Information Security Awareness Program

This document is part of a collection of documents that make up the Information Security Awareness Program. The following is a link to the main Information Security Awareness Program document.

E-mail Security

E-mail is a vital part of daily business and is an official communication vehicle of the College. Although there are significant safeguards to protect us (firewalls, anti-virus, spam filter, etc.), there are still great risks associated with e-mail. We will review a few of them in information security awareness. Read How Outlook helps protect you from viruses, spam, and phishing for more information on this topic.

Spam E-mail

Wikipedia defines spam as *"… the use of electronic messaging systems to send unsolicited bulk messages indiscriminately"*. Over 90% of all e-mail messages received in the U.S. is spam. That number holds true for Cincinnati State as well. Although our firewall and spam filtering devices do keep more than 90% of spam from making it to your inbox, some still get through. You can use the Rules and Alerts feature of Outlook to help automatically move specific types of e-mails to different folders. The feature can delete the emails altogether as well.

Spam is a nuisance and is best ignored. Replying alerts spammers that the e-mail address is valid and the amount of spam will significantly increase. Don't let spam deceive you. It can include serious security threats and we'll talk about these threads next. For more information, read the article The Dangerous Side of Spam from PC World.

If you suspect an e-mail is spam, don't open it. Call the ITS Helpdesk at (513) 569-1234.

Receiving E-mail Attachments

E-mail is a major security risk and a great deal of this risk revolves around e-mail attachments. Although anti-virus software is a strong defense against attachments that contain malware, you should use caution anytime you open an attachment. Never open an attachment if you don't know the sender. If you suspect an e-mail you received may contain a dangerous attachment do not open it. Call the ITS Helpdesk at (513) 569-1234. For more information on malware, see the Information Security Awareness document Staying Safe & Secure Online.

Sending E-mail Attachments

Keep in mind that you can forward an e-mail that contains a virus to another recipient. If you suspect a file may contain a virus, do not open, forward, or reply to the email. Call the ITS Helpdesk at (513) 569-1234.

Another information security concern with e-mail attachments is the data contained within the attachment. Systems often generate output that can be saved as Microsoft Office files (Excel or Word), text files (csv, xml, or plain text), PDF files (Portable Document Format), and many others. Information security comes into play when these files contain sensitive data. The systems that house sensitive data typically have some type of security that protects the data from inappropriate access. The security is removed when data is exported from these systems into stand-alone files. You should be aware of the type of data contained in attachments you send through email.

Never attach files containing sensitive data to an e-mail without taking proper security precautions. If you are unsure of the sensitivity of the data you are sending in an e-mail, call the ITS Helpdesk at (513) 569-1234.

Phishing

Google defines phishing as "… *a type of online fraud where someone tries to trick the victim into revealing sensitive details such as a username, password or credit card details, by masquerading as a trustworthy entity in an electronic communication*." These scams are typically financially motivated. Google continues by saying "*A phishing website or message tries to trick you into revealing personal information by appearing to be from a legitimate source, such as a bank, social network*…" or even as Cincinnati State. Often an e-mail phishing attempt may have a link to a website that asks for highly-securable information such as:

