Phishing emails appearing to come from Blackboard

Issue Overview

Phishing scams use fraudulent emails to get users to reveal confidential information. Such emails usually look like they come from a legitimate organization such as Blackboard but contain links to illegitimate sites.

Blackboard has become aware of a mass phishing scam targeting customers using Blackboard Learn. To be clear, Blackboard Learn has not been hacked -- these are emails sent directly from a spammer to emails it may have harvested by spidering the institution's websites for email addresses.

Examples of Phishing Attempts

It is important to realize that the messages will vary.

EXAMPLE 1: "RECEIVED NEW MAIL"

<table>
<thead>
<tr>
<th>Purported Sender</th>
<th>Blackboard ITS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Email Subject</td>
<td>Received New Mail[School Board]</td>
</tr>
</tbody>
</table>
| Content          | From: Blackboard ITS [mailto:its@blackboard.com]  
Sent: Monday, June 22, 2015 12:16 PM  
To:  
Subject: Received New Mail[School Board]  

Dear blackboard user:

You have 2 unread messages from your Admin stored in your Blackboard area.  
Please login below to view messages. Ker1745758767676  
The above link will become inactive 10 minutes after mail has been read.  
Thanks for your attention  
Regards,  
Blackboard ITS |

EXAMPLE 2: "NEW COURSE INFORMATION"

<table>
<thead>
<tr>
<th>Purported Sender</th>
<th>Blackboard Learn <a href="mailto:notifications@blackboard.com">notifications@blackboard.com</a></th>
</tr>
</thead>
<tbody>
<tr>
<td>Email Subject</td>
<td>New Course Information</td>
</tr>
</tbody>
</table>
| Content          | Good Morning,  
An important course form has been posted to you through the Blackboard Learning System.  
Please sign in immediately to view the form.  
Click here to sign in <--Link to malicious website  
Thank you,  
Blackboard Learn. |
### EXAMPLE 3: "BLACKBOARD LEARN: IMPORTANT NEW COURSE"

<table>
<thead>
<tr>
<th>Purposed Sender</th>
<th>Blackboard Learn <a href="mailto:email@blackboard.com">email@blackboard.com</a></th>
</tr>
</thead>
<tbody>
<tr>
<td>Email Subject</td>
<td>Blackboard Learn : Important new course</td>
</tr>
</tbody>
</table>
| Content               | Dear Staffs/Students  
Access to e-mail is about to expire,  
We recommend that you upgrade your account to avoid the suspension.  
Please click on the link below to re-activate your account, please sign in to Blackboard system immediately.  
Click here to sign in to the Blackboard System <--Link to malicious website  
Thank You.  
© 2013 Blackboard | Technology and Solutions Inc. All Rights Reserved. |

### EXAMPLE 4: "NOTICE: IMPORTANT NEW COURSES ALERT."

<table>
<thead>
<tr>
<th>Purposed Sender</th>
<th>Blackboard Learn <a href="mailto:email@blackboard.com">email@blackboard.com</a></th>
</tr>
</thead>
<tbody>
<tr>
<td>Email Subject</td>
<td>Blackboard Learn : Important new course</td>
</tr>
</tbody>
</table>
| Content               | Dear Member  
Access to e-mail is about to expire,  
We recommend that you upgrade your account to avoid the suspension.  
Please click on the link below to re-activate your account, please sign in to Blackboard system immediately.  
Click here to sign in to the Blackboard System <--Link to malicious website  
Thank You.  
© 2013 Blackboard | Technology and Solutions Inc. All Rights Reserved. |

### Solution
- Notify your end users that these emails are phishing emails and to delete and disregard the emails.
- Do NOT go to the link in the email. Delete the email immediately.
- Please continue to send questionable messages to spam@jhu.edu. For immediate response, please call the Help Desk (410-516-HELP).

### More Information
- [http://www.it.johnshopkins.edu/security/phishing.html](http://www.it.johnshopkins.edu/security/phishing.html)