After Successful Phishing Scam, UA Officials Offer Tips to Stay Safe

University Communications
January 2017

University officials are reminding the campus community to beware of phishing scams after several employees complied with a bogus email request for their UA NetIDs and passwords and then had their paychecks diverted.

The person or people behind the scam – which originated from Nigeria – used the information provided by the employees to change their direct deposit settings via UAccess.

Bob Sommerfeld, UA Police Department assistant chief of police, said**UAPD** [1] worked with University Information Technology Services to investigate and resolve the breach. Since the crime originated from outside the United States, UAPD notified the FBI.

Gil Salazar, interim deputy information security officer at the UA, said the issue was resolved fairly quickly with the help of UAPD, Human Resources and the payroll office, which was able to reissue paychecks to the affected employees.

There are several steps that employees can take to ensure that their accounts, information and computers aren't compromised or fall prey to a phishing attack.

One way is to sign up for NetID+, the UA's two-factor authentication system, which puts an extra layer of security on accounts by requiring a person's NetID and password plus additional verification via a phone call, text message, or other methods.

"Because the use of the internet and computers is a daily way of life and handles things from research to paying bills to making purchases, make sure that you use the web wisely and take steps that are designed to protect you," Sommerfeld said. "Yes, they might require added effort. But it's miniscule when compared to the efforts needed to correct a problem."

It's also recommended that employees enable Global NetID+, which will enforce two-factor authentication for all sites that use UA WebAuth authentication services, such as email and UAccess.

The UA, officials said, will never ask employees to provide their NetIDs or passwords via email.

Another recommendation is to not click on links in emails from unknown senders as they often have hidden URLs attached to them, Salazar said.

Sommerfeld encouraged employees to report any emails that ask for that information – and emails that look even slightly suspicious – by calling 621-8476 or forwarding the email with headers to **infosec@email.arizona.edu** [2]. To learn more about email headers, click **here** [3].

Salazar suggested that employees also visit the UA **Information Security** [4] website, which offers workshops on detecting phishing emails. A feed is also set up on the **website** [5] to alert visitors of any known phishing emails.

Source URL:https://uaatwork.arizona.edu/lqp/after-successful-phishing-scam-ua-officials-offer-tips-stay-safe

Links
[1] http://uapd.arizona.edu [2] mailto:infosec@email.arizona.edu [3] http://security.arizona.edu/full-email-headers-guide [4] https://security.arizona.edu/phishing [5] http://security.arizona.edu/