HOW TO SPOT A PHISHING SCAM

Fraudulent emails ‘phish’ for your personal information, hoping to steal your identity and compromise your computer.

NEVER RESPOND TO A SUSPICIOUS EMAIL!

Not sure if a message comes from UMass Amherst IT? Contact the IT Help Desk at 413-545-9400.

Incorrect Recipient Information
Phishing emails are usually not addressed directly to you.

Forged Sender’s Email Address
Phishers can easily forge an organization’s email address. The message below is a scam even though the sender’s email includes umass.edu. Never assume an email is legitimate because you recognize the sender’s email.

Date: To: Subject: Reply-To:
May 18, 2011 1:32:48 PM EDT undisclosed-recipients; Official message webmaster@umass.edu

Deceptive Subject Line
The subject line is designed to scare or entice you to open the email. The message is often labeled ‘important,’ ‘official,’ or ‘required.’

Logo & Other Trademarks
Sophisticated phishing scams will use a company’s logo and other trademarks to make the email look genuine.

Impersonal Greeting
Some phishing emails use a generic salutation or an incorrect version of your name. More sophisticated scams will spell your name correctly.

Dear web mail Owner,

We are contacting you to inform you that our Account Review Team identified some unusual errors in your account profile. This may be due to the following:

* Using a shared computer to access your online webmail.
* Not logging off after webmail usage.

Due to this, an account update has been issued to rectify. Follow the Link Below providing the required security information correctly to re-gain access or we will locked your account permanently.

click here Or umass.edu security update

**Thanks *

Faulty punctuation, spelling & grammatical errors
Many phishing messages contain grammar and spelling mistakes. Upper and lowercase letters may be used incorrectly.

Links or attachments
Some phishing emails ask you to click a link or download an attachment that installs malware on your computer. Others ask for your user name, password, or other personal information.

Deceptive Subject Line
The subject line is designed to scare or entice you to open the email. The message is often labeled ‘important,’ ‘official,’ or ‘required.’

No Signature or Contact Information
This message does not include a signature, URL, phone number, or address. Some phishing emails may provide fake telephone numbers and other contact information.

© 2011 University of Massachusetts Amherst • Amherst, MA 01003. All rights reserved