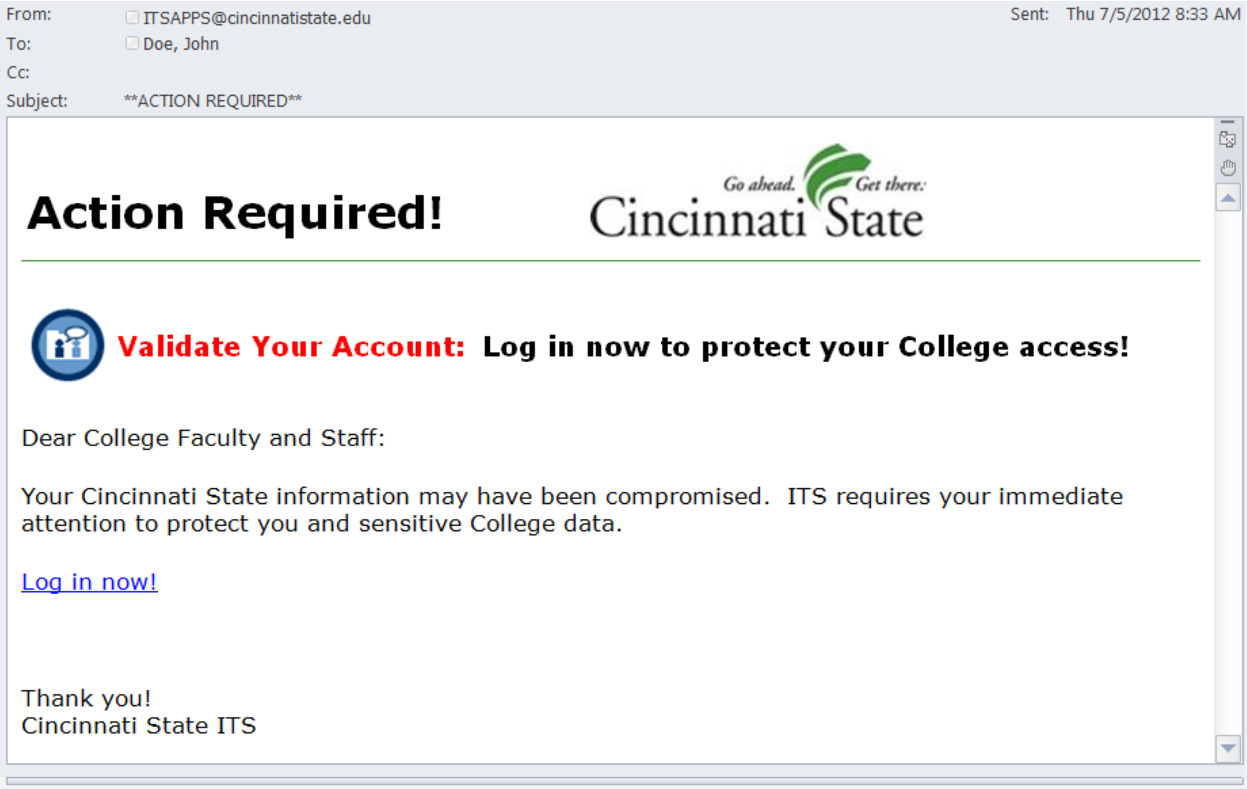
CAUTION

Never disclose your sensitive data until you verify the authenticity of the receiver.

- Usernames and passwords
- Social Security numbers
- Bank account numbers
- PINs (Personal Identification Numbers)
- Full credit card numbers
- Your mother's maiden name
- Your birthdate

Cincinnati State will never ask for sensitive data via e-mail. For more information on this, see the Information Security Awareness document Username and Password Security. If you suspect an e-mail or website is phishing for your information, call the ITS Helpdesk at (513) 569-1234.

The following is an example of an e-mail phishing attempt trying to get your Cincinnati State username and password. These e-mails can look very authentic. There are several warning signs that will help detect a phishing attempt.



From: ITSAPPS@cincinnatistate.edu
To: Doe, John
Cc:
Subject: **ACTION REQUIRED**
Sent: Thu 7/5/2012 8:33 AM

Action Required!

Validate Your Account: Log in now to protect your College access!

