MIAMI INFORMATION TECHNOLOGY

Phishing 101: How to Spot a Phishing Attempt

What is phishing?

The Federal Trade Commission (FTC) defines phishing as "when Internet fraudsters impersonate a business to trick you into giving out your personal information." In summary, phishing is a way criminals try to convince you to give them your sensitive information, such as credit card numbers, account information, and social security numbers.

The most common form of phishing is emails pretending to be from a legitimate retailer, bank, organization, or government agency. The sender asks to “confirm” your personal information for some made-up reason (i.e. your account is about to be closed, an order for something has been placed in your name, or your information has been lost because of a computer problem). Another tactic phishers use is to say they’re from the fraud departments of well-known companies and ask to verify your information because they suspect you may be a victim of identity theft. In a national case, a phisher claimed to be from a state lottery commission and requested people’s banking information to deposit their “winnings” in their accounts.

How can I tell if an email or website is a phishing attempt?:

While today's technology has becoming increasingly sophisticated, so have criminals. Attackers work diligently to create emails and websites that may seem legitimate. They can copy company's logos, images, and even login pages.

Upon opening your email, you may see a message similar to the ones below:

- "We suspect an unauthorized transaction on your account. To ensure that your account is not compromised, please click the link below and confirm your identity."
- "During our regular verification of accounts, we couldn't verify your information. Please click here to update and verify your information."
- "Our records indicate that your account was overcharged. You must call us within 7 days to receive your refund."

If you are unsure if an email is legitimate, ask yourself these questions:

- Does this company or sender look unfamiliar?
- Does the sender's identity not match the purpose of email?
- Is the “To:” line addressed to undisclosed-recipients or a large number of recipients? Does the website link look invalid?
- Are there misspellings and typos?
- Is the grammar and tone inappropriate?
- Am I being promised a lot of money for little or no effort on my part?
- Am I asked to provide money up front for questionable activities, a processing fee, or to pay the cost of expediting the process?
- Is someone asking me for my username and password, bank account number, and/or other personal financial information?

If any of the answers above are "yes," you might have received a phishing email.

Report phishing email immediately!

- For UM accounts, please forward phishing emails to: ciso@miami.edu.
- For other accounts, forward phishing email to spam@uce.gov as well as to the company, bank, or organization impersonated in the email.
- Additionally, Anti-Phishing Work Group is an anti-phishing organization. Emails can be reported to: ReportingPhishing@antiPhishing.org.

I was tricked! What should I do?

1. Change your password(s) immediately.
2. If you believe you have been a victim of phishing at UM, please call the UMIT Service Desk at (305) 284-6565. For other accounts, a report can be filed with the Federal Trade Commission at: www.ftc.gov/complaint.
3. Check and monitor your financial accounts. If you suspect your accounts have been compromised, immediately contact your financial institution to cancel all your cards and change your account information. Always call the number that appears either on your statement or on the back of your credit card or bank issued card.

For more information about keeping the University's data – as well as your personal data – safe, please contact UMIT Security at: ciso@miami.edu or visit: miami.edu/it/security. There is also phishing training available via ULearn; Visit: ulearn.miami.edu and search "*Phishing - Don't Get Hooked*."