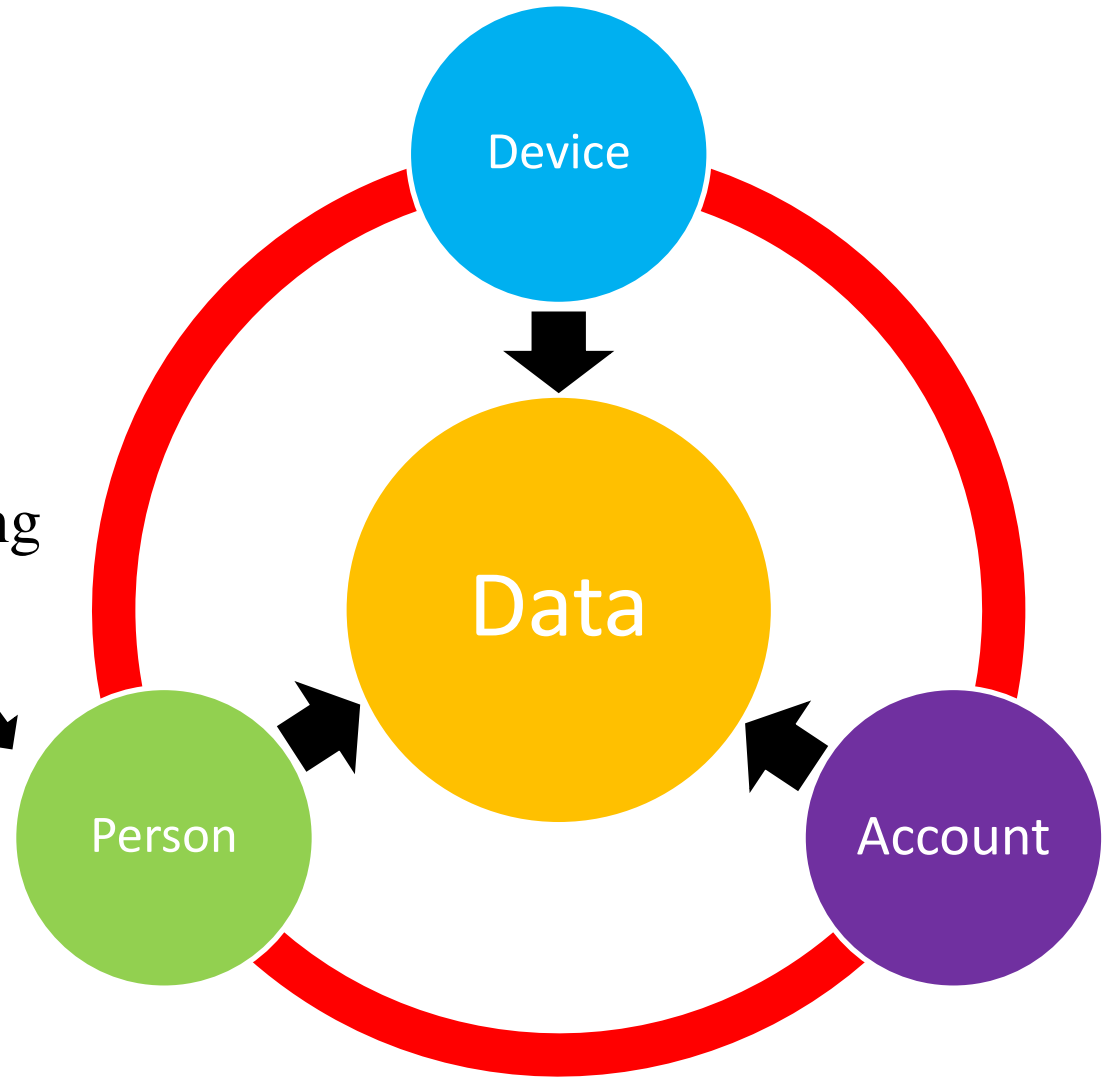
The image shows a Microsoft Internet Explorer browser window with a red background and white polka dots. The text "WINNER!" is displayed in large white letters. Below it, there is a "FREE!" starburst and an image of an iPod. The browser title bar reads "You've won a iPod - Microsoft Internet Explorer".