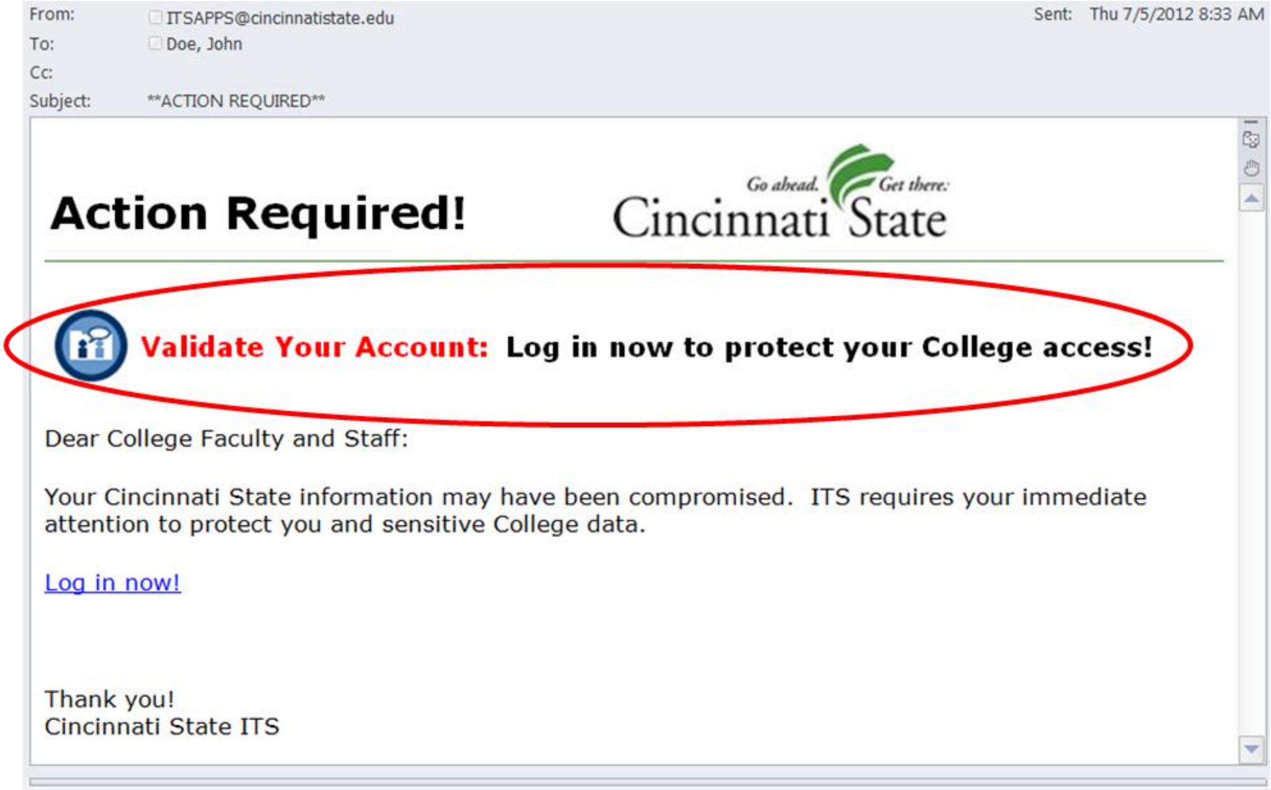
Dear College Faculty and Staff:

Your Cincinnati State information may have been compromised. ITS requires your immediate attention to protect you and sensitive College data.

Log in now!

Thank you!
Cincinnati State ITS

Phishing Warning Sign 1: The message encourages you to enter confidential information.



From: ITSAPPS@cincinnatistate.edu
To: Doe, John
Cc:
Subject: **ACTION REQUIRED**
Sent: Thu 7/5/2012 8:33 AM

Action Required!

Validate Your Account: Log in now to protect your College access!

