THE
UNIVERSITY
OF RHODE ISLAND

This message is sent on behalf of Public Safety Director Stephen Baker.

July 17, 2014

We want to alert the community about some recent cyber-related scams victimizing university employees nationwide:

▪ In one scam, employees receive an email stating that: "The University is having a salary increment program again this year with an average of 2.5%. The Human Resources department evaluated you for a raise on your next paycheck. Click below to confirm and access your salary revision documents..."
Once there, the victims are asked for their bank account numbers to bypass a “fix” that payroll put in place to keep employee records safe.
▪ In another scam, criminals are filing fraudulent tax returns using stolen Social Security numbers and collecting tax refunds. When employees file their tax returns, they learn false tax returns have already been filed and that the IRS has sent their tax refunds to fraudulent filers.

If you encounter these or any other phishing emails, DO NOT RESPOND.

All users are urged to be cautious of any email asking for a university email address, user name, password, full name, date of birth and any other personal information. Some of these emails may appear to come from URI, but they do not. **Regardless** of what the sender address is listed as, the University will never ask you to provide any of this information through email.

Any victim who has received or responded to such emails can report cyber crime to the FBI at www.ic3.gov.

Download the Internet Crime Complaint Center's public service announcement (from URI's website) about these recent scams.