Spear Phishing Alert

There have been recent reports of successful spear phishing campaigns at other campuses in the USM system.

Spear Phishing is a targeted email containing information specific to individuals or groups within an organization and involves prior research to identify these targets. It is a malicious tactic to get users to divulge personal information or perform actions that cause network compromise, data loss, or financial loss.

Please be vigilant and suspicious when opening emails from any sources where you see the following warning banner.

CAUTION: This message originated from a non-UMB email system. Hover over any links before clicking and use caution opening attachments.

Carefully check the email address in the "from" field of all emails sent to you, not just the name on email messages. If the email address is not @umaryland.edu (i.e., @gmail.com), do not open any attachments and delete the email even if the name of the person and the username matches a UMB colleague.

In a recent attack campaign, the email contained a PDF attachment that, once opened, takes the recipient to a page that requests their username and password. If the username and password are entered, they receive a fraudulent request from the DUO multi-factor authentication (MFA) system. If they click "Approve" to this fraudulent MFA attempt, the attacker then has access to their UMB accounts and services.

This puts both the individual's and the university's data at risk.

Unfortunately, in the past week multiple members at USM campuses have clicked "Approve" on a fraudulent DUO request and had their accounts compromised.

To prevent this type of attack, here are a few important cybersecurity steps to follow:

- Again, look for the banner warning that the email originated from a non-UMB email system, carefully check the email address in the "from" field of all emails sent to you, not just the name on email messages. If the email address is not @umaryland.edu (i.e., @gmail.com), do not open any attachments and delete the email even if the name of the person and the username matches a UMB colleague.
- Be suspicious and double check anything that asks you to provide your UMB username and password.
- Stop and think before clicking "Approve" on a DUO request. Only approve the request if you are currently trying to log into a UMB system or application.

To the extent possible, please use the DUO app on your mobile device rather than DUO phone calls or Apple watches. The DUO app shows the city and state you are attempting to log in from. It should match, or be nearby to, your current physical location. If it shows a location far away from where you are, click “Deny” on the request.

Should you open a questionable email attachment, supply your password to a non-UMB source, or click “Approve” to a DUO request that you realize was not from you, please contact the CITS Security & Compliance group at security-compliance@umaryland.edu as soon as possible.

Thank you for remaining vigilant to help protect yourself and UMB’s data.