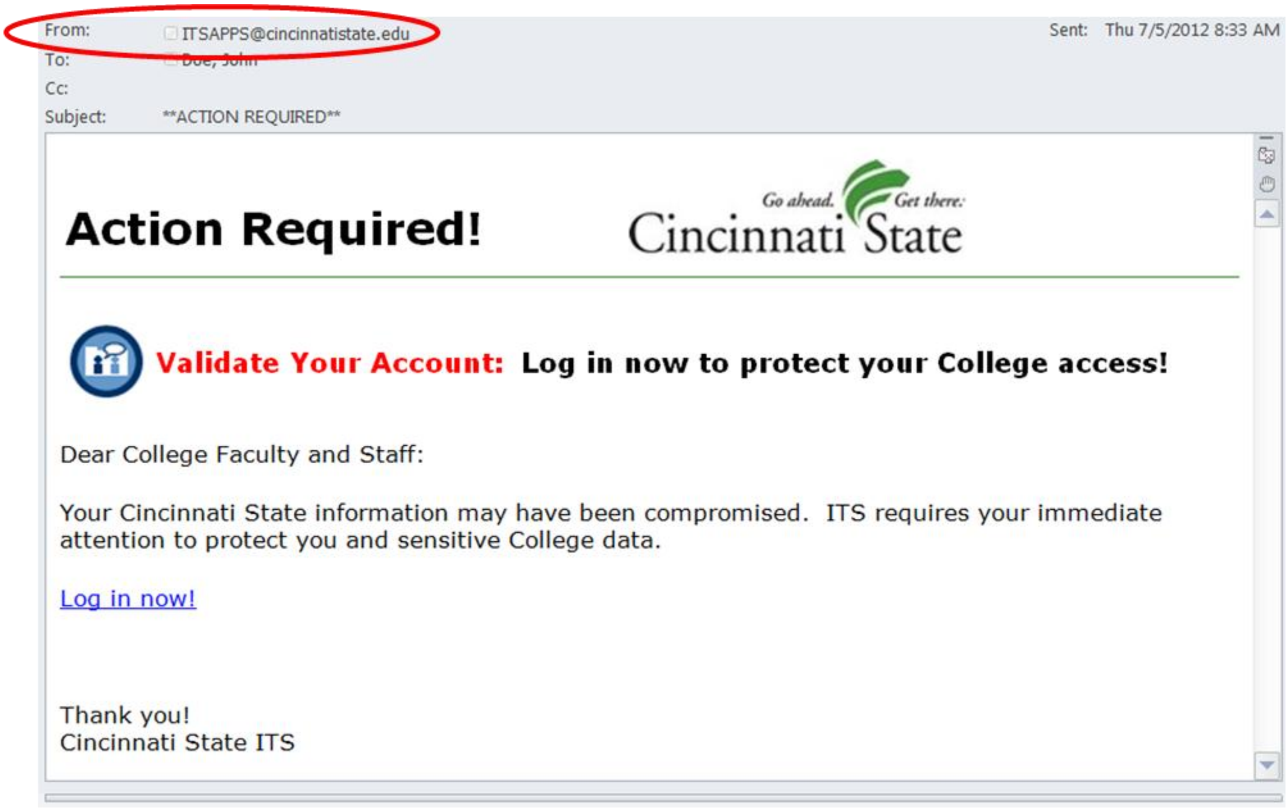
Dear College Faculty and Staff:

Your Cincinnati State information may have been compromised. ITS requires your immediate attention to protect you and sensitive College data.

Log in now!

Thank you!
Cincinnati State ITS

Phishing Warning Sign 2: The “From” address appears to be authentic. It is easy to forge a “From” address.



From: ITSAPPS@cincinnatistate.edu
To: Doe, John
Cc:
Subject: **ACTION REQUIRED**
Sent: Thu 7/5/2012 8:33 AM

Action Required!

Validate Your Account: Log in now to protect your College access!

