UPDATE on EMAIL SECURITY and PHISHING ATTACKS 8/14/14

Unfortunately we have had several recent phishing attacks using compromised UF accounts.

***** Do not respond to ANY email asking for your username and password *****

Do not click on any email links or respond to emails asking for your personal information or passwords. No legitimate IT, banking, brokerage, social networking, shopping site, or educational institution will ever ask you for this information in an unsolicited email.

Here is an example that we are seeing today. It is from a UF account, but it is a compromised one. Please note that the malicious links have been removed.

----Begin Example Phishing Message----

From: UF Account <———— Do not respond to these even if they are a UF account
Sent: Wednesday, August 13, 2014 11:48 AM
To: ***snipped***
Subject: RE: Your mailbox is full

Your mailbox is full.

465MB 500MB
Current size Maximum size

Your mailbox has exceeded it storage limit. You will not be able to receive new mails at 480MB. Click here to update your account.

----End Example Phishing Message----

If you have any questions about phishing or other cyber security topics please let me know.

Sincerely,
Craig

Craig Gormé
Information Security Manager
UF Health IT
University of Florida
Phone: (352)273-5203
Email: craig@ufl.edu

Everyone,

It is a new fiscal year and we have many new faculty, residents, and students at UF Health so I just wanted to take a couple of minutes and warn everyone about phishing attacks.

Phishing attacks use email, websites, and sometimes unsolicited phone calls from seemingly trustworthy organizations and people to ask for personal or confidential information. The links that they provide may point to an infectious web site or a computer virus which would try to infect your computer.

****Do not click on any links or respond to emails asking for your personal information or passwords. No legitimate IT, banking, brokerage, social networking, shopping site, or educational institution will ever ask you for this information in an email.****

If you have a question about an email from an organization with which you do business, please call a known and trusted phone number or go a bookmarked favorite; do not use the link in the email.

Here is an example we are seeing today. It pretends to be from the UF Help Desk, but it is not. Please note that the malicious links have been removed.

----Begin Example Phishing Message----

From: ****snipped*** <——————————from an unknown person or organization not UF
Sent: Monday, July 28, 2014 7:34 AM
Subject: Staff and Faculty Mailbox Message !

Your mailbox is full.

465MB **500**MB

Your mailbox need to be cleanup, no longer send messages. Please cleanup your mailbox.
By Automatically clicking on Cleanup.(<——————**Hidden non UF address/Link)** and fill out the necessary mailbox requirement to cleanup your mailbox Quota.
IMPORTANT NOTE: You won't be able to receive mail messages at 480MB.

ITS help desk

ADMIN TEAM

----End Example Phishing Message----

Also, I would like to remind everyone that to protect yourself from computer malware and viruses please take the time every month to update your personally owned computers and devices with the latest updates from Apple, Microsoft, Adobe (Flash and Acrobat), Oracle (Java), and others.

If you have any questions about phishing or other information security topics please let me know.

Sincerely,
Craig

Craig Gormé
Information Security Manager
UF Health IT
University of Florida
Phone: (352)273-5203
Email: craig@ufl.edu