Because we must be right 100% of the time to not fall for a phish.

Many are easy to spot, but some are so well-crafted, they will fool the most security savvy among us.

This month’s newsletter provides you with a security toolkit to help you avoid the “phish” hook. These tips, plus a healthy dose of skepticism, will help protect you, your identity, and the University’s information.
Phishing: All About Social Engineering

Social Engineers are masters of manipulation. In short, they are con artists who prey on human nature, and our desire to be helpful, our tendency to trust others, and our fear of getting into trouble or losing access to something valuable. Phishing is the most prevalent form of social engineering we witness in our day-to-day lives.

What is Phishing?
TechTarget.com defines phishing as “a form of fraud in which the attacker tries to learn information such as login credentials or account information by masquerading as a reputable entity or person in email, IM or other communication channels.”

Phishing is broad term that encompasses other scams performed over other media than email, including:
1. Text messaging
2. Phone calls or voice mails
3. Malicious advertising on websites

Phishing.org has a lengthy list of phishing techniques, but they all have the same purpose: to trick you into giving away something the bad guys want.

Phishing is a Crime
The Anti-Phishing Working Group (APWG) defines phishing as “a criminal mechanism employing both social engineering and technical subterfuge to steal consumers’ personal identity data and financial account credentials.” The Group’s latest report highlights disturbing phishing trends in the first quarter of 2016, such as:

- More than 500,000 unique phishing email campaigns were reported
- 290,000 unique phishing websites were detected, with a whopping 36% increase between February and March
- The United States continues to lead the list of countries hosting phishing sites, topping out at almost 82% in February 2016

Why Can’t Spam Filters Catch All Phishes?
Spam filters do a fairly decent job of catching spam, but phishing emails are a different breed. UA Information Security has shared in its phishing alerts feed some samples that demonstrate how much scammers have done their homework. Here are two examples we have seen just in the month of June:

1. Not a UA email address
Your Pay Advice is now ready for online review on Employee Self Service: [link]
If you have any questions, please contact your Payroll Department.

2. UA Information Security’s email address was spoofed; UA logo, phone number, and copyright included; Appears to be from UA department, but link is not to a legitimate UA site
[Detailed analysis of phishing email]
These two particular samples are referred to as “spear phishing.” TechTarget.com defines spear phishing as “is an email spoofing fraud attempt that targets a specific organization, seeking unauthorized access to confidential data.” These types of phishing attacks are very sophisticated. These scammers did enough reconnaissance so that they could spoof two legitimate departments on campus, and trick employees into clicking and providing information. This level of sophistication cannot be caught by your average spam filter. The only prevention for these types of scams is well-informed employees.

How to Recognize a Phish

The key to protecting your information and the University’s information assets is learning how to spot a phish, and reporting it to UAIS to assist us in alerting campus to the latest scam.

Look for these clues to detect a phishing email:

- **A “sense of urgency” to trick you into acting 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.
- **Is there a link in the email? Do the "hover" test:** Hover over it with your mouse and see if the URL matches the one in the email. 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, including your NetID password.
- **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 such as a Gmail, Hotmail or Yahoo! account.

For more information, please go to UAIS’s phishing page.

Help Us Help UA – Report That Phish!

UA Information Security posts phishing alerts on our website to keep our community informed of the latest scams hitting campus email boxes. For instructions on reporting phishing, please visit our website.
What Does a “Good” Email Look Like?

Security-minded employees frequently forward suspicious emails to UA Information Security, asking if the emails are legitimate or spam/phishing. In response, our office has produced many articles, brochures and webpages covering recognizing phishing emails that employees receive.

But what about helping departments learn how to SEND emails that don’t look “phishy” in the first place? Here are a few tips to help you with that effort.

DON’T HIDE LINKS. Seeing CLICK HERE in an email should cause you to hit the delete key. While long hyperlinks may look unsightly to you, they are a signal to the email recipient that you have nothing to hide. What is a better way of handling hyperlinks? Spell it out, and make it “not clickable.” For emails sent between employees who regularly interact, go ahead and send a “live link.” However, if you are sending an email to individuals or groups that are not expecting them, we recommend that you ensure that the link will not be “clickable” by changing the “http” to “hxxp.” We then add the following verbiage after the link:

Copy and paste the URL, and replace “hxxp” with “http.”

By doing this, we have ensured that a link is not sent live, and that the recipient knows we aren’t hiding anything suspicious.

PROOFREAD, or ask a colleague to do it for you. Phishing emails routinely have misspelled words and poor grammar. Make sure that the email looks professional, especially one sent to large numbers of people. We don’t always catch our own mistakes, but an extra set of eyes can help prevent embarrassing or costly mistakes.

REVIEW EMAIL TEMPLATES. Many departments routinely use templates to disseminate information to large numbers of people on a regular basis. Take a look at those templates to see if you need to update them with an eye to security. If you aren’t sure, contact us! We are happy to help!

USING A THIRD PARTY TO SEND EMAILS? EDUCATE THEM! Remember, you are paying for these services to represent you. Vendors should be happy to comply with up-to-date secure practices for sending email. If they aren’t, find another provider.

GIVE A HEADS-UP: Sometimes, you have to send bulk emails that bend best practices a little. If possible, give your recipients advance notice that they will be receiving emails regarding certain topics. That way, if the email does have hidden links, etc., recipients won’t immediately delete the email, or mark it as spam.

Would you like to promote security awareness in your department? Download our custom screensavers!

THINK BEFORE YOU CLICK
In one year the number of malicious web links grew by nearly 600%