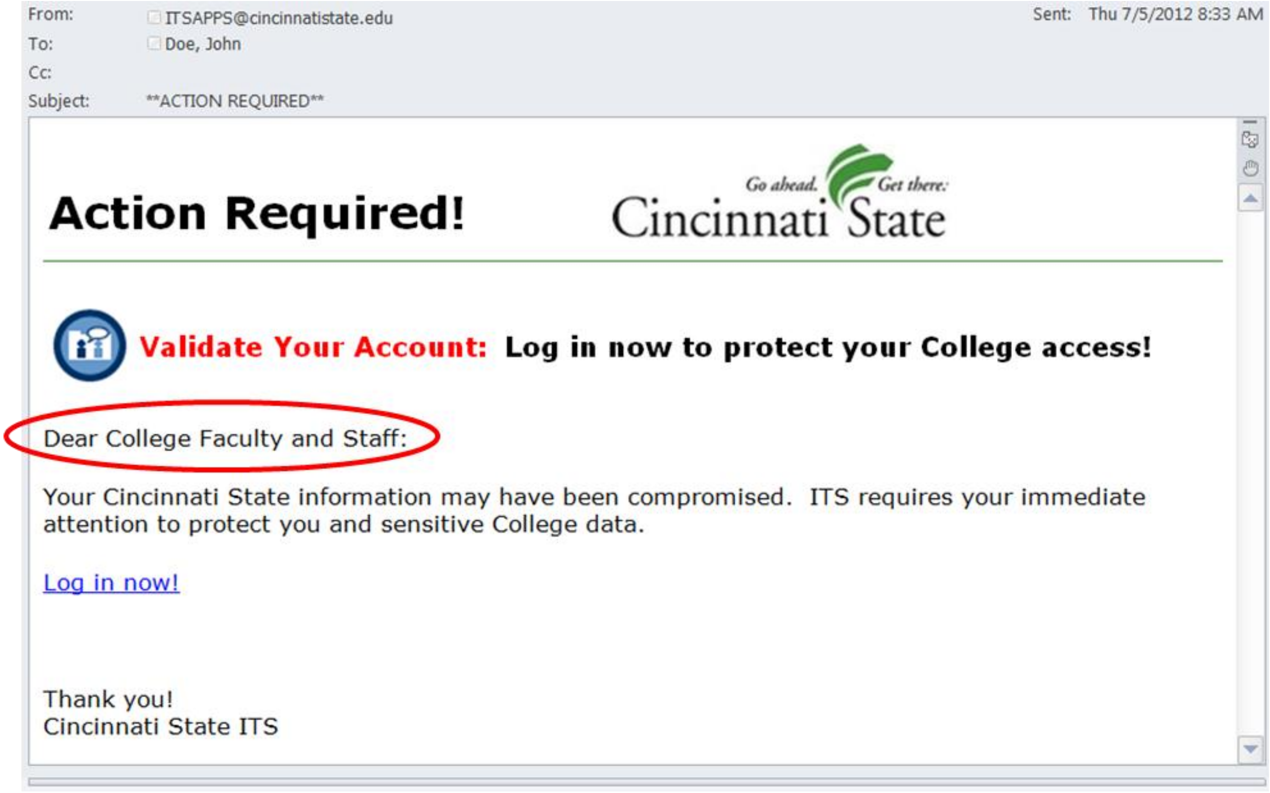
Dear College Faculty and Staff:

Your Cincinnati State information may have been compromised. ITS requires your immediate attention to protect you and sensitive College data.

Log in now!

Thank you!
Cincinnati State ITS

Phishing Warning Sign 3: Often the message will begin with a general greeting such as “Dear Cincinnati State user” or “Dear valued customer” rather than being personally addressed to you.



From: ITSAPPS@cincinnatistate.edu
To: Doe, John
Cc:
Subject: **ACTION REQUIRED**
Sent: Thu 7/5/2012 8:33 AM

Action Required!

Validate Your Account: Log in now to protect your College access!