Overlaid on the browser is a blue window titled "AntivirusGT Resident Shield: Virus detected". The window contains the following information:

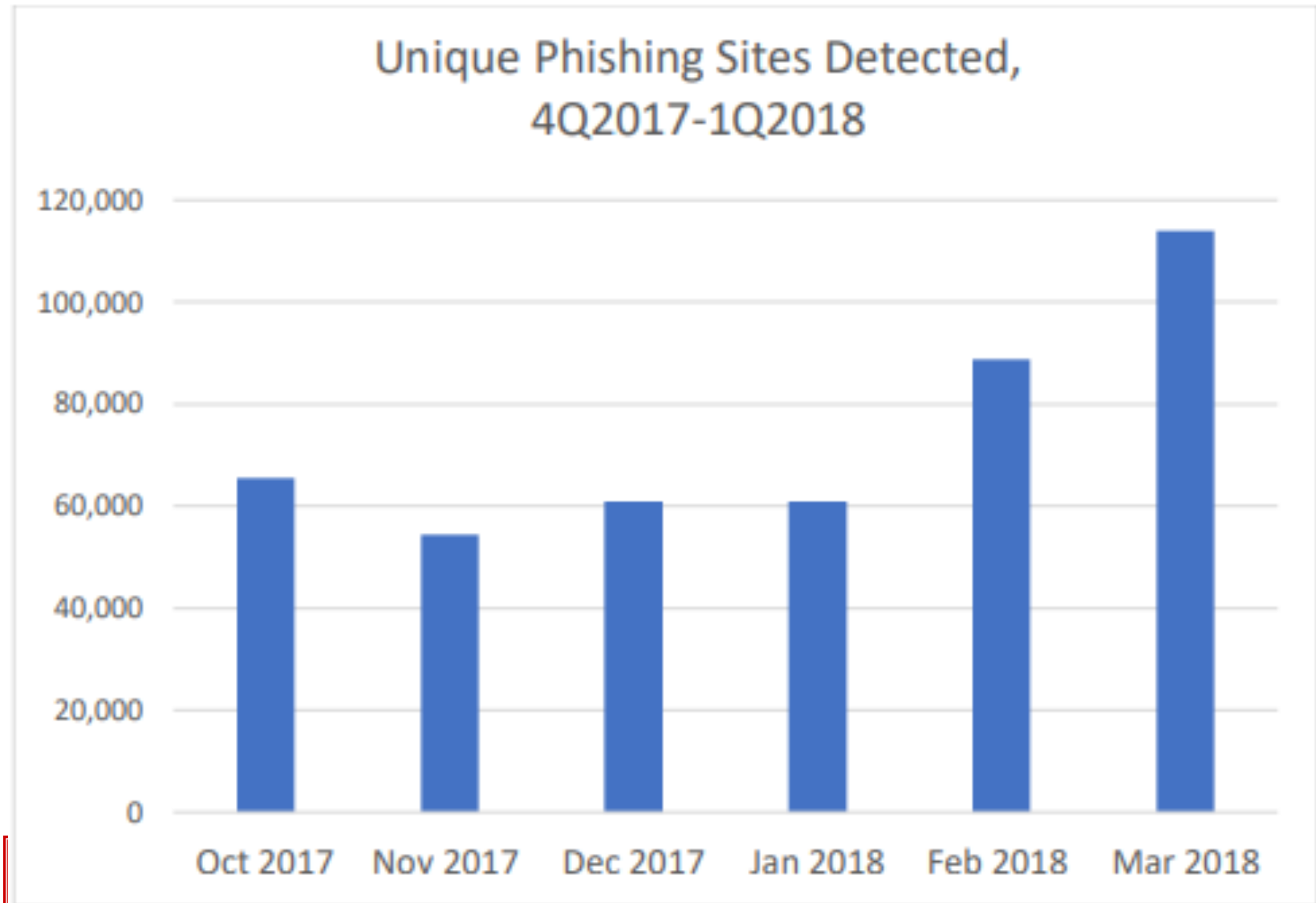
- Warning! Active virus detected**
- Threat detected: Trojan.Injector.BZ**
- Security risk:** A progress bar showing a high level of risk.
- Infected file:** C:\WINDOWS\system32\rundll32.exe
- Action taken:** Application blocked
- Description:** Trojan.Injector is a detestable Trojan infection that is highly capable of downloading dubious files and software onto a computer without the user ever knowing about it until their system is actually damaged. Trojan.Injector is particularly damaging to a computer system.
- Do not block this application again
- Recommended:** Please click "Remove All" button to heal all infected files and protect your PC
- Remove All** button



