Phishing & Spam

Phishing attacks have been a problem for many years. Typically, hackers send messages asking members of our community to click on a link or reply to an email message with a password. Their goal is to trick our community members into giving them access to our accounts and information. Sometimes, they pretend to be DoIT and send messages to ask for your password or to tell you that there is a problem with your UMBC account.

Recently, hackers have expanded their efforts by trying to send messages as people from the campus community using that person’s name and title to request information. They try to choose a name or title that the community would trust. As examples, they have requested information about how to wire money out of the campus and get people to send checks to outside addresses. They have also requested that people send them files containing the social security numbers of community members. In some cases, they have also impersonated UMBC vendors. In each of these examples, they have tried to make their phishing messages appear to come from a person that the campus would trust.

Hackers are motivated by money and resources and will continue to try to get to our accounts, information, and resources. The only thing that can stop them is the UMBC community working together to block their attempts. Here are some questions that DoIT frequently receives and the answers.