codeforgrove

CYBER SECURITY BOOT CAMP

Authentication

Session 3

Sponsored by:

ca technologies

intel

KOVARUS Integrated IT Expertise

SMUD

CALIFORNIA COMMUNITY COLLEGES Doing What MATTERS™ FOR JOBS AND THE ECONOMY

ISSE SERVICES

YELLOW CIRCLE

YELLOW CIRCLE INC
PO Box 2383
Elk Grove California 95759-2383

Teacher Lesson Plan

Authentication

Session Name:

Authentication

Summary:

The way a computer understands who it is interacting with. There are three common factors used for authentication: Something you know (such as a password), something you have (such as a smart card or secret token), something you are (such as a fingerprint or other biometric method).

Similar to buying a lock to protect your things in your locker at school, you need a lock to protect your Cyber Identity with Authentication.

Time Allotment:

75 minutes

Learning Objectives:

- What is authentication, and process involved
- Multi-factor authentication
- Importance of strong passwords
- New generation of authentication methods (biometrics)

Supplies:

- Scrap paper / notepad to take notes
- Top worst passwords worksheet (print)
- Laptop / computer with Internet access to research topic of selected project

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) - Volunteer Introductions

  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

  Passwords are the way we access the majority of our information and online accounts. The passwords we use are often weak in a way that would allow hackers to guess them or we use the same password on multiple accounts.

  If one of those accounts is compromised, then our password to other sites is exposed. E-mail is one of the most-used forms of communication. How secure are the systems that we use daily and what are the implications of insecure systems?

- (13 minutes) - Video : Cybersecurity Crash Course

  https://youtu.be/bPVaOlJ6ln0

- (5 minutes) - What is authentication?

  Authentication is the process of determining whether someone or something is, in fact, who or what it is declared to be. It is a process in which the credentials provided are compared to those on file in a database of authorized users' information on a local operating system or within an authentication server. If the credentials match, the process is completed and the user is granted authorization for access.

- (5 minutes) - Class Discussions
  - *How does two-factor authentication make you safer online?*
  - *What are potential problems with two-factor passwords?*
  - *What would I tell my friends or family to do to make their passwords more secure?*

- (18 minutes) - Video: What's Wrong with your pas$$w0rd?

  https://www.ted.com/talks/lorrie_faith_cranor_what_s_wrong_with_your_pa_w0rd

  Teacher can pause the video few times to let students soak in a slide, specifically the one with quilted passwords.

- (5 minutes) -Student Activity: How secure is my password?

  Have volunteers pass top worst passwords sheet

  In groups or as individuals, students can practice password selection.

  https://howsecureismypassword.net/

- (5-10 minutes) - Activity review feedback

  Discuss activity with students

  What makes password more secure?

- (5-10 minutes) - Student Assessment

  Opportunity to assess student learning with short-response discussion questions summarizing best practices or cybersecurity stories.

- (2 minutes) - Session Feedback

  Have volunteers distribute feedback form to students, and give them a 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 snack break, and remind them to use restroom before next session starts.

The top worst passwords

1. 123456
2. password
3. 12345678
4. qwerty
5. 12345
6. 123456789
7. letmein
8. 1234567
9. football
10. iloveyou
11. admin
12. welcome
13. monkey
14. login
15. abc123
16. startwars
17. 123123
18. dragon
19. passw0rd
20. master
21. hello
22. freedom
23. whatever
24. qazwsx
25. Trustno1

Having a good password is very important. If it is easy to guess or a word from the dictionary, then a hacker can easily crack it. The most common password is “123456”. Do not have that password or any password that you see in the list above. They are all too easy!You must be able to remember your password. You must not write it down!

Use this website to test your password: https://howsecureismypassword.net/

Tips for a good password:

- Your password should be 8-12 characters long
- Do not use your name or words in the dictionary like school
- Have lower and upper case letters like ahTjow
- Have letters and numbers like oP87sDbU
- Use symbols like @#$%()*?!
- The best passwords are like this: 8fG$lwR56#