Topic: Passwords   **Date:** _____

Trainer Checklist

Task	Date Completed
1. Print Trainee Checklist, fill in employee names.	
2. Review objective and training materials on passwords web page at **https://sites.google.com/site/kissatisat/topics/passwords**.	
3. Choose one or more methods for employees to learn about passwords.	
4. Communicate requirement to employees to complete training.	
5. Verify employees can create strong passwords, know not to share them, and know to change passwords periodically.	
6. Document employee progress on Trainee Checklist and/or ISA Training Checklist.	

Topic: Passwords_____   Date: _____

Trainee List

Employee Name	Supervisor/Department	Trainer Initials
1.		
2.		
3.		
4.		
5.		
6.		
7.		
8.		
9.		
10.		
11.		
12.		
13.		
14.		
15.		
16.		
17.		
18.		
19.		
20.		
21.		
22.		
23.		
24.		
25.		

Topic: **Passwords**_____   Date: _____

Lesson Plan

Objective: Demonstrate knowledge of secure password management

Require individual user accounts for each employee on business computers and for business applications

1. Every employee should have an individual login account.

2. Employees should not be logged in as administrator, to avoid harmful actions if the computer is compromised.

3. Passwords should be complex, including a combination of upper/lower case, numbers, and punctuation, and at least 8-10 characters long. Passwords should be changed every 3 months.

4. Login IDs and passwords should not be shared

Source: *Small business information security workbook, version 2.2*. Lincke, 2011.

Teaching tip: The two most important areas to focus on are the importance of frequent password changes and selecting a strong password.

1. Dangers

    a. "80% of all network security problems are caused by bad passwords" (Mellor & Noyes, 2005).

    b. Bad passwords can allow intruders access to your financial information and the possible theft of your identity.

2. Passwords should contain:

    a. At least 8 characters

    b. Upper and lowercase letters

    c. Numbers

    d. Special characters such as: ! @ # ,) (

3. Methods to remember extremely strong passwords:

    a. Turn a full sentence into a password.

        i. Example: **17 y**ears **a**go**, I w**ent **t**o **I**taly translates into `17ya,IwtI`

        ii. Example: **M**y **l**ittle **s**ister **t**urned **7 t**his July**!** translates into `Mlst7tJ!`

    b. A password should be guarded with the utmost care and never divulged to anybody.

4. 25 Worst Passwords on the Internet

1. password
2. 123456
3. 12345678
4. qwerty
5. abc123
6. monkey
7. 1234567
8. letmein
9. trustno1
10. dragon
11. baseball
12. 111111
13. iloveyou
14. master
15. sunshine
16. ashley
17. bailey
18. passw0rd (The "O" is a zero here)
19. shadow
20. 123123
21. 654321
22. superman
23. qazwsx
24. Michael
25. football

5. Activity "Check your password - is it strong?"
    https://www.microsoft.com/security/pc-security/password-checker.aspx

Discussion point: A simple password such as "Idaho" can be broken in less than two minutes. On the other hand, a more complex password, such as "Mlst7tJ!" would (theoretically) take almost 2,000 years to break (Mellor & Noyes, 2005).

Note: The material contained in this lesson plan was adapted from the case study "Awareness and Accountability in Information Security Training" (Mellor & Noyes, 2005) and used with permission.

Lessons

Title	URL	Duration	Use
InfraGard Awareness Information Security Awareness Training Course – Lesson 4 Passwords	https://www.infragardawareness.com	9 Minutes, 23 Seconds	☐
Microsoft Digital Literacy, Computer Security and Privacy Course, Guidelines for Protecting Your Computer Topic	http://www.microsoft.com/about/corporatecitizenship/citizenship/giving/programs/up/digitalliteracy/eng/curriculum3.mspx		☐

How To

- Check Your Password - Is It strong? https://www.microsoft.com/security/pc-security/password-checker.aspx

- Choosing Your Password - http://securingourecity.org/resources/pdf/choosing_your_password.pdf

- Create Strong Passwords - http://www.microsoft.com/security/online-privacy/passwords-create.aspx

Policy Templates

- Password Protection Policy – http://www.sans.org/security-resources/policies/computer.php

Posters

- Different Passwords - http://www.stopthinkconnect.org/download/galleries/16/data/image.jpg

- Safe Passwords - http://www.stopthinkconnect.org/download/galleries/18/data/image.jpg

- Strong Passwords - http://www.stopthinkconnect.org/download/galleries/15/data/image.jpg

Tutorials

- Password Protect Your Computer in Windows XP - http://www.onguardonline.gov/media/video-0012-password-protect-your-computer-windows-xp

Videos

Source: Creating a Secure Password - SOeC & FBI Cybersecurity Tips
http://www.youtube.com/watch?v=lTvElkejKTs, Length: 2 Minutes, 31 Seconds