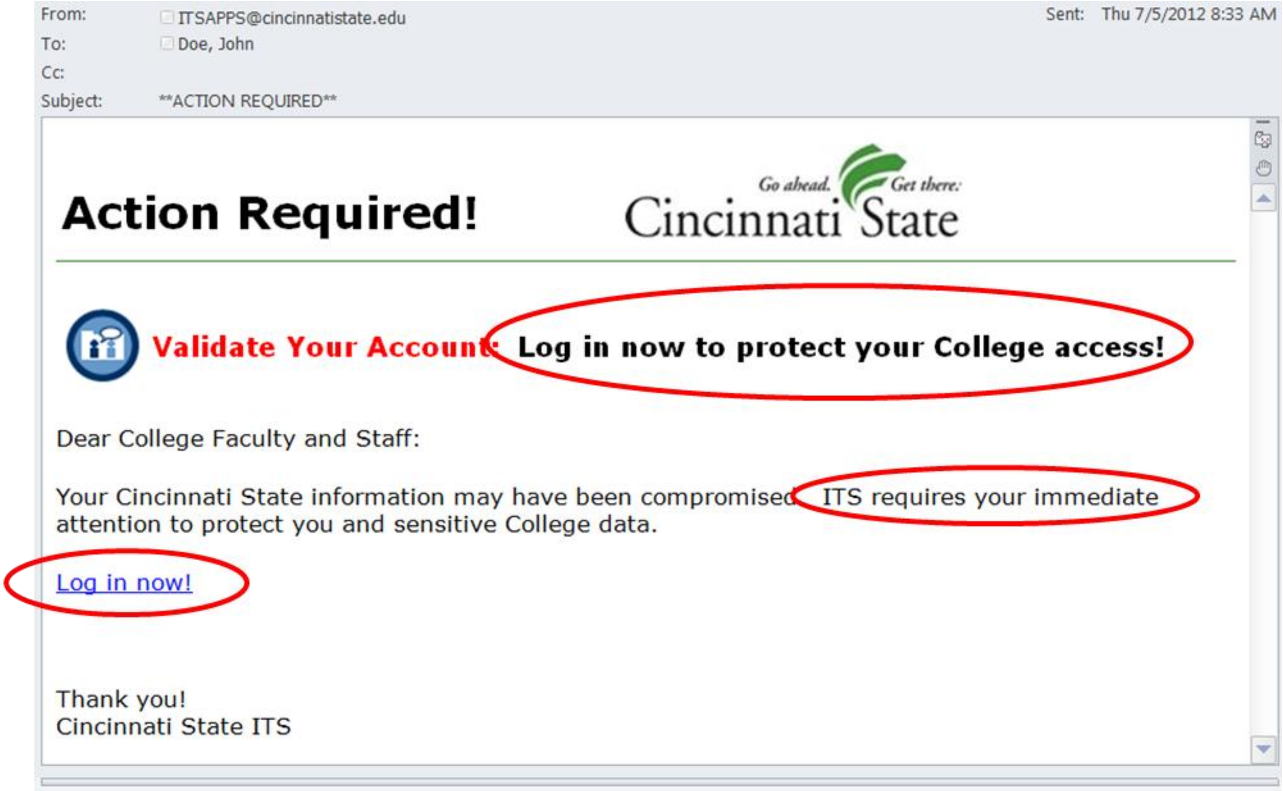
Dear College Faculty and Staff:

Your Cincinnati State information may have been compromised. ITS requires your immediate attention to protect you and sensitive College data.

Log in now!

Thank you!
Cincinnati State ITS

Phishing Warning Sign 4: These attempts often use scare tactics or the message has a sense of urgency.



From: ITSAPPS@cincinnatistate.edu

To: Doe, John

Cc:

Subject: **ACTION REQUIRED**

Sent: Thu 7/5/2012 8:33 AM

Action Required!

Validate Your Account: Log in now to protect your College access!

