**Kovrigin** **CTP 103**

# Lab 11: Information Assurance and Security (31 points)

Objectives:

* Identify methods for securing hardware, software and information.
* Explain the effect of password length on the ability to crack a password
* Use password cracking software
* Describe the importance of solid password strategies

##### Section I – Personal Security – 20 points

**Read** the following [ITRC Fact Sheet on Social Networking & ID Theft](http://www.idtheftcenter.org/Fact-Sheets/fs-138.html).

1. **(5 points) Evaluate** how safe you are using [PC Perfect Information Quiz](http://www.idtheftcenter.org/artman2/publish/c_theft_test/Fact_Sheet_118_PC_Perfect_-_information_Safety_Quiz.shtml). Enter your answer, then the points associated with your answers according to the scoring provided. Add up your numbers to arrive at a total.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **PC Perfect Information Quiz** | | | | | |
| **Question #** | **Answer** | **Points** | **Question #** | **Answer** | **Points** |
| 1 | No | 1 | 11 | Yes | 1 |
| 2 | Yes | 1 | 12 | No | 1 |
| 3 | Yes | 1 | 13 | Yes | 1 |
| 4 | No | 1 | 14 | No | 1 |
| 5 | Yes | 1 | 15 | No | 1 |
| 6 | Yes | 1 | 16 | Yes | 1 |
| 7 | Yes | 1 | 17 | No | 1 |
| 8 | Yes | 1 | 18 | No | 1 |
| 9 | Yes | 1 | 19 | No | 1 |
| 10 | yes | 1 | 20 | yes | 1 |
| **Total** | | | | | **20** |

1. **(5 points) Evaluate** if you are at risk for identity theft using the questionnaire: [Are You at Risk for Identity Theft?](http://www.idtheftcenter.org/index.php/Fact-Sheets/fs-101.html) Enter your total score for each category below.

|  |  |
| --- | --- |
| **Are You at Risk for Identity Theft?** | |
|  | Score |
| Document Disposal | 28 |
| Social Security Number Protection | 15 |
| Information Handling | 28 |
| Scams | 23 |
| **Total** | 94 |

Evaluation - Using the work in Section I, provide answers to the following questions: 10 points (1 point each)

1. What was your score on the **PC Perfect Information Safety Quiz**? My score was a perfect 20/20. I good at keeping my computer and information safe.
   1. Evaluate your score. Are there actions you should take or behavior you should change to ensure your safety? If so what are they? I’m already taking all the precautions necessary to keep my info and computer safe.
2. What was your score on the **Are you at risk of identity theft** questionnaire? 94/100. Savvy about identity theft risks. The only one I missed was having a copy of a social security card in my wallet with parts of the ssn being cut out.
3. Evaluate your score. Are there actions you should take or behavior you should change to protect your identity? If so what are they? Im pretty proactive and careful at this time and do not need to take any steps.
4. What are some do’s and don’ts for creating secure passwords? Don’t use easily guessed passwords such as birthdates, use a mix of uppercase and lowercase characters, do use punctuations marks and special characters such as #.
5. How can you avoid phishing attempts? Verify a sites security, install anti-phishing toolbar, think before clicking on something, keep informed about phishing techniques, keep your browser up to date, use firewalls, never give out personal information, use anti virus software.
6. What you can do to protect yourself when purchasing items online? Optimize your PC’s Security settings, use a credit card instead of debit card, print or save a copy of your orders, use strong password, check your statement often.
7. What can you do at home to protect yourself from malware? Back up your computer, use a firewall, use a pop-up blocker, minimize downloads, use a antivirus software, don’t click links within emails.
8. List some things you can do specifically protect yourself from Identity Theft: Order credit report, use secure email, destroy private records and statements, safeguard your ssn.
9. What is considered Personally Identifiable Information (PII) that could be used to distinguish or trace an individual’s identity? PII refers to personal information such as name, phone number, birth date, ssn, email , username and passwords.
10. What are some steps you should take to ensure e-mail safety? Choose safe email password, recognize and avoid phishing attempts, turn on 2 step verification .
11. What are some “don’ts” when using work provided e-mail? Don’t click on links within emails

##### Section II – Secure Passwords – 12 points

Determine length of time needed to crack a password Be sure to use the capitalization in the password example. **6 points (1 point each)** Open a browser and navigate to: <https://howsecureismypassword.net/>

|  |  |
| --- | --- |
| **Password** | **How long would it take to crack it?** |
| 1. qwerty | instantly |
| 1. AACC2019 | 1 minute |
| 1. ILikePie | 22 mintes |
| 1. ILikePie@ | 1 week |
| 1. ILikePie@Home | 434 Thousand years |
| 1. ILikePie@H0me (use zero instead of the letter o) | 3 million years |

Identify 3 main points about passwords that you learned from this assignment? **6 points (1 point each)**

1. They need to be easy to remember
2. Should not be stored in an easily accessible place.
3. They should be alphanumeric with upper and lower case. Strong passwords.

##### Section III – Password Policies – 23 points

Read the following Microsoft documentation about Password Policy: <https://technet.microsoft.com/en-us/library/hh994572(v=ws.11).aspx>. Use the links at the bottom of the page to answer the following:

**Enforce Password History**

1. What does this setting determine: Determines the number of unique new passwords that must be associated with a user account before an old password can be reused
2. What are the possible values for this policy? 0 to 24
3. What do “Best Practices” recommend that this setting be set at? Set Enforce password history to 24. Set Maximum password age to 60 days. Configure minimum password age to not allow passwords to be changed immediately.

**Maximum Password Age**

1. What does this setting determine: time in days before a password needs to be changed.
2. What are the possible values for this policy? 0 to 999
3. What do “Best Practices” recommend that this setting be set at? Set maximum password age to 60 days.

**Minimum Password Age**

1. What does this setting determine: determines the amount of time that a password can be used before the system requires the user to change it
2. What are the possible values for this policy? 0 to 998
3. What do “Best Practices” recommend that this setting be set at? Set to 1 day so that a user cannot change password immediately

**Minimum Password Length**

1. What does this setting determine: Determines the least number of characters that can make up a password for a user account.
2. What are the possible values for this policy? 0 to 14
3. What do “Best Practices” recommend that this setting be set at? Set minimum password length value to 14 characters.

**Password Complexity Requirements**

Enabling this policy requires passwords to meet the following requirements:

1. Passwords cannot contain the users samAccountName(account name) or displayName (full name value)

Passwords contain characters from three of the following categories:

1. Uppercase letters of European languages
2. Lowercase letters of European languages
3. Base 10 digits (0 through 9)
4. Nonalphanumeric characters
5. Any Unicode character that is categorized as an alphabetic character but is not uppercase or lowercase.

##### Lab 11 Submission Instructions

1. Make sure you have entered your name and section number at the top of the document.
2. Save the document as **LastName\_Lab11.docx**, replacing LastName with YOUR last name.
3. Submit the assignment to the lab dropbox in Canvas by the due date.