# Transcript: IT Podcast - Ep 111 - C836 Lesson 8 - with Arthur Moore and Jessica Galterio

*The following transcript is a verbatim account of the video or audio file accompanying this transcript.*

Speaker # 1: Arthur Moore

WGU's IT Audio Series, flexible, portable, profound.

Hey, this is Arthur with WGU. I'm one of the course instructors for C836, fundamentals of information security. Just as a reminder, this series is there to enhance the learning resources, not to replace the learning resources. Let's go ahead and jump into it. Humans, the weak leak. Feel how you want to about this topic, and there is a saying in opposite that every solution is 10 percent technical and 90 percent training.

The end user will always be the point of compromise in any system and insert random IT security joke here about the end users. But at the end of the day, without end users, we would not have employment nor with this web series be available. Even though our end users are the weakest leak and the easiest point of contact for a breach, we still need to educate, train, and increase their awareness of a security situation.

Security awareness is the knowledge and the attention shown by users with physical, logical, and administrative controls. Protecting data, regardless of the industry in which we operate, we will always have a need to protect data in some variety. As we have covered in lesson 6, there are numerous laws and regulation that govern data, and compliance with them is one of the cost of doing business. These compliance laws are HIPAA, GLBA, FISMA, PCI, DSS, COPA, FERPA, and the list goes on and on. Passwords. Always enforce certain levels of password strength at least eight characters, at least one uppercase, one lowercase, one symbol, and one number. This would produce a password of capital P, at symbol, lowercase s, lowercase s, w, 0, r, d. The key is to balance the complexity of the password with the importance of what is being protected.

Eight characters is probably fine for a site that stores family photos but not recommended for a bank account. What that goes into saying is eight character minimum with complexity was the norm when we had dial-up modems. I would recommend going 10 characters or more today, depending on what type of data you're storing and using. What's that complexity is called camel casing when we actually use lowercase letters and uppercase letters to create the passwords that we're using. Ten plus characters with the complexity, special characters, numbers, and camel casing. Social engineering, one of my favorite topics. Social engineering is a technique that refers to the willingness of people to help others and particularly when the target is faced with someone that appears to be in the stress, intimidating, or someone that we wouldn't normally expect to see in a given situation. In shorter terms, social engineering is lying to manipulate somebody's good nature. Pretexting is when we assume the guise of a manager, customer, reporter, or even a coworker's family member. Using a fake identity, we create a believable scenario that elicits the target to give a sensitive information or perform an action that they normally would not do for a stranger. Phishing is a particular social engineering technique and is largely employed through the use of electronic communications such as email, texting, phone calls. Most phishing attacks are very broad in nature and involve convincing a potential victim to click on email in order to send the victim to a fake site designed to collect personal information, credentials, or had the victim install malware on the system. Tailgating, also known as piggybacking, is what we think of when we hear the term you use quite simply. It's the act of following somebody into a building beyond a control point without having a proper credentials, badge, or key that they would normally use to enter. I'm going to go back and talk a little bit more about phishing. Phishing attempts are really easy to spot and you can hover over the link.

If the link is in all sorts of characters and it's not from your bank or somewhere known with the known good URL, don't click on it. Just hover over the link and you can actually see where it goes. Tailgating. Now, here's a very good method for tailgating. I'm not endorsing this, but this is what I've heard. You should not use any of these techniques unless you are authorized. That is my warning to you.

If you are looking to perform a physical penetration test, you can tailgate someone. Just hold up a cake, donuts, balloons, whatever come in with your arms full and people will naturally open a door for you or try to get the door for you. Not checking to see if you have your ID badge and not checking and see if you're there, but assuming that you might be a delivery person or someone or someone in the office is having a party or some gathering and they just want to help you.

There's a good tailgating technique that, again, I don't endorse you using unless you have permission.

Network usage and admin policies. Network usage or, perhaps more accurately, network awareness is the important concept to discuss with users. It is certainly the case today with a large number of users having access to multiple networks, both wired and wireless, from relatively restricted networks in the workplace to wide open networks such as in the homes, coffee shops, or airports. Malware is any application that makes an unauthorized change to a device.

Malware can come from many sources, but most commonly email. We just touched on that with phishing in the previous slide. Personal equipment. Bringing your own device, BYOD. Use of a personal device which brings cost savings to the organization, but can open up certain risks such as data leakage, malware, and intellectual property issues. Forgive me there. Clean desk is a policy that sensitive information should not be left out on a desk and should not be unattended for a significant amount of time such as leaving for the day or going to lunch. This is typically followed up with a discussion on how sensitive data on physical media such as paper, tape, should be disposed of, and needs to be done properly, namely shredding bins, destruction devices, media shredders, and so on. Just from my personal experience being in health care and dealing with HIPAA, most of the people that I worked actually had a small shred bin under their desk. Once they would get done with that PHI, they would put it underneath the desk. Before they went on their 15-minute break or went to lunch, they would just go ahead and dump it into the shredder or shred bin. That is a part of that clean desk policy. Now security awareness and training. We have to communicate with our users the desired information to drive the vehicle of security awareness. Through training programs in education, we build that security awareness. Let's all be honest. For security professionals, this is all very interesting to us. But for somebody who's in accounting, this is probably like watching the grass grow or watching paint dry. Let's spice it up. Let's do some gamification. Let's add certain elements to what we're doing in training.

Let's make it a competition. Let's make it some jeopardy show or Family Feud type setup. Let's make it fun for our users because this is not their bread and butter, this is not their cup of tea. We're hired in the organization to build the security awareness and train. We also want to do giveaways: pins, coffee mugs, newsletters.

Gift cards really make great giveaways. A five dollar gift card to your favorite coffee shop or restaurant would really get your attention for whatever the game is trying to mention. Food, food, food. I can't stress this enough. People are more willing to receive information from any event as long as there is somebody that has catered the event. If you have to sit through a computer-based training for an hour and some change, more than likely you're going to end up for getting that information by the time you hit Submit. But if you go to a catering event where there is food, you're more engaged because, number 1, you're not hungry. When you add hunger into those situations, adult attention span goes out the window. That's why whenever you have, let's say you have a vendor that comes to your job, they're always offering to buy lunch.

Because they know if you get people with food and they're sitting down and talking, they are more likely to receive the information that you have to give to them. Ineffective means of communication. Mass email, just shooting out the email. This is what you need to do to make sure you're completing your security awareness training. Annual-based computer training. Death by PowerPoint and I put in outside trainers. The reason why I put in outside trainers is when you're an employee of a company and this particular company pays somebody, bring somebody in to train you on something else, that's revenue that they could have spent on the actual catering of the event, gamifying the event, and save money. A lot of end users look down upon outside trainers compared to those internal trainings and catered event.

With this, I'm going to bring this session to a close. This has been Arthur Moore with C836. I appreciate your time and have a nice day. Schedule time with your course instructor to explore more deeply. WGU, a new kind of you.