codeforfolsom

A cybersecurity boot camp organized by YELLOW CIRCLE

Social Engineering

Session 6

YELLOW CIRCLE INC
PO Box 2383
Elk Grove, CA 95759-2383

Teacher Lesson Plan

Session Name:

Social Engineering

Summary:

This course will help learners to identify and protect against social engineering attacks via social media, email, text, and other communication channels.

Time Allotment:

75 minutes

Learning Objectives:

- *Describe social engineering*
- *Identify ways in which personal information can be harvested from social media*
- *Identify ways to protect personal information posted on social media*
- *Define phishing*
- *Identify clues that a communication is either genuine or suspicious*
- *Identify actions to take if a phishing attack occurs*

Supplies:

- *Scrap paper / notepad to take notes*
- *Digital Footprint Worksheet (print)*
- *Profiler Practice Worksheet (print)*
- *Laptop / computer with Internet access for research activities (optional)*

Learning Activities:

- **(2 - 5 minutes) - Teacher Introduction**

Introduce yourself to students if you are new to the classroom. If you are continuing from a previous session, start with welcome back.

- **(2 - 5 minutes) - Volunteers Introduction**

  Introduce any new volunteers that might be present. Teachers will be provided with a quick bio of each volunteer who are helping in the classroom. Only new volunteers need to be introduced.

- **(5 minutes) - Session overview**

  Social engineering is the non-technical cracking of information security (IS). It applies deception for the sole purpose of gathering information, fraud or system access. (https://www.techopedia.com/definition/4115/social-engineering)

  The more information available, the greater the potential for social engineering

- **(5 minutes) - Video : What is Social Engineering**

  https://www.youtube.com/watch_popup?v=CLinev3eNc8

- **(3-5 minutes) - Counting Connections**

  Social Media: Counting Connections

  - *How often do you check social media each day?*
  - *How often do you post on social media?*
  - *What social media services do you use?*
  - *Which ones do you use most often?*
  - *How many people (friends or followers) are you connected to on each service?*
  - *How many more people are they connected to?*

  Questions on Connections

  - *Is it possible to be too connected?*

- **(5-10 minutes) - Student Activity : Digital Footprint**

  "What's Your Digital Footprint?" (Digital-Footprint-Worksheet)

  - *Have learners complete the assessment and use the rating system to see the size of their digital footprints*
  - *Are you comfortable with the size of your digital footprint?*
  - *What can you do to reduce it?*
  - *Open Discussion to segue into 2 main topics of course*
    - *Share Smart*
    - *Fakes and Phishing*

- **(2 minutes) - Share Smart Introduction**

  Often times, information we share can make us vulnerable to Social Engineering attacks.

- **(8-10 minutes) - Video : 6 Degrees of Information**

  Explain to students that the researcher was able to find so much information about the teens in the video because they left a lot of digital footprints (e.g. linked accounts, accounts that share email addresses or profile pictures, posts that included personal information, etc.).

  https://www.youtube.com/watch_popup?v=GYHbanR3EiU

- **(3-5 minutes) - Share Smart**

  Social Media Data Sources - Identify ways information can be found on social media.

  - *Pictures*
  - *Posts*
  - *Location Tags*

- *Friend Tags/Accounts*
- *Connected Accounts*

Discovering Personal Information - Identify what types of personal data can be found.

- *Location/Vacation*
- *Hobbies & Interests*
- *Personal Details (DOB, Schools, Work)*
- *Secondary Info (Info about friends and family)*

Protecting Personal Information - Identify ways to protect this information

- *Customize social media privacy settings*
- *Make decisions about each item you share (use post security controls)*
- *Make decisions about how much profile information to provide*
- *Check the background of your photos*
- *Other ideas?*

- **(10-15 minutes) - Student activity : Profiler Practice**
  - *Review the sample posts from 3 people*
  - *Identify personal data that can be determined from the posts*
  - *What could they (and you) do to help protect their personal data?*
- **(2 minutes) - Fakes & Phishing Introduction**

  Phishing is an attempt to obtain financial or other confidential information from Internet users, typically by sending an email that looks as if it is from a legitimate

organization, usually a financial institution, but contains a link to a fake website that replicates the real one - http://www.dictionary.com/browse/phishing

- **(3-5 minutes) - Video : Fakes & Phishing**

  https://www.youtube.com/watch_popup?v=FZp4mBtJBNQ

- **(5-10 minutes) - Fakes & Phisting Introduction**

  What is this phishing?

  - *Phishing is an attempt to steal login credentials or other private information by impersonating a trusted source*
  - *Phishing can happen via email, text, or almost any other form of communication (including phone calls and in person)*
  - *Even if you don't provide information, opening an infected attachment in a phishing email may infect your computer and result in data theft or loss*

  Some things to look for:

  - *Is the URL spelled correctly?*
  - *Do the links in the text match the hover over link?*
  - *Does the top level domain match what you would expect?*
  - *Is all of the contact information accurate and specific?*
  - *Is the text well formatted and professional?*

  More things to look for:

  - *Does the site have a secure certificate?*
  - *https://*
  - *Valid Certificate*
  - *Review Secure Connection Window*

- *Review Certificate Window*

Worst Case Scenario - What to do if you take the bait:

- *DO NOT PANIC - Knowing there is a problem is the first step in solving it.*
- *Inform a responsible adult right away - fast action can minimize risk of harm*
- *Change passwords*
- *If you think your contact or friend information has been taken, let friends know so they can be on the lookout*
- *Report it to appropriate service providers*

- **(15 minutes) - Student Activity : Find the phishing**

Owl Cinema Email – Real or Fake? - Real

- *How can you tell? – Header address is what one would expect. Email does not ask for personal information. Suggests going to site (but does not provide a link) to check and update info.*
- *A phishing email would likely have provided a link to a "cloned" website to try and steal login credentials.*

Internaut Mail Login – Real or Fake? - Fake

- *How can you tell? – No SSL, URL uses numbers in place of some letters (trivia what is one name for this? 1337 "leet")*

Robin Loxley Email – Real or Fake? - Fake

- *How can you tell? – "Offer" too good to be true, asks for personal details*

Internaut Account Verification – Real or Fake? – Fake

- *How can you tell? – No SSL, URL domain is very different from other internaut URLs, Asks for info without providing any (usually, verifications that ask for your email will provide a partial email that you must complete like*
- *J****@I********.com to challenge John@internaut.com)*

- **(2 minutes) - Session Feedback**
  - *Have volunteers distribute feedback form to students, and give them few minutes to fill out the survey.*
  - *Volunteers to collect feedback forms and save them for event manager.*
- **(2 minutes) - What's next?**

  Inform students to head back to cafeteria for lunch, and remind them to use restroom before next session starts.