Phishing Scam Regarding Salary
There is a new phishing email that is circulating to the George Mason University community. Because it purports to be from HR, we wanted to get the word out that this is a phishing incident. This email did not come from Mason HR & Payroll. If you get this message, DO NOT reply, DO NOT click any links, and DO NOT provide any personal information. Instead, simply delete the email.

Please share this message with your faculty and staff.

ITS has posted this incident on their IT security website under alerts: http://itsecurity.gmu.edu/Alerts/Advisories.cfm. Phishing incidents are quite frequent with a new one being posted almost daily.

· **What does the email message look like?**

  From: GMU HR [*link removed*]  
  Sent: Wednesday, April 22, 2015 9:38 AM  
  To: ....  
  Subject: Salary Increment Notice

  [GMU LOGO JPEG FILE]

  Hello,

  The 2014 salary structure was recently reviewed ....

· **Please be aware....**

  Messages of this type are malicious phishing* attacks. Do not respond. If you have responded contact the ITS Support Center at 703-993-8870 or via email at support@gmu.edu.

  *Phishing is a term used by hackers who imitate legitimate companies and organizations in emails to entice users to share passwords, Social Security numbers, credit card or bank account numbers.

  The Federal Trade Commission warns that victims of phishing can become victims of identity theft and offers tips on how to avoid it at www.ftc.gov/bcp/edu/microsites/idtheft/index.html.

  How you can recognize a Phishing email: www.ncsu.edu/cc/essentials/antivirus_security/phishing/recognize.html.