Go Phishing



Phishing for Accounts



Source: www.antiphishing.org.

What happens when you get phished?

- The intruder has access to everything in your e-mail
 - Everything you've received and often everything you've sent
 - This can trigger reporting requirements if it is protected data about others.
- The intruder may forward some or all of your e-mail to a different mailbox
- Your e-mail may be deleted
- Your e-mail account may be used to phish other people

Lose access to your other accounts

1ST *First National Bank*

Menu

Login

Forgot Online Banking Password

If you have already enrolled in Online Banking and were using it, but now you don't recall your password or somehow you are locked-out, then you **may** be able to RESET your password now. **Here's how!** You will need to know your last valid **User ID** and **email address**.



Loss Access to your BU Account

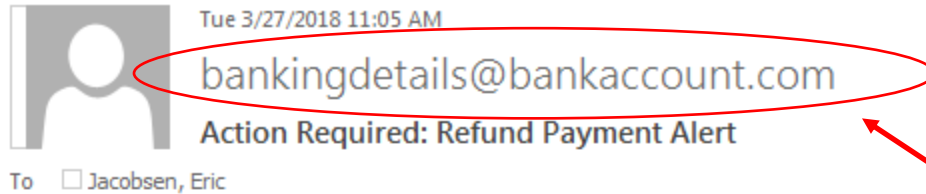
The screenshot shows the top navigation bar of the BU TechWeb site. On the left is the BU TechWeb logo. To its right is a search box labeled "Search this site" with a magnifying glass icon. Further right is a green "Get Help" button with a question mark icon. Below the search bar is a blue navigation bar with three items: "services" (with a gear icon), "support" (with a speech bubble icon), and "about" (with a person icon). Below the navigation bar is a breadcrumb trail: [services](#) > [information security](#) > [identity ... \(iam\)](#) > [authentication ...](#) > [kerberos authentication](#) > [bu login](#) > [reset locked account](#).

Reset Locked Account

- Login Names >
- Reset Password >
- Reset Locked Account >**

If you have [reset your BU Kerberos password](#), you will also need to change it wherever it has been saved. Mail clients and many other network tools will often recognize that they can no longer access the network and will prompt you to supply the new password. When this occurs, you provide the new password and should then be able to connect without any issues.

However, there might be occasions when you are not prompted and, perhaps without even knowing it, make multiple



What's wrong here?

1. Generic Sender
2. Link URL: microransom.us
3. False urgency

Action Required: Refund Payment Alert

We double charged your card for your last posted payment, a refund process was initiated but could not be completed due to errors in your mailing information.

As part of these new procedures we will be implementing our two step authentication feature which will prevent unauthorised access to your account.

In order for us to carry out the refund successfully, we require you to validate your account information.

Log on to [your bank account profile](#) to begin the process.

Please note: Failure to comply with this request can lead to temporary suspension of access to our online banking service.

Sincerely,
Account Support

What is BU doing?

 Information Services & Technology

Malicious Web Page Blocked



The web page you were trying to visit has been known to cause harm, and may try to install [dangerous software](#) on your computer that can steal or delete your information. Please contact us at ithelp@bu.edu or call (617) 353-4357 if you believe this to be in error and include the information below in your message.

