RECOGNIZE PHISHING SCAMS AND FRAUDULENT E-MAILS

Phishing is a type of deception designed to steal your valuable personal data, such as credit card numbers, passwords, account data, or other information.

Con artists might send millions of fraudulent e-mail messages that appear to come from Web sites or organizations you trust, like your bank, Credit Card Company or this school, and request that you provide personal information.

What does a phishing scam look like?

As scam artists become more sophisticated, so do their phishing e-mail messages and pop-up windows.

They often include official-looking logos from real organizations and other identifying information taken directly from legitimate Web sites. **In the case of MVSU**, the scammer may include an official looking address such as accountmanager@mvsu.edu or sign the message "mvsu.edu support team."

Please note that Mississippi Valley State University will never request any account information in an email. In addition, we will not send out a mass email with attachments requiring action from you!

To make these phishing e-mail messages look even more legitimate, the scam artists may place a link in them that appears to go to the legitimate Web site (1), but it actually takes you to a phony scam site (2) or possibly a pop-up window that looks exactly like the official site.

These copycat sites are also called "spoofed" Web sites. Once you're at one of these spoofed sites, you might unwittingly send personal information to the con artists. ***A virus or spy ware may be released onto your computer just by clicking on the link!***

How to tell if an e-mail message is fraudulent

Here are a few phrases to look for if you think an e-mail message is a phishing scam.

"Verify your account."

Businesses should not ask you to send passwords, login names, Social Security numbers, or other personal information through e-mail.

If you receive an e-mail from anyone asking you to update your credit card information, account information, passwords, or download an attachment to fix a virus do not respond: this is a phishing scam.

"If you don't respond within 48 hours, your account will be closed." Or "Please change your password"

These messages convey a sense of urgency so that you'll respond immediately without thinking. Phishing e-mail message might even claim that your response is required because your account might have been compromised.

"Dear Valued Customer." Or "Dear user of mvsu.edu"

Phishing e-mail messages are usually sent out in bulk and often do not contain your first or last name.

"Click the link below to gain access to your account."

HTML-formatted messages can contain links or forms that you can fill out just as you'd fill out a form on a Web site.

The links that you are urged to click may contain all or part of a real company's name and are usually "masked," meaning that the link you see does not take you to that address but somewhere different, usually a phony Web site.

Example of masked URL address

Con artists also use Uniform Resource Locators (URLs) that resemble the name of a well-known company but are slightly altered by adding, omitting, or transposing letters. For example, the URL "www.microsoft.com" could appear instead as:
www.micosoft.com
www.mircosoft.com
www.verify-microsoft.com

Please do not open any email (requiring action) that does not originate from a known member of the MVSU IT staff. The attachments, linked sites or requests for information will most likely be a phishing scam. Before taking action, we advise that you call to verify the legitimacy of the email.