Security Alert - Phishing email

IT Services has detected a phishing message that is being sent to many HWS email accounts. Over the past several days, a number of users have fallen victim to this phishing attempt. The phishing attempt is characterized by the attacker masquerading as a representative from IT Services 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.

Ref: 52/019/IT3x
Due to the recent Virus attack on our database, We are currently upgrading our database and all email accounts need to be verified. IT Helpdesk will be upgrading to the latest anti-spam version. You are required to CLICK: “LINK REMOVED”

Login with your correct Webmail information and wait for responds from our database service. We apologize for any inconvenience and do appreciate your understanding. Failure to confirm and verify your email account on our database as instructed, Your e-mail account will be blocked in 24 hours.

Thank you for your cooperation
©2013 System Administrator.

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