With the advent of Spring 2014, UA Information Security is launching a new quarterly newsletter, the SecureCat Courier. Each quarter, we will highlight security topics and how they apply to your daily routine as a University employee.

We welcome your questions and ideas for future editions! Is there a security topic you’d like to know more about? Did you see a recent news story about security and you would like to understand it better? Please let us know by sending your suggestions!

**ALL ABOUT PHISHING**

What do the following phrases have in common?

- Illegal Sign-In Alert
- Your UA Pay Increase
- Your UA NetID was compromised

**ANSWER**: They have all been subject lines for phishing emails to UA faculty, staff and students in the past few months.

UA Information Security is asked on a regular basis, “Why do we receive so much spam and phishing?” Here’s the answer: because it is effective.

As users become savvier about recognizing phishing, the bad guys become more deceptive. They are doing their research in order to get their messages past spam filters. And, unfortunately, these messages continue to deceive members of our community into sharing usernames and passwords, clicking on links, opening attachments, and ultimately putting their computers, personal information, and university data at risk.

But all is not bleak. UA Information Security is here to provide you with the tools so that you can recognize a phish when you see it.

**DON’T GET HOOKED BY AN EMAIL SCAM**

68% of email traffic contains phishing threats*

*Kaspersky 2013 Security Report
**HOW DO I RECOGNIZE A PHISH?**

In the old days (aka, the 1990s), spam was primarily made up of the online world's junk mail. These emails try to sell you something, and may or may not be harmless.

In the world of phishing, social engineering is the name of the game. These emails are designed to entice the recipient to behave in a way that goes counter to the user’s best interests.

How do social engineers do this? Look at some sample phishing subject lines:

- Illegal Sign-In Alert
- Your UA Pay Increase
- Your UA NetID was compromised

These subject lines elicit an emotional response from the recipient, even if it is only curiosity. And, if the phishing email is fairly well-crafted, it will fool some people in our community.

Let’s look at one of the more deceptive phishing emails that was sent in the past few months.

**Your UA NetID was compromised:**

Such a subject line is going to make the calmest among us anxious. Our UA NetIDs allow access not only to University information assets, but also to our own personal information, including our compensation and benefits.

In this email, the bad guys included a fake UA logo that, unless you are a campus brand advocate or pay close attention to detail, would fool most users into believing this was a legitimate UA email. The “sender” also appeared to have an arizona.edu email address.

To view our campus alert, as well as an illustration of how to spot the “phish” in this email, click [here](http://security.arizona.edu).

---

**PHISHING INFORMATION ON OUR WEBSITE**

Because of the pervasiveness of this problem, we have devoted more real estate on our website to combatting phishing than any other issue.

1. **Phishing Awareness Page:** Designed to educate users on analyzing suspicious emails, and what to do if they fall prey to a phishing attack.
2. **Phishing and Fraudulent Email Illustrated:** Three phishing emails received on campus are dissected to help users understand how to detect that these messages are phishing.
3. **Phishing Alerts:** An RSS feed that can be accessed from any page on our website where we report the latest phishing attacks seen on campus. Users can subscribe to this feed and receive the alerts in their email boxes.

---

**TEST YOURSELF!**

Can you spot a phish when you see it? These fun quizzes will inform as well as entertain, and take only a few minutes. Look at it as personal and professional development!

- [OnGuard Online](http://security.arizona.edu)
- [Open DNS](http://security.arizona.edu)
- [SonicWall](http://security.arizona.edu)
HELP US HELP UA – REPORT THAT PHISH!

If you receiving a phishing email, and it is NOT listed in our Phishing Alerts, please report the phish to our office on our "Report an Incident" page. Please do one of the following when you are reporting phishing activity:

1. If possible, forward the suspicious email to infosec@email.arizona.edu, and include the "subject line" in the incident form below with an explanation that you are forwarding the email as an attachment. For instructions on forwarding the email as an attachment, click here, OR
2. If you are unable to forward the email as an attachment, please copy the full email headers into the field under "Describe security-related concerns." For instructions on accessing headers, click here.

Our office works with UITS Security Operations and other campus units using the information you provide in order to minimize the current phish threat. We will also use the information for analysis and trending information on security threats to campus.