TECHNOLOGY CAMP

DAY 1 : CYBER SECURITY

Identity & Social Engineering

Session 2

Session Name:

Identity & Social Engineering

Summary:

Internet has grown and changed in ways that are very different from earlier versions. The Internet is fundamentally insecure. Your real identity and online identity may be vulnerable to outside sources. However, there are some simple things you can do to protect yourself and your information. This course will help learners to identify and protect against social engineering attacks via social media, email, text, and other communication channels.

Time Allotment:

65 minutes

Learning Objectives:

- *Define Identity (Personal & Virtual)*
- *Identity Theft*
- *How to secure your Identity*
- *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:

- **(3 minutes) - Session overview**

  Your real identity and online identity may be vulnerable to outside sources. However, there are some simple things you can do to protect yourself and your information. This course will help learners to understand the importance of protecting our real and digital identities and discuss ways to protect against social engineering attacks via social media, email, text, and other communication channels.

- **(3 minutes) - Personal Identity / Real Identity**
  - *Legal name of a person - First Name + Last Name*
  - *Social Security Number*
  - *Home address / phone number*
  - *Biometrics - height, weight, gender, color of eyes, color of hair*
  - *Identity documents - SSN card, Drivers' License, Passport, Birth Certificate, Vehicle Title, Property Deed, Credit cards*

- **(2 minutes) - Video: Kaspersky Lab / Don't Become a Victim of ID Theft**

  https://www.youtube.com/watch?v=Fztuohj3Fck

- **(5 minutes) - Virtual Identity**

  Internet identity or Internet persona - is a social identity that an Internet user establishes in online communities and websites. It can also be considered as an actively constructed presentation of oneself. Although some people choose to use their real names online, some Internet users prefer to be anonymous, identifying themselves by means of pseudonyms, which reveal varying amounts of personally *identifiable information. An online identity may even be determined by a user's relationship to a certain social group they are a part of online. Some can even be deceptive about their identity.*

Some examples include:

- *Instagram username*
- *Email account*
- *Twitter handle*
- *SnapChat account name*
- *XBOX / PlayStation - GamerTag*

- **(3 minutes) - Video : Manage Your Online Reputation**

  https://www.youtube.com/watch?v=w7qEbPVw3hA

  Discuss geo-tagging (ask students)

- **(3 minutes) – Catfishing / Impersonation**
  - *Explain Catfishing / Impersonation - is a way for a user to create a fake online profile, sometimes with fake photos and information*
  - *Catfishing / Impersonation – can be a means in itself or used as a tool of social engineering attack*

- **(1 minutes) – What is Social Engineering**

  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*

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

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

- **(8 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

- **(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?*

- **(3 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?*

- **(1 minutes) - Fakes & Phishing Definition**

  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 minutes) - Video : Fakes & Phishing**

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

- **(5 minutes) - Fakes & Phishing Discussion**

  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*

- **(10 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)*

- **(1 minutes) - What's next?**

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