HWS Information Technology Services Bulletin

Number: 2014-39
Date: September 15, 2014
Title: Security Alert - Phishing email

Description:

IT Services has detected a phishing message that is being sent to many HWS email accounts. Already, a number of users have fallen victim to this phishing attempt. The phishing attempt is characterized by the attacker masquerading as members of the HWS community and tricks users into providing their HWS credentials. Once the credentials have been compromised, the user’s email account is hijacked and used to generate thousands of spam email messages. Below is a representative example of the text in the phishing email. Please keep in mind that you may see several different variants based on this same theme.

From: Fake HWS User
Date: September 15, 2014 at 11:26:53 AM EDT
To: Undisclosed recipients:;
Subject: Hobart and William Smith Colleges WebMail Alerts

Dear User,

Your account has exceeded its megabyte limit and needs to be verified. Verify within 24 hours, to avoid account suspension.

Click Here to verify your email account

Thank you for helping us protect you.

© 2014 Hobart and William Smith Colleges.

While many of these types of messages are filtered out before they ever reach a user’s inbox, some of these messages do get through. Therefore, it is important to remember that IT Services will NEVER ask you for this information via an email, or ask you to visit a webpage to confirm your identity. If you ever feel your password may have been compromised contact the Help Desk or reset your password at http://password.hws.edu.

Contact: Current information about this bulletin may be found at http://web.hws.edu/administration/itservices/alerts.asp. If you have any questions or concerns, please contact IT Services at helpdesk@hws.edu or call 315-781-HELP.
Type:

Unscheduled

Category:
  Alert

Distribution:
  HWS Network Accounts
Type:
Unscheduled

Category:
Alert

Distribution:
HWS Network Accounts