Continued Email Phishing Activity

To::
All UA Faculty, Staff and Students
Names and titles:
University Information Technology Services

Date::
February 13, 2019

University Information Technology Services (UITS) is continuing to see a high amount of email phishing activity on campus. These attempts are specifically requesting users to make purchases, send funds, or change bank account information, which can have a detrimental effect, including financial loss or fraud. UITS continues to apply additional steps to remediate the situation.

Current situation:

- Malicious emails were detected starting in December and have continued.
- Specifically, University leadership is being targeted as well as any staff who may have access to financial accounts. This includes the president's office, the provost's office, the Financial Services Office, and other staff.
- Examples of campus phishing emails received can be found at Phishing Alerts: security.arizona.edu/phishing_alerts [1].
- If the recipient responds to the email, the hacker asks the recipient to purchase a gift card or provide a personal loan.

What you can do:

If you receive an email that does not contain any information indicating that it is spam or you are uncertain if the message is legitimate, take the following actions.

1. Review the "from" email address for indications that it is not coming from the implied individual.
2. Before responding to requests sent to your University email account for purchasing gift cards or sending funds, contact your immediate supervisor.
3. Contact the Information Security Office at security@arizona.edu [2] or 520-621-6700.

Please forward phishes you receive to phish@arizona.edu [3] as described here: https://security.arizona.edu/content/phishing [4]. If you have any additional questions, please contact the Information Security Office at security@arizona.edu [2].

Resources:

- What's Phish? security.arizona.edu/node/335 [5]
- Phishing Alerts: security.arizona.edu/phishing_alerts [6]