University of Connecticut
Office of Audit, Compliance and Ethics

Compliance Chats Podcast
Topic: Phishing Attacks: Don't Let Them Reel You In!

Podcast Title:	Phishing Attacks: Don't Let Them Reel You In!	**Podcast Date:**	4/26/17
Host:	Omar Andujar	**Guest Speaker(s):**	Jason Pufahl
Purpose	In this interview with Jason Pufahl, listeners will learn about common red flags associated with phishing attacks and strategies for detecting and protecting against such attacks.		
About Guest Speaker	Jason Pufahl is the Chief Information Security Officer for the University of Connecticut. He has over 20 years of infrastructure and information security experience and has spent the last 10 years dedicated to information security and privacy. He has responsibility for information security for the institution, encompassing security awareness and training, disaster recovery, risk management, identity management, security policy and regulatory compliance, security analytics, and controls implementation.		

TRANSCRIPT OF INTERVIEW

INTRO:

OMAR: Hello and welcome back to Compliance Chats a new podcast series intended to keep Faculty and Staff up-to-date on various compliance matters.

I am Omar Andujar with OACE, and today I am joined by Jason Pufahl, the University's Chief Information Security Officer. We are here to speak about a very important topic… Phishing…

SAMPLE INTERVIEW QUESTIONS:

OMAR: Jason, can you tell our audience what is phishing and why is this topic so relevant to all of us here at the UConn community?

JASON: Phishing is the practice of sending fraudulent emails purporting to be from reputable companies or trusted individuals in order to induce people to reveal personal information, such as passwords and credit card numbers. Phishing is a major contributor to security threats such as computer virus infections, data loss and identity theft.

Specifically:

- Phishing is the #1 way to deliver Ransomware
- Phishing is the #1 way to deliver Malware
- 30% of phishing emails get opened and Criminals are developing much more sophisticated techniques for convincing users their email is legitimate.

OMAR: It sounds like Phishing attacks can present in a number of different ways, can you describe some red flags that can help us identify a potential phishing attack?

JASON: We posted an email of the recent w-2 phishing attack on the UConn security site at security.uconn.edu as an example. That email contains a common set of markers that can assist in identifying phishing. It's also an example of a phishing email that was designed and distributed by professional cyber criminals.

Taking a quick look at the email we see the following:

- The From address looks like it is coming from UConn payroll, but the real information displayed in parenthesis clearly shows it is not from a UConn email address
- Hovering over the core-ct link shows a URL that isn't associated with UConn or the State of CT
- The signature is generic, UConn payroll or any other official office is going to provide a signature of a responsible individual
- The phone number is generic, again you should expect dedicated contact information

These are not all of the indicators, but they are certainly common one. If the email doesn't feel right, maybe due to other markers like spelling or grammar, please feel free to reach out to the UITS help center or security office.

OMAR: Can you describe how you protect us from these attacks, how the threat landscape has changed and how we can report a phishing attack?

JASON: The University is able to detect and block >90% of the phishing that is delivered to the University. We utilize spam prevention software that is well-regarded in the industry that maintains a database of current threats that is continually updated. The challenge we face is primarily related to phishing campaigns that are targeted at the University, often small or very targeted populations that include financial functions. In those cases we are the first to see the attack and the spam prevention system often cannot benefit from information curated from other sources.

If you someone receives a phishing email please forward it to reportphishing@uconn.edu. Remember, it's phishing spelled **phishing.** Once we received reports we will evaluate it, block access to any URL's the email may contain, remove the mail from any mailboxes it has been delivered to, report the phish to the vendor and begin our investigation process to determine if anyone succumbed to the phish.

OMAR: What would someone do if they opened a phishing email or clicked a link? What if they are concerned that they disclosed their NetID password or perhaps some other personally identifiable information like social security number?

JASON: It's helpful if you contact the UITS HelpCenter if you have clicked on a phishing link, it's very possible that malware has been downloaded or installed. If you have inadvertently provided your NetID password it's extremely important that you let the security office know and that you change your password. The security office can assist in determining if any University of CT resources have been accessed with your NetID/Password. In certain cases, for example in the w-2 incident where the intention of the phish is to gain access to w-2 information, the security office may have other recommendations that can help protect you against future identity issues.

However, there are some precautions you can take to reduce the risk of a phishing attempt being successful and to protect not just your UConn account information but account and personal information that you may have available online.

OMAR: I'm sure that some specific examples of that would be helpful, would you mind going into some additional detail?

JASON: Common techniques include:

- Utilize Long/complex passwords
    - Passphrases often work well for this, as they are easier for you to remember and typically long.

- Individual passwords for each company/website
    - Remember, companies have security threats just like UConn and can sometimes be compromised. If you use a unique password for each company you do business with, like your bank or social media accounts, then a breach at one company does not put any of your other data at risk
- Password managers
    - Of course, managing all your passwords is challenging, and impossible to do without storing them somewhere. There are many password managers online that can make this task extremely easy, and greatly increase your security. Lastpass and 1password are a couple, but googling password manager will provide a variety of choices.
- Two factor Authentication
    - Finally, many sites like your bank or email provider will provide two-factor capabilities. These systems are the best mechanism to protect your data, but do introduce an additional step into the login process. Many companies provide these capabilities for your account. UConn is also evaluating places where this may be effective.

OMAR: Jason, thank you for walking us through the common red flags associated with potential phishing attacks and sharing strategies for protecting ourselves from such attacks. That is all the time we have for today, thanks again for joining us today.

RESOURCES MENTIONED BY TODAY'S SPEAKER:

Information Security Office Website: www.security.uconn.edu

W-2 Phishing Scam Alert: http://security.uconn.edu/2017/02/14/0214-w2-phishing-scam-alert/

Always be on Alert for Phishing Attacks: http://security.uconn.edu/be-on-alert-for-phishing/

MUSIC CREDITS:

Mining by Moonlight. Kevin MacLeod. Royalty Free 2012. Retrieved from: https://incompetech.com/music/royaltyfree/music.html