Phishing 101: Tips to Protect Yourself

How can I protect myself from phishing?

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. Here are few tips to protect yourself from phishing attacks:

- **Don't reply to emails, texts, or pop-up messages that ask for your personal or financial information.** Delete them immediately.

- **Don't click on suspicious links within emails.** Fraudsters use these links to lure people to phony websites that looks just like the real sites of the company, organization, or agency they're impersonating. If you follow the instructions and enter your personal information on the website, you'll deliver it directly into the hands of identity thieves. To check whether the message is really from the company or agency, call it directly or go to its website (use a search engine to find it).

- **Beware of "pharming."** In this latest version of online ID theft, a virus or malicious program is secretly planted in your computer and hijacks your web browser. When you type in the address of a legitimate website, you're taken to a fake copy of the site without realizing it. Any personal information you provide at the phony site, such as your password or account number, can be stolen, and fraudulently used. Make sure to check the URLs of all websites before entering any personal information.

- **Never enter your personal information in a pop-up screen.** Sometimes a phisher will direct you to a real company, organization, or agency's website, but then an unauthorized pop-up screen created by the scammer will appear, with blanks in which to provide your personal information. If you fill it in, your information will go to the phisher. Legitimate companies, agencies, and organizations don't ask for personal information via pop-up screens. Install pop-up blocking software to help prevent this type of phishing attack.

- **Protect your computer with spam filters, anti-virus/anti-spyware software, and a firewall – and then keep them up-to-date.** A spam filter can help reduce the number of phishing emails you get. Anti-virus software, which scans incoming messages for troublesome files, and anti-spyware software, which looks for programs that have been installed on your computer and track your online activities without your knowledge, can protect you against pharming and other techniques that phishers use. Firewalls prevent hackers and unauthorized communications from entering your computer – which is especially important if you have a broadband connection because your computer is open to the Internet whenever it's turned on. Look for programs that offer automatic updates and take advantage of free patches that manufacturers offer to fix newly discovered problems.

- **Only open email attachments if you're expecting them and know what they contain.** Even if the messages look like they came from people you know, they could be from scammers and contain programs that will steal your personal information.

- **If someone contacts you and says you've been a victim of fraud, verify the person's identity before you provide any personal information.** Legitimate credit card issuers and other companies may contact you if there is an unusual pattern indicating that someone else might be using one of your accounts. But usually they only ask if you made particular transactions; they don't request your account number or other personal information. Law enforcement agencies might also contact you if you've been the victim of fraud. To be on the safe side, ask for the person's name, the name of the agency or company, the telephone number, and the address. Get the main number from the phone book, the Internet, or directory assistance, then call to find out if the person is legitimate.

- **Job seekers should also be careful.** Some phishers target people who list themselves on job search sites. Pretending to be potential employers, they ask for your social security number and other personal information. Follow the advice above and verify the person's identity before providing any personal information.

- **Be suspicious if someone contacts you unexpectedly and asks for your personal information.** It's hard to tell whether something is legitimate by looking at an email or a website; it's even hard to tell if something is legitimate by talking to someone over the phone. But if you're contacted out of the blue and asked for your personal information, it's a warning sign that something is "phishy." Legitimate companies and agencies don't operate that way.

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*.”