

Secure Software Engineering Lab

Lab 6: Human Factors in Cybersecurity

Institute of Software Security (E-22)

1. Objectives

Apply the knowledge acquired in the lectures on the following areas of software security:

- Identification of human vulnerabilities.
- Elaboration of user-centered countermeasures.
- Privacy-enhancing technologies for behavior change.

2. Motivational scenario

You are the project manager of a company “XYZ GmbH” that is about to start its transition into the Metaverse. Concerned about the cybersecurity threats of this new technology, you decide to conduct a human vulnerability assessment to determine how prone are your employees to become victims of social engineering attacks. Particularly, you are worried about the security and privacy of your executive board members Alice, Bob, Sam, and Lily:

- **Alice** is a very sociable person and enjoys involving her friends in different fun activities. She values dependability a lot. Family is of utmost importance to Alice. She enjoys having habits and routines to depend upon because this gives her a sense of stability and predictability. Sometimes she needs guidance and rules to have a sense of order. Maintaining the status quo is important to her, and she often becomes involved in civic duties, government branches, and community organization. She prefers solid facts over abstract theories.
- **Bob** enjoys spending time with other people and has excellent interpersonal skills. He is very spontaneous and likes to focus on the present rather than plan ahead. When solving problems, he trusts his prior experiences and puts trust in his own ability to come up with a solution. Often times, he likes to put himself in other people’s shoes before making decisions. At times, Bob can be very impulsive and he is often the first person to try new rides in an amusement park or try out new adventure sports.
- **Sam** is very quick witted and is known for his good people skills. Sam likes to pay attention to things like patterns and impressions to think about possibilities and abstract theories. However he imposes logic and order to make sense of ideas obtained from his observations. Sam finds routines and schedules unbearable and gets easily bored. He loves to find excitement in his life and wants to express creative freedom in his work. Sometimes he suffers from lack of focus when he does repetitive tasks.

Summer Semester 2022

- **Lily** is a quiet, reserved and thoughtful person. She likes to explore what-ifs and possibilities through ideas formed from insights and imaginations. She likes to break down larger problems or ideas and understand how the individual components fit and function together. She is pretty open, flexible and adaptable. Even though she is a little shy, she can be an outgoing person when she is surrounded by familiar people. She loves to bond over deep conversations and shared passions.

3. Tasks

- 1. Classify the executive employees using the BMTI personality types.**
- 2. Assessment of human vulnerabilities.**
 - The Metaverse includes a Virtual Reality (VR) e-mail app.
 - Consider the phishing emails included in the Appendix.
 - Determine which of them may be more effective against Alice, Bob, Sam and Lily.
 - Justify your findings by mapping the attacker tactics with the personality types.
- 3. Identify suitable (all purpose) countermeasures for preventing phishing attacks.**
- 4. Elaborate personalized countermeasures**
 - Consider now the Westin privacy attitudes (*pragmatist, unconcerned, fundamentalist*).
 - Consider Cialdini's principles of persuasion (*reciprocity, scarcity, authority, commitment, liking, consensus*).
 - Elaborate persuasive prompts for each privacy attitude to promote the use of privacy countermeasures.

4. Materials

Case study, lecture slides, lab slides, phishing e-mails.

Appendix - Phishing E-mails

Subject #1: Apple FaceTime Information Disclosure

Dear User,

A vulnerability has been identified in the Apple FaceTime mobile applications that allow an attacker to record calls and videos from your mobile device without your knowledge. We have created a website for all the citizens to verify if their videos and calls have been made public. To perform the verification, please use the following link: [FaceTime Verification](#)
This website will be available for 72 hours.

Sincerely, National Security Department

Subject #2: Support Ukraine #StandWithUkraine

Dear Employee,

Ukraine is staying strong, our army is fighting back and our enemy is suffering heavy losses. What YOU can do — join protests, raise awareness and push the EU into more serious actions. Missiles are landing literally within a few hundred km from the EU border. One protest is happening today between 12:00 - 16:00 in the center square where thousands of people are taking part. Not everyone can go, so you can do something else:

1. Unsubscribe from all the enemy media.
2. Donate money to an organization that directly supports Ukrainian army:

http://pay.foondey.com/api/*****

Sincerely, Human Resources Team XYZ GmbH

Subject #3: Sports and Activities Club

Dear Employee,

As a part of the new health and fitness initiative, our company is starting a new Sports and Activities club exclusively for the employees. We also offer beginner courses for various sports events for a discounted price. To register to this club please follow the link given below:

http://staff.sports&activities.com/register/*****

The first 20 applicants will be rewarded with a special bonus for the first three months.

Kind Regards, Sports and Activities Club, XYZ GmbH

Subject #4: Verify your PayPal account

Dear User,

We recently have determined that different computers have logged into your PayPal account, and multiple password failures were present before the login. One of our Customer Service employees has already tried to telephonically reach you. As our employee did not manage to reach you, this email has been sent to your notice. Therefore your account has been temporarily suspended. We need you to confirm your identity in order to regain full privileges of your account. If this is not completed by July 1, 2022, we reserve the right to terminate all privileges of your account indefinitely, as it may have been used for fraudulent purposes. To confirm your identity please follow the link below:

<http://paypal.com.login-user1616.info/webscr.php?cmd=LogIn>

We thank you for your cooperation in this matter.

Kind Regards, PayPal - Customer Service Team