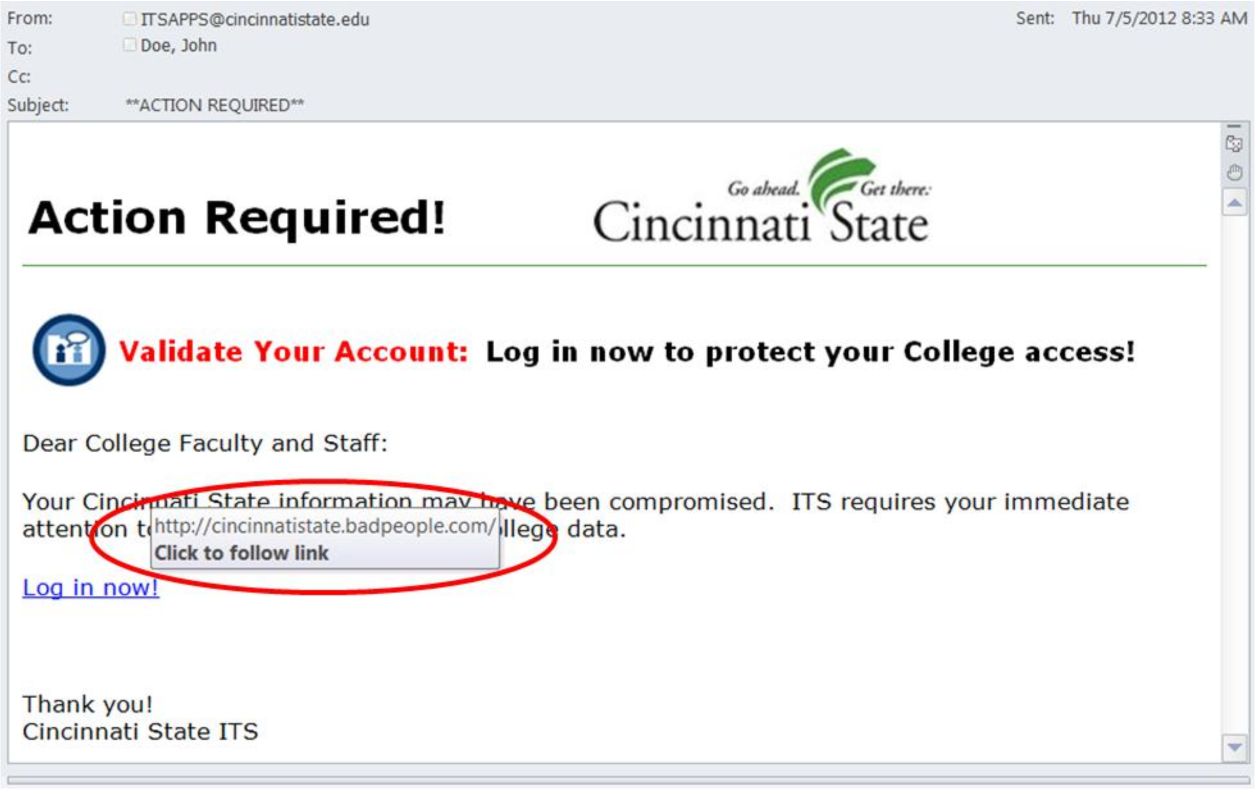
Dear College Faculty and Staff:

Your Cincinnati State information may have been compromised. ITS requires your immediate attention to protect you and sensitive College data.

Log in now!

Thank you!
Cincinnati State ITS

Phishing Warning Sign 5: Although the link may look safe, you can't always determine the website it will use by simply reading the link. If you hover your mouse pointer over the link, making sure you don't click the link, Outlook will show you a small pop-up of the website. To entice you more, this example has "cincinnatistate" as a component of the website. Once you click the link, the page displayed may look exactly like a Cincinnati State login page. If you enter your username and password, they have you! Never click a link in an e-mail if you are unsure of the sender, especially if it is asking for highly securable information.



From: ITSAPPS@cincinnatistate.edu
To: Doe, John
Cc:
Subject: **ACTION REQUIRED**
Sent: Thu 7/5/2012 8:33 AM

Action Required!

Validate Your Account: Log in now to protect your College access!

