Flag mail as phishing

Phishing mail is spam that is attempting to obtain specific information from an individual. This information can vary, however, it is usually of the type that is personal and not meant to be shared with others. Example of this type of information is: Social Security Numbers, sign in credentials to various accounts, name, address, etc. The email can request that you reply to the email with the information or, more common, you will be request to select a link embedded within the email.

If you suspect an email is phishing, never reply and never select any link within the email. Instead mark the email as phishing. When an email is marked as phishing, the system will mark future mailings from the sender as junk and direct those mailings to your junk email folder and Microsoft will be sent a copy of the email so they can investigate it further and improve their protection of the email accounts system wide.

We strongly urge individuals to mark phishing email as such and help Microsoft to improve security on the system.

To mark an item as phishing you must first sign into your account via a browser, the option to flag mail as phishing is not available via a client or mobile device.

To sign into your account via a browser, open a browser and go to http://mail.csuohio.edu

Once you are signed into your account, select the item to be marked as phishing.

At the top expand "Junk" and then select "Phishing"