Protecting Yourself Against Phishing

Information Systems recommends the following:

1. Use the Gmail web client instead of Outlook or Macmail. Once hackers have compromised your account they can setup filters to direct mail from specific persons. This is easier to detect when you are using the Gmail client.
2. Do not click on links in email. Phishers will use emails that look genuine to entice you to click on the links. You should always be able to go directly to a website and get the same information from any reputable company. You can also open another browser window and type the URL into the address bar.
3. Reputable companies will not call you to help you with malware on your computer.
4. Do not click on pop-ups reporting malware on your computer. Instead shut down your browser and run a Windows Defender scan.
5. Do not respond to emails requesting personal information. i.e. username, email address, password, phone number.
6. Ignore email notices that include threats or have urgency. Reputable companies will not use scare tactics like threatening to close your account or charge a fine. If you are unsure call the company to check.
7. Do not give personal information on phone calls unless you have initiated the call.
8. Ignore emails with typos and misspellings.
9. Be suspicious of social media invitations from people you don't know. Over one in five phishing scams target Facebook.
10. If an email seems to good to be true, it is.