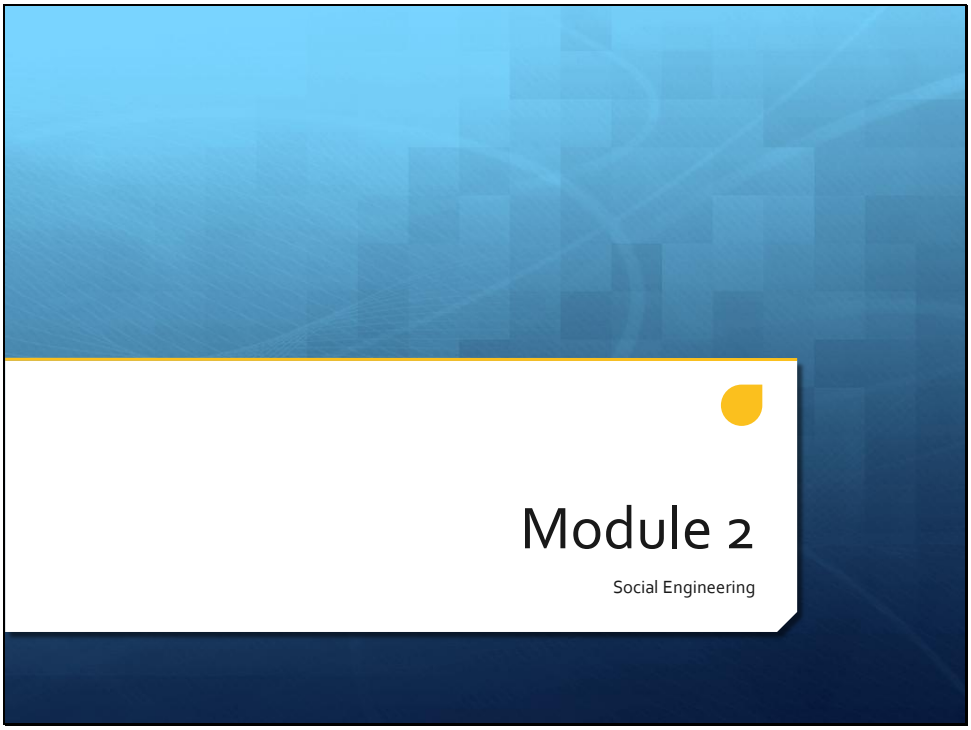
# Security Awareness

# Module 02 – Social Engineering

WORKBOOK

Slide 1

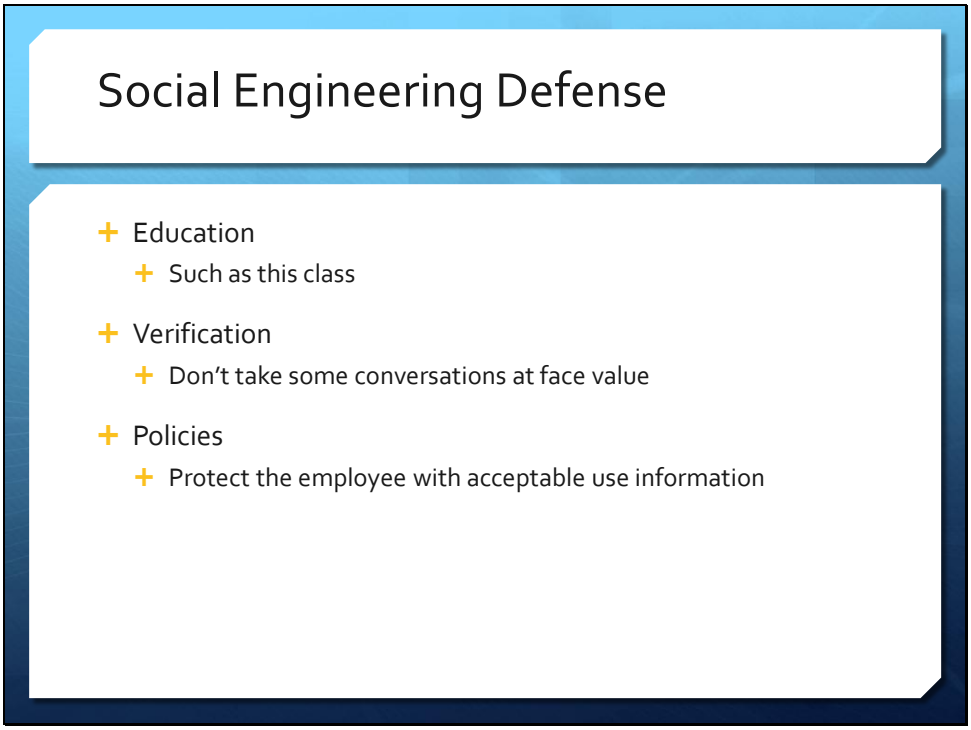


Slide 2

# What is Social Engineering?

- First, this is at least half of most hacks
  - Kevin Mitnick
  - Taking advantage of trust
- How social engineering is done
  - Shoulder surfing
  - Impersonation
  - Phishing
  - Phones
  - Eavesdropping
  - Dumpster diving

