CWU Internal Audit

# The Audit Insight

ISSUE No. 8, Spring 2020

## IN THIS ISSUE:



## COVID-19 Fraud Scams

Scammers take advantage of current events, such as the COVID-19 pandemic, and find ways to scam vulnerable people. There are several recent fraud scams listed below with tips on how to avoid scams, what to look out for, and how to protect yourself and the University against scammers.

### Coronavirus Phishing Scam Targets University Students, Staff

*www.edscoop.com – Written by Betsy Foreman. Published 3/18/2020*

Hackers are aware that students, faculty, and staff want to know about University decisions and responses to the pandemic, and they take advantage of the current events. Fake emails appearing to be from trusted sources led to email user names and passwords being stolen. The fake email tempted readers to click a link to access important information from the university's "health team." The link led readers to a fake Office 365 website login screen. The reader would enter their user name and password in an attempt to access the information, when in reality, they had just given the hacker their email credentials. In some instances, harmful malware was also installed on computers.

### Common Natural Disaster Fraud Schemes

*https://www.acfe.com/disasterfraud/ - ACFE*

The Association of Certified Fraud Examiners (ACFE) has provided resources for how to avoid common frauds related to natural disasters including charity, contractor, and vendor fraud. Be sure to research any organization before donating. Searching "scam" followed by the name of the organization on a search engine may reveal scams related to the organization. Also be sure to research any companies you do business with by reviewing history of work performed in your area and read customer reviews.

## How to be successful at this stuff

## Security Tips

### Working from Home?

CWU employees working from home should do so securely.

- Familiarize yourself with the Information Security & Privacy Roles & Responsibilities Policy.
- Ensure the PC or Mac being used has Antivirus Software.
- Utilize Cisco AnyConnect client for VPN for a secure connection.
- Set a strong password for your home's wireless network.
- Use OneDrive or other CWU-approved services for cloud storage, file sharing, and collaboration.
- Computers should be configured to apply application updates and operating system (OS) patches regularly.
- Check out tips on how to prevent eavesdropping and protecting privacy on virtual meetings at Work and Learn Online Securely.
- Click here for current information on relevant information security alerts.
- For more information about working from home securely, here is the Remote Work Toolbox.

## Learn to Identify Phishing

Phishing Emails are a common identity theft scheme. Phishing occurs when cybercriminals create FAKE EMAILS that appear to be from trusted organizations or people and attempt to get you to; provide your confidential information; give them your username & password; download or open a malicious attachment.

This brief **presentation** will help you learn how to identify a phishing attack.

For more information, please go to **http://www.cwu.edu/security-services/**

## Prevent Zoombombing: Change these 4 Zoom Settings Now for Secure Video Chat

*www.cnet.com – Written by Rae Hodge. Published 4/8/2020*

Online users can easily utilize Google to find unprotected meetings. If employees decide to utilize Zoom there are settings that should be changed immediately such as enabling the "Waiting Room" feature and disabling the "Join Before Host" options. The article also goes into detail about how to handle someone "zoombombing" a meeting that employees should be familiar with just in case.


## Coronavirus: Scammers Follow the Headlines

*www.consumer.ftc.gov – Written by Colleen Tressler. Published 2/10/2020*

This article gives additional tips on how to protect yourself against scammers such as:

- Beware of emails claiming to be from the Centers for Disease Controls and Prevention (CDC) or experts claiming to have information about COVID-19
- Ignore offers for vaccinations
- Be alert to investment opportunities such as those that claim to prevent, detect, or cure COVID-19.

## TRAINING WITH INTERNAL AUDIT

Unsure what to do when you receive an audit recommendation? No worries, this audit training video provides tips on what to do and what to avoid when writing a solid response.

Have a look at our Conflict of Interest Examples and learn more about situations where a conflict of interest may, or may not, arise or exist.

## IN THE NEWS

"How to Work from Home without Losing Your Mind" – Brian Barrett – wired.com

"A Guide to Managing your Newly Remote Workers" – Barbara Z. Laron, Susan R. Vroman, & Erin E Makarius: Harvard Business Review

## INTERNAL AUDIT HOTLINE

www.cwu.edu/internal-audit/hotline

## FREQUENTLY ASKED QUESTIONS

**Q:** When should I make an online report to the Internal Audit Hotline?

**A:** Some examples of situations that you may want to report to the Hotline:

- Conflict of Interest
- Fraud/Theft
- Financial Policy Violations

**Q:** What happens when I make a Hotline report?

**A:** We review all hotline submissions and assess each one before deciding how to proceed. Once received, your report will be handled discretely and treated confidentially to the extent possible under applicable laws.

**Q:** Do I have to give my name when I make a report to the Hotline?

**A:** No, you can remain anonymous.

**Q:** What about retaliation for making the report?

**A:** University policy prohibits retaliation against employees who in good faith report apparent violations.

**Q:** How do I start a hotline report?

**A:** Report a concern using the hotline web form.


## CONTACT INFORMATION

**Jesus Baldovinos**
Internal Audit Manager
400 E University Way
Ellensburg WA 98926
Barge Hall, Room 311
Office: 509-963-1911
Fax: 509-963-2025
Email: Jesus.Baldovinos@cwu.edu
www.cwu.edu/internal-audit