What should I do if I receive a suspicious email?

Tell Me

Do not click any attachments or links in an unsolicited or suspicious email, even one that says "unsubscribe." Never respond to suspected phishing emails, and never send personal information like passwords via email.

Here are a few ways you might recognize these messages:

- They ask you to provide your username and password or other personal information (e.g. Social Security number, bank account number, PIN number, credit card number, mother's maiden name, or birthday). Even if they appear to be from a legitimate source, or contain an official-looking webpage, be careful. Spammers often ask for this information in an attempt to steal your email address, your money, your credit, or your identity. You should always be wary of any message that asks for your personal information, or messages that refer you to a webpage asking for personal information. One thing to be sure of: UMBC, Google or Gmail will never ask you to provide this information in an email; if the message asking for it claims to be from us, don't believe it.
- You might see a warning from Gmail when you open one of these messages. These phishing messages operate automatically, much like spam filtering. Gmail's spam filters automatically divert messages that are suspected of being unwanted messages into 'Spam'. Similarly, Gmail's phishing alerts automatically display warnings with messages we suspect are phishing attacks so you know to exercise caution before providing any personal information.

See How can I identify a phishing attack? for more tips.

If you think that the message is asking you to do something that seems unusual, look up the phone number of the person the message is from in the UMBC directory, call the person, and ask them if they really sent the message. Do not call a person back at a phone number that is listed in the suspicious email message. The phishing message may include the phone number of the hacker. For example, if you get a message saying that there is a problem with your computer account and you aren't sure if it's a real message, please call the DoIT Technology Support Center (410-455-3838) and ask if it's a real message. This also applies to any messages that might appear to come from Human Resources, Finance, Financial Aid, or any other department. If the message seems strange, trust your instincts, look up the correct phone number for the person, and call to verify the message.

If you believe the message to be a phishing email, send a copy of the "full headers" and as much information as you can to security@umbc.edu. DoIT will review the messages, verify that they are phishing messages, and take steps to try and protect the rest of the community.

Gmail may block sending of an email if it has already been identified as fraudulent. If this is the case, you do not need to forward the copy to security@umbc.edu.

Once you've reported any phishing messages to security@umbc.edu, please delete the messages, and very importantly, never click on the links in a phishing message. Just by clicking on the link in a phishing message, you may download a malicious program onto your computer.

Feedback: Correct or Suggest an Article | Request Help