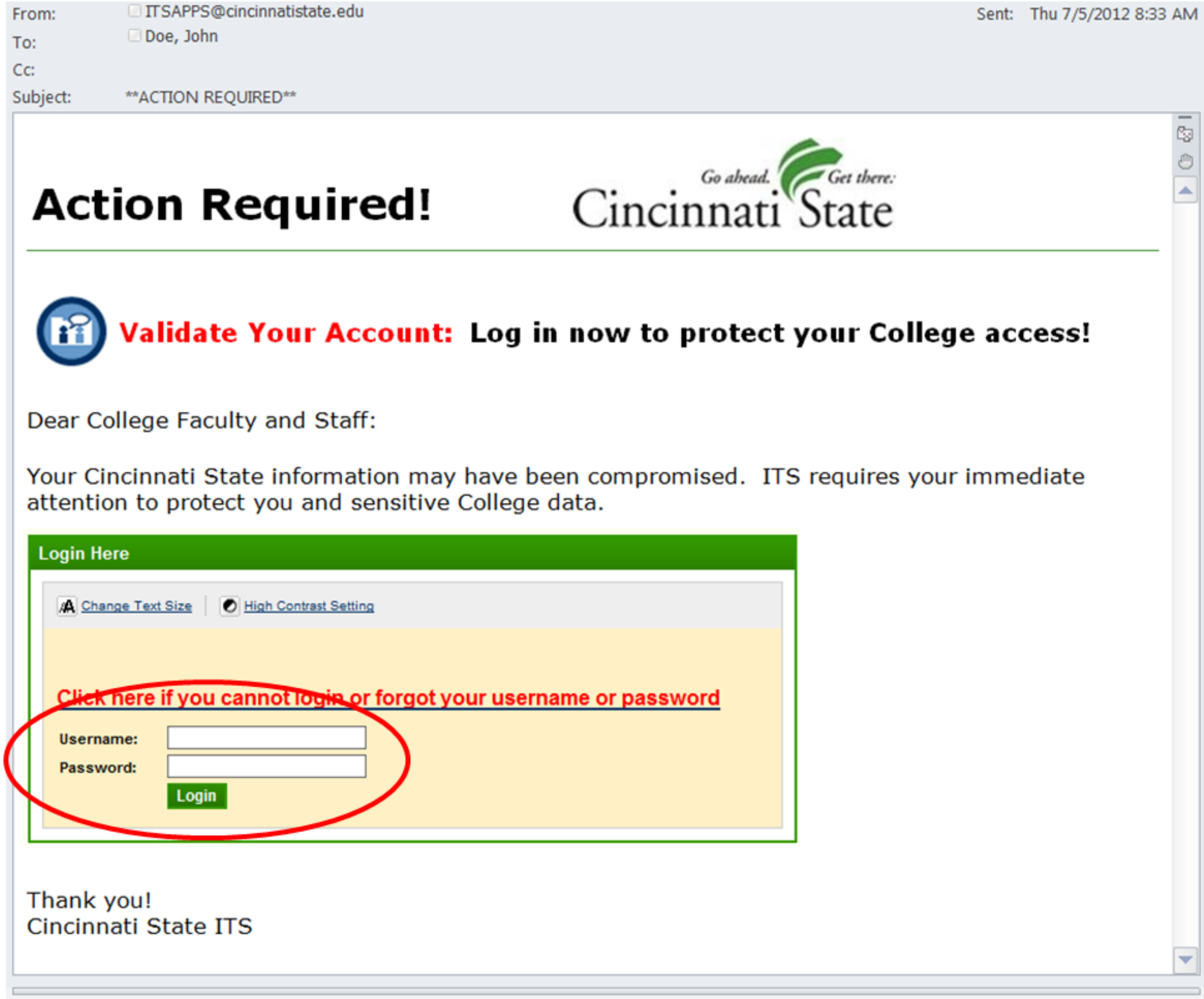
Dear College Faculty and Staff:

Your Cincinnati State information may have been compromised. ITS requires your immediate attention to College data.

Log in now!

Thank you!
Cincinnati State ITS

Phishing Warning Sign 6: Phishing attempts also request sensitive information to be entered within the body of an e-mail. Never enter information or click a link in an e-mail if you are unsure of the sender, especially if it is asking for highly securable information.



From: ITSAPPS@cincinnatistate.edu

To: Doe, John

Cc:

Subject: **ACTION REQUIRED**

Sent: Thu 7/5/2012 8:33 AM

Action Required!

Validate Your Account: Log in now to protect your College access!

Dear College Faculty and Staff:

Your Cincinnati State information may have been compromised. ITS requires your immediate attention to protect you and sensitive College data.

Login Here

Click here if you cannot login or forgot your username or password

Username:

Password:

Thank you!
Cincinnati State ITS

Another important tactic to combat phishing and other fraudulent activity is to inspect the website displayed in your browser. For more information, see the Information Security Awareness document on Sensitive Data.

Additional Resources

eBay's Tutorial: *Phishing*
http://pics.ebaystatic.com/aw/pics/securityCenter/tutorial/Spoof/player.html

Microsoft's Safety & Security Center: *Phishing FAQ's*
http://www.microsoft.com/security/online-privacy/phishing-faq.aspx

Google's Stay Safe Online: *Phishing*
http://www.google.com/goodtoknow/online-safety/phishing