Guest Column: Don't Get Hooked by Phishing Attacks

UA Information Security
October 2014

Every day, University of Arizona employees and students receive thousands of phishing emails. Some of these emails have been so believable and well-crafted, recipients were tricked into providing personal information, such as usernames and passwords, which were used to reroute direct deposit of their University paycheck to the hackers' accounts.

The UA is not alone when it comes to these scams. Universities around the country have seen an increase in direct deposit hijacking attacks. Over the past year, UA Information Security [2] has worked with the Financial Services Office [3] and University Information Technology Services [4] to implement safeguards against these attacks.

FSO and UITS set up an alert system to notify staff members via email when their direct deposit information is changed. These alerts help make employees aware if their banking information is modified inside UAccess Employee.

Now when UAIS detects a login to UAccess Employee from a suspicious location, FSO contacts the employee to confirm the login was legitimate and that no sensitive data was altered by anyone other than the employee.

"These steps have helped in securing UA employee accounts," says Christian Schreiber, University Information Security Officer. "However, employees should take an additional step and sign up for Global NetID+.

In March 2014, Lo Que Pasa covered the launch of UA's two-factor authentication solution, UA NetID+ [5] (read the initial coverage here [6]). UAIS's newsletter, SecureCat Courier, covered Global NetID+ and its benefits at length in its June 2014 issue [7].

"Global NetID+ requires that all UA WebAuth logins use two-factor authentication," Schreiber says. "Putting this extra layer of protection in place makes it harder for someone to pretend to be you, even if they've stolen your password. This helps protect sensitive information, such as your banking account information in UAccess Employee."

UAIS has developed an outreach campaign to educate the UA community on phishing attacks and how to recognize phishing emails. In October 2013, UAIS added a new Phishing Alert [8] RSS feed to its webpage. Staff and students are able to subscribe to the feed [9] to receive alerts on the latest phishing attempts. The critical piece of this process is receiving notifications from UA community members when they receive phishing emails. Reporting has increased tremendously over the past year. We would rather receive multiple reports of the same phishing attempt rather than no report, and we do.
In addition, UAIS asks that users either forward suspicious emails as attachments [10], or send us the full email headers [11]. This way, we are able to more fully investigate the source of the email. The information helps us to mitigate future attacks.

When it comes to recognizing suspicious emails, check out these five UAIS tips on "How to Smell a Phish."

- **Sender tries to get you to act quickly before thinking.** The subject line will be alarming or enticing. Just remember, if it looks too good to be true, it is.
- **Grammar and misspelled words.** Phishing emails often contain typos and poor grammar.
- **Do the "hover" test: Is there a link in the email?** Hover over it with your mouse and see if the URL matches the one in the email. However, keep in mind that phishers are becoming more sophisticated in their scams, and may use web addresses similar to the correct link. For example, they could use "mybankonline.com" instead of "mybank.com."
- **Sender requests sensitive information.** If you are asked to provide sensitive information, such as passwords or account numbers, either in an email or by clicking on a link, the email is a scam. No legitimate business or organization – including the UA – will ask you to provide sensitive information in this way.
- **The "reply to" address or sender's address does not match the company's URL.** If you receive an email claiming to be from your bank, a credit card company or the UA, it should not be from an email address that you would not expect to find from the sending company, such as a Gmail, Hotmail or Yahoo! account.

For more information about NetID+ information and instructions for opting in to the service, visit [webauth.arizona.edu/netid-plus](http://webauth.arizona.edu/netid-plus) [12]. For more information on phishing and recognizing suspicious emails, visit [security.arizona.edu/phishing](http://security.arizona.edu/phishing) [1].

**Source URL:** https://uaatwork.arizona.edu/lqp/guest-column-dont-get-hooked-phishing-attacks

**Links**
[1] http://security.arizona.edu/phishing
[5] https://webauth.arizona.edu/netid-plus/
[7] http://security.arizona.edu/securecat-courier-archive#five
[8] http://security.arizona.edu/phishing-alerts