Email Security: Preventing Phishing

This week, a large number of faculty and staff email addresses received fake emails from the “helpdesk." Cybercriminals use email and fake websites in an attempt to steal your MasonID and password. This is called phishing. Once criminals phish credentials, they will use them in an attempt to exploit Mason’s computer networks, your Mason email, and your personal information.

If you clicked on the link in the phishing email and then provided your username and password you must **immediately**:

1 Change your password at password.gmu.edu.

2 Contact the Support Center at 703-993-8870 to report that you provided information.

If you provided your username and password, but fail to notify the Support Center, this could result in your account being locked for an unknown duration. Because of the volume of affected accounts, there may be a substantial delay in getting your account unlocked.

Here are some common cybercriminal social engineering and phishing themes we see at Mason:

- Notice of an overdue bill
- Notice of a package delivery or a missed delivery
- Notice of an eFax message
- Notice that an email mailbox has exceeded its limit
- Notice of an award, monetary deposit, or prize
- Notice of an invoice that needs to be paid
- Threat to close a bank account

How to avoid getting phished:

- DO NOT CLICK EMAIL LINKS OR OPEN ATTACHMENTS FROM UNKNOWN SOURCES. Delete email from unknown addresses.
- Be wary of requests for confidential information. No legitimate organization will ask you to provide your password in an email response. Passwords, user names, or accounts should never be shared.
- Question any “scare tactic” message. Account closures and loss of access are common fraudulent threats.
- Keep anti-virus software up to date and perform regular scans.

Beware, sender email addresses, links, and websites can be faked to appear to originate from Mason. Any official email communication from Mason's Information Technology Services will always include a local phone number that you can call to verify the email. If you receive an email and are unsure of whether it is a phishing attempt, contact the ITS Support Center at 703-993-8870 or support@gmu.edu for assistance.

Stay safe online and thank you for helping keep Mason secure!