Phishing Alert and Increased Compromised Accounts

To::
All Faculty and Staff
Names and titles:

Gil Salazar, Interim Deputy CISO, UA Information Security

Date::
May 5, 2016

Multiple phishing campaigns targeting faculty and staff this week have been reported to UA Information Security. As a reminder, phishing is a technique used to obtain sensitive information, such as usernames or passwords, by sending emails designed to trick the user into providing the information, or to open an attachment that installs malware on devices.

Subject lines in recent phishing emails included **Project Review** and **File Message.**

Following these phishing reports, UA Information Security and the Financial Services Office has seen an increase in suspicious changes to employee direct deposit information.

What should I do if I receive a suspicious email?
If you receive an unsolicited email or you are unsure of the sender:

1. Do not reply, click on any links, or open any attached files

2. Check the **UA Information Security phishing alerts page** [1] to see if this is a known phishing message.

3. If the suspicious email is not listed in the phishing alerts, **forward the email as an attachment** [2] to infosec@email.arizona.edu [3].

If you are concerned that you or your device may have been compromised, please contact your local IT support or the 24/7 IT Support Center (520-626-8324).

How do I know if my information has been compromised?
If your direct deposit information is changed, you will receive an email alert. However, if your NetID has been compromised, remember that the perpetrator may be checking your email and delete the notification. If you are concerned, log into your **UAccess Employee account** [4], and verify that your information is correct.

What can I do to protect my information and account?
You are strongly encouraged to enroll in **Global NetID+** two-factor authentication. While NetID+ can provide a layer of protection, it will not protect your UAccess accounts if your NetID password is compromised. Enabling Global NetID+ requires two-factor authentication on all University systems.

Enroll in NetID+ [5] **today,** and enable **Global NetID+** [6] after you enroll.

Visit our **phishing awareness page** [7] for additional information and advice about these and other kinds of email phishing attacks.

https://uaatwork.arizona.edu/sites/default/files/5-5-16phishingalert.pdf

Links
[1] http://security.arizona.edu/phishing-alerts [2] http://security.arizona.edu/forwarding-phishing-email-attachment-guide [3] mailto:infosec@email.arizona.edu [4] http://uaccess.arizona.edu/ [5] https://webauth.arizona.edu/netid-plus [6] http://security.arizona.edu/netid-plus#global [7] http://security.arizona.edu/phishing