

Lab 1: introduction to security & your online footprint

Lab 1: Social Engineering on Social Networking Sites (your online footprint)



CSCI 415: Computer and Network Security

Dr. Nazi Hardy

Adapted from Computer Security: Principles and Practice, Stallings and Lawrie

Lab 1: introduction to security & your online footprint

Lab 1: Social Engineering on Social Networking Sites (your online footprint)

- Social networks have become the norm in the last 2 years – so new that they are not part of the most cited published security statistics. However they pose a unique and potential hazardous risk to us all with far reaching impacts (personal and professional). As an avid “social networker”, I am not discouraging their use – however, it is important to cognizant of the risks.
- **Objectives of the Lab 1:** 1) to be aware of daily security threats in our lives and to illustrate that 2) the strongest security measures are no match to human ignorance/ impulses and 3) how individual security is connected to organizational/ personal security 4) how lax we all are about online security 5) how age, profession, gender, political and marital status etc. have little to do with security intelligence, and 6) that people are unwittingly vulnerable to information and/or identity attacks.
- **Outcomes:** understanding that security does begin on an individual level and that many of us are not secure online.
- Total: 20 points

CSCI 415: Computer and Network Security

Dr. Nazi Hardy

Adapted from Computer Security: Principles and Practice, Stallings and Lawrie

Lab 1: introduction to security & your online footprint

Lab 1: Social Engineering on Social Networking Sites (your online footprint)

1. How long have you been using computers? (years)
2. Are you confident about the level of your confidentiality online? (Y/N)
3. What are the chances that your personal information is easily available online? (high, moderate, low)
4. Why? (briefly explain no. 3)

5. With respect to any social networking site (e.g. Blogger, FB, MS), is your profile restricted to a network or to only friends or other?
6. What is a means via which people outside your network or friends can have knowledge of what you write online?
7. Are people able to see your list of friends? (Y/N)
8. Briefly describe what is the danger or safety feature of no. 7?
9. In the "info" section, what information about you can be used against you and how?
10. What photos do you have online?
11. Who is able to access these photos? Would a potential employer or relative or significant other or ex be able to find and use any posted information/ photos on you?

12. What is the value (or disturbance) of twittering or revealing "what is on your mind?"
13. What are 2 obvious security flaws to social networking?
14. Please describe a brief social engineering scenario involving information (text and or photographic) that could potentially hurt a person (no names please). I expect a creative and interesting example here.

15. Differences between viruses and worms (1 line)
16. List 3 freely available hacking/ spy/ malicious software (name and website)

Lab 1: introduction to security & your online footprint

Format for Labs

Your Name
Lab #
Date
CSCI 415, Dr. Nazli Hardy