Slide 3

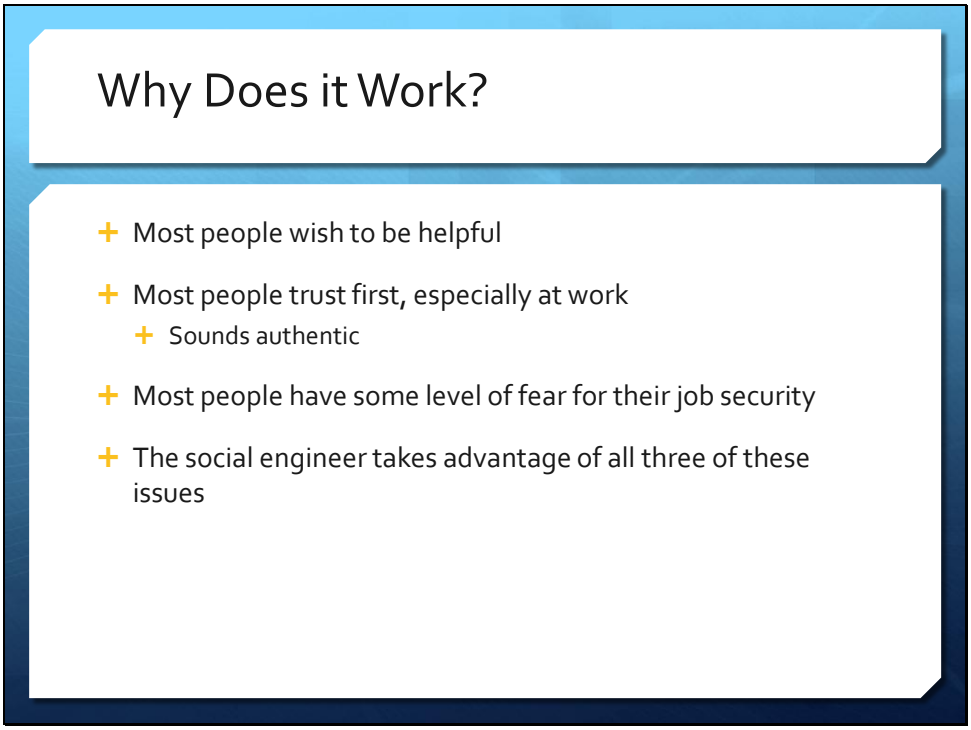

Social Engineering Defense
Education
Such as this class
Verification
Don't take some conversations at face value
Policies
Protect the employee with acceptable use information

Slide 4

# Manipulation

- Taking advantage of trust
- Taking advantage of fear
- Just being nice
- Impersonation
  - Officials
  - Directors
  - Contractors

