Dear Security Liaisons,

One of the easiest ways hackers gain access to computer systems and steal information is through phishing.

Like many other institutions, George Mason University has experienced an increase in phishing attempts. The most common phishing attempt is through an unsolicited email with a link to a site requesting information such as your username and password. With your credentials, a hacker will try to gain access to Mason’s computer systems to find and steal information.

Please make sure you evaluate emails to determine if they are legitimate before responding.

Most phishing emails have misspelled words, words used incorrectly, awkward wording and incorrect spacing. Also, a phishing email usually comes from a stranger, but it can look like it is from a person you know or a department at Mason. It is usually unsolicited, general, sounds urgent and can even be threatening.

Do not click on the link in such emails. If you hover over the link, you will find it does not go to the site it claims to go to. Forward the email to the ITS Support Center at support@gmu.edu before you delete it. The Support Center will have an alert issued about the attempt to warn others.

If you click on a phishing link, contact the Support Center by email or by phone at 3-8870. The Support Center will help you with taking corrective action, including changing your password.

Mason’s best defense against these attacks is its alert employees. Please be vigilant and careful about the links you click on and the information you provide. Keeping the Internet safe and secure at Mason is a job for each of us.

Please keep your department informed and aware. We need your help in getting these messages out to staff.