User:

URL:

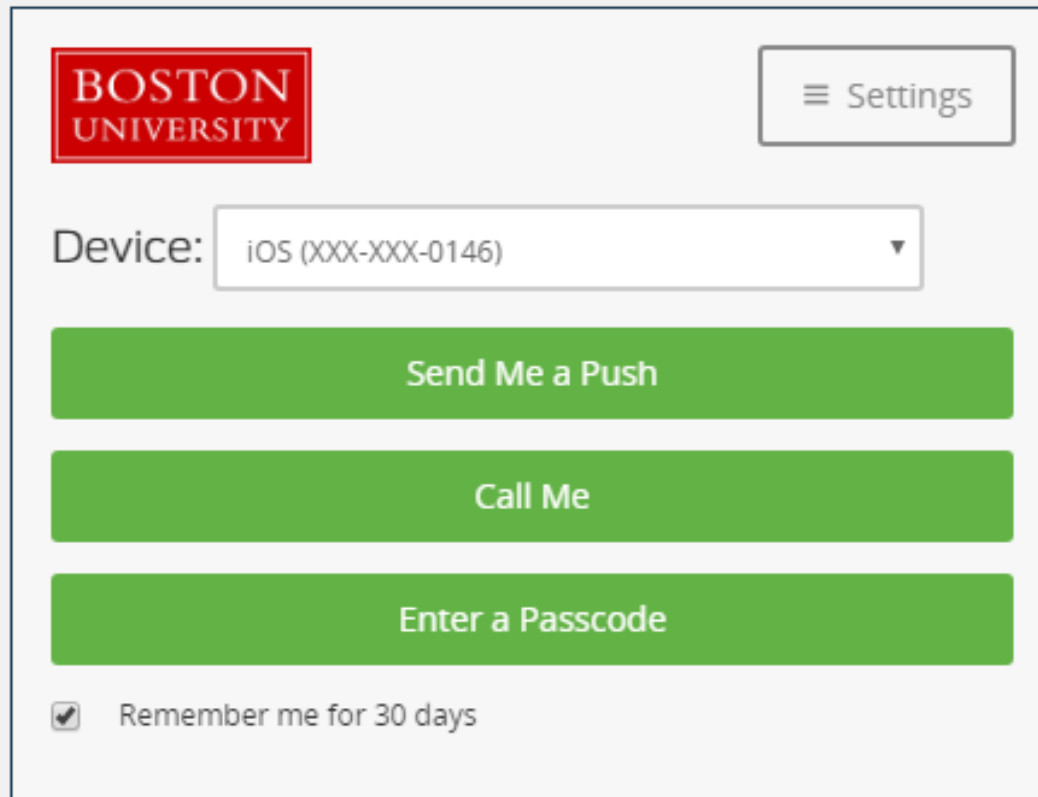
Category:

[Return to previous page](#)

What is BU doing?

Two-Step Login Started

Boston University uses software from Duo to protect your information. Please follow the steps below to complete the login process.



BOSTON UNIVERSITY Settings

Device: iOS (XXX-XXX-0146) ▼

Send Me a Push

Call Me

Enter a Passcode

Remember me for 30 days

Coming soon...



[Data Sheet](#)

Cisco Email Security Advanced Email Protection

Product overview

Customers of all sizes face the same daunting challenge: email is simultaneously the most important business communication tool and the leading attack vector for security breaches. Cisco® Email Security enables users to communicate securely and helps organizations combat Business Email Compromise (BEC), ransomware, advanced malware, phishing, spam, and data loss with a multilayered approach to security.



Not expecting to see that logo?

Boston University Information Security, in coordination with your unit's management, is conducting an assessment to determine our vulnerability to phishing e-mails and our training needs. Please help us to obtain an accurate assessment by not discussing the e-mail that brought you here with your coworkers until the test completes on December 15, 2017.

While your participation in this exercise will help us understand how vulnerable our test communities are to phishing, the results will not be used for disciplinary action. Information Security will report only on the percentages of individuals that clicked on the message, not individual names.

If something bad does happen...

BU Information Security
(Cyber) Incident Response Team

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

We're here to help!

Questions

