Information Security

SecureCat Courier

March 2017

The W2s and 1099s are ready to go. You have entered your deductions and are ready to file your tax return. Then you discover that a return has already been submitted in your name. What do you do now?

This month's newsletter highlights:

- Tips for protecting your identity and sensitive data
- Preparing for UA security enhancements

We will also introduce you to our new Chief Information Security Officer, Lanita Collette!

In This Issue

UA InfoSec Resources

- Security for Faculty and Staff
- All-Employee Security Awareness
- Phishing Alerts

SecureCat Courier is UA's monthly cybersecurity newsletter, distributed by Information Security Liaisons to UA faculty and staff.

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

Tax Season=Tax Fraud & Identity Theft!

According to the Federal Trade Commission (FTC), identity theft is the top consumer complaint received. And the most common identity theft complaint is tax- or wage-related fraud. In fact, tax refund theft is the fastest-growing form of identity theft.

HOW DO THEY DO IT?

While conventional wisdom may lead you to believe that identity thieves are stealing W2 forms, they generally file federal tax returns online with stolen identity information and phony wage and tax withholding figures. They then provide information so that the refund is loaded onto debit or prepaid credit cards, direct-deposited into the thieves' accounts, or mailed to a certain address.

TIPS FOR PROTECTING YOUR IDENTITY

- ❑ Don't carry your Social Security card or any document(s) with your SSN on it.
- ❑ Check your credit report on a regular basis.
- ❑ Practice good online security.
- ❑ Never use the "remember my password" function.
- ❑ Always use a secure Wi-Fi connection.
- ❑ Shred paper documents that have sensitive data before discarding them.
- ❑ Be careful about where you share information on the internet, such as your birthdate, address and phone number.
- ❑ Don't give personal information over the phone, through the mail or on the Internet unless you have initiated the contact.

For more tips on identity security, visit our Identity Theft page.

Meet Our New CISO, Lanita Collette!

Chief Information Security Officer for University of Arizona

Lanita Collette landed on campus February 27, 2017 as UA's new Chief Information Security Officer (CISO). Although she is new to UA, she has called Arizona home for quite some time. Prior to her appointment, Lanita most recently served as Deputy CIO and University Information Security Officer at Northern Arizona University. Before that, she held various management positions in IT at NAU, including Assistant Director for Enterprise Information Solutions, Interim Director of Academic Computing, and a variety of team lead positions.

Prior to moving into IT, Lanita was an archaeologist engaged in research on the Colorado Plateau. She has a BA in Anthropology from Bryn Mawr College and an MA in Archaeology from Arizona State University, and holds both Project Management Professional (PMP) and Certified Information Systems Security Professional (CISSP) certifications.

UA Information Security has set up a new email address for "Ask the CISO" questions. You can reach out to Lanita at ciso@list.arizona.edu.

Coming Soon! UAConnect365

UA is moving the UAConnect faculty/staff email and calendaring system to Microsoft's Office 365 cloud in spring 2017, bringing greater storage size, functionality and, most importantly, security.

Office 365

What Does This Mean to You?

Microsoft Office 365 (O365) and UAConnect365 (email/calendaring) services will require a new NetID password and NetID+ to log in. Act now to avoid any interruptions in accessing Office 365.

- Change your password now. You need a UA NetID password created or changed since March 6, 2017. The standard expiration (360 days for a strong password) will apply.
- Sign up for NetID+ now if you do not currently have two-factor authentication.

If you have questions or need assistance, contact your department's IT support or the 24/7 IT Support Center (520- 626-8324).