Slide 5

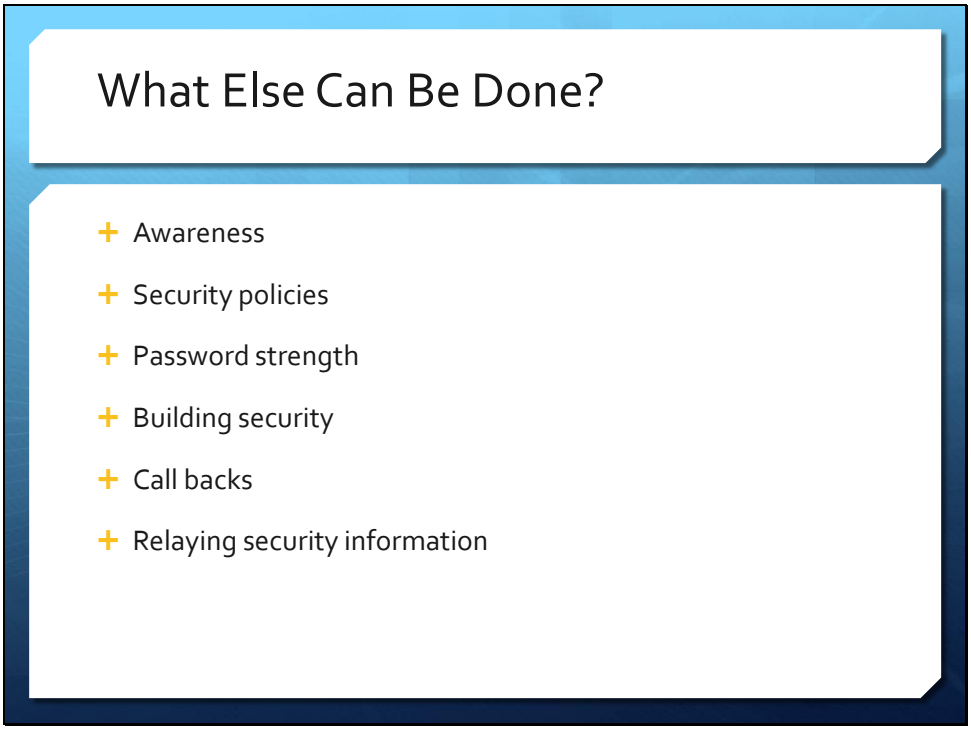

Why Does it Work?
Most people wish to be helpful
Most people trust first, especially at work
Sounds authentic
Most people have some level of fear for their job security
The social engineer takes advantage of all three of these issues

Slide 6

# Fooling People

- Phishing
- Pharming
- Winning a prize
- Web attacks
  - Back to pharming
  - Misspelled URLs

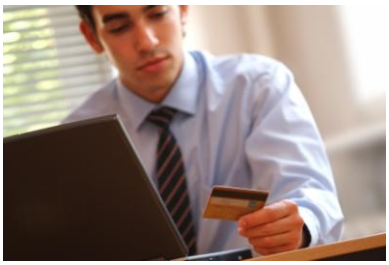
Slide 7


What Else Can Be Done?
Awareness
Security policies
Password strength
Building security
Call backs
Relaying security information

Slide 8

# Personal Precautions

- Credit/ATM card use
  - Is the Internet safe for e-commerce?
  - Is the restaurant safe?
  - Is the grocery store safe?



# Questions and Answers

## Review Questions:

1. What method do hackers use more than 50% of the time to help them in hacking?
    A. Digital decryption
    B. Wiretaps
    C. Network captures
    D. Social engineering

2. Which method of social engineering would be described as watching someone enter their password?
    A. Shoulder surfing
    B. Impersonation
    C. Phishing
    D. Eavesdropping

3. Which method of social engineering would be described as sending a forged e-mail to a victim in an attempt to gather that person's information?
    A. Shoulder surfing
    B. Impersonation
    C. Phishing
    D. Eavesdropping

4. How can you best stop a hacker from gaining information through dumpster diving?
    A. Shred all documents
    B. Don't print out important documents
    C. Place guards at the dumpsters
    D. Have each user take their paperwork home

5. Which of the following can help mitigate the risk of social engineering? (Choose all that apply)
    A. Education
    B. Policies
    C. Private offices
    D. Paperless systems

6. Which of the following do social engineers take advantage of? (Choose all that apply)
    A. Trust
    B. Fear
    C. Stupidity
    D. Impersonation

7. Social engineers may send fake e-mail (often impersonating another website) for the purpose of getting a user to believe the spoof, then stealing their login information. This process is known as what?
    A. Pharming
    B. Phishing
    C. Dumpster diving
    D. Impersonation

8. True or False: A misspelled URL will not cause a problem for an end user, because it will automatically be sent to the real targeted URL.
    A. True
    B. False

9. Which would be better for a more secure password?
    A. Longer password (15 or more characters)
    B. Complex password

10. What can be done to deter a social engineer who attacks over the phone?
    A. Call backs
    B. Verification
    C. Awareness
    D. All of the above

## Answer Key:

1. D
   Social engineering is used in the vast majority of hacks. It's the easiest and most effective way to find the information needed to either break into a building or a network.

2. A
   Shoulder surfing is basically looking over someone's shoulder while they are typing in their password.

3. C
   Phishing involves sending a fake e-mail to a victim. For example, pretending to be that person's bank. In an effort to get that victim to login with their credentials, the e-mail will include a link to a fake site setup by the hacker to resemble a real site (like an online banking site) and tell the victim they need to login to check/change something, thus capturing their credentials to use against them later.

4. A
   Destruction of all important paper documents, such as shredding, would be best practice to keep someone from stealing that data from a garbage can.

5. A, B
   Making people aware of what the dangers of social engineering are, as well as having policies to let people feel protected by their actions, will mitigate the risk of social engineering.

6. A, B, D
   A good social engineer will take advantage of a person's trust, fear, and do so at times through the impersonation of other people.

7. B
   Phishing (like fishing for information) is this attack.

8. B
   False. A misspelled URL will usually go to a hacker's site without knowing that they've navigated elsewhere.

9. A
   Because of the types of reverse hashing available, a longer password is almost always going to have a more difficult reverse-hash lookup.

10. D
    All of these defenses can mitigate a phone-based social engineering attack.