Not exactly the reason you want to be in the news.

What does that have to do with the University of Arizona community? We are an environment that is rich in valuable data that the bad guys want to access.

By now, many New Year’s resolutions have already been broken. But UA Information Security is on a mission to help you take small, achievable, and very significant steps toward security, both for yourself and for the University of Arizona.

The University has made significant strides in the past year toward improving our security posture as an institution. But those strides mean nothing without your help.

This month’s newsletter highlights important security building blocks. Adopting even a few of these habits will greatly enhance your security.

SecureCat Courier is the University of Arizona’s quarterly security newsletter.
Safe computing practices include a combination of how you technically protect your computer by using software and security settings, and the physical actions you take. Your actions make a difference! "Security Building Blocks" can function as a security checklist to protect your data. For further information on each topic, as well as instructions on how to implement these steps, visit the accompanying links to our website.

1. Keep Systems up to Date with Automatic Updating.
3. Use Stronger Passwords.
4. Back Up your Data, Twice.
5. Secure your Physical Environment.
6. Email: Think Before you Click, Open, or Reply.
8. Protect Sensitive Data.
10. Most Importantly, Stay Informed.

UA NetID+ JUST GOT BETTER

The University of Arizona introduced UA NetID+ to the UA community in April 2014. NetID+ is the UA’s method of two-factor authentication for all UA faculty, staff and student NetID accounts.

UA Information Security wholeheartedly endorses the use of NetID+, especially Global NetID+. However, many users found having to authenticate their UA NetIDs using their smartphone, cell phone, landline or Yubikey a huge inconvenience. In response to this issue, CIO senior leadership approved a “Remember Me” checkbox.

UITS is applying a trusted devices feature, similar to 'remember my computer’ options users are accustomed to seeing during authentication on websites for banks and other financial institutions.

How it Works
When faculty, staff or students are prompted for a second authentication using NetID+, they can select the checkbox Remember this device for 30 days option. By selecting this option, users will not be prompted for a second authentication for 30 days. After the 30-day period, users will once again be prompted for a second authentication.

The Remember this device feature:
- works for all UA WebAuth and Outlook Web App (OWA) services
- is not a global setting, and must be enabled on each computer/device/browser
- SHOULD NEVER BE ENABLED on public computers.

Click here to learn more about NetID+, and to start using this great security tool today!

COMING IN APRIL!
NetID+ with the University’s Virtual Private Network (VPN)
Employees are asking:

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 “fishy” in the first place?

Here are a few tips that, if followed, will save your department from hearing complaints about your emails.

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 being sent back and forth 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. We send so many emails a day that we are bound to have an occasional typo. But when you are sending emails to large numbers of people, or to people who may not be expecting to hear from you, make sure that the email looks professional. We don’t always catch our own mistakes, but an extra set of eyes can help prevent embarrassing or costly mistakes.

UPDATE YOUR TEMPLATES. Many departments routinely use templates to disseminate information to large numbers of people on a regular basis. For example, your department may send out information at the beginning of a semester. 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 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: There are times when you will need to send bulk emails that bend best practices a little. If at all 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.

UA InfoSec Website | Contact Us
UA Information Security
1077 North Highland Avenue
Tucson, AZ 85721
520.621.8476 (UISO)

©2015 Arizona Board of Regents