Identifying Yourself

TRAINER RESOURCE

This document is a reference and preparation sheet for the trainer, and a companion to the lesson plan.

The Learning Objectives summarize the knowledge that learners should have gained by the time they reach the end of the module.

The Background and Detail for Trainer provides greater details on the content, and links to references. It will allow trainers to learn more about the topic so they can lead discussions or answer questions confidently without being limited to the classroom content. Each item in the Background supports a section in the Lesson Script.

Learning objectives

> An understanding of the security aspects of authentication and passwords

> An understanding of how to choose a good password

> Ability to create a strong password

Background and Detail for Trainer

1 Authentication (Who am I?)

1.1 In Brief

Passwords help to prove your identity online. Good passwords make it possible to uniquely prove who you are, without someone else being able to pretend to be you. They are unique, random, long and secret but still memorable.

1.2 In Detail

- Authentication
  - Sometimes you want to identify yourself as the unique person that you are. This might be for the convenience of obtaining customized services or the confidence that a service (such as access to bank funds) is only available to you.
    - You can convince others of who you are with a unique item, such as a card or a key, by a unique biological feature such as a fingerprint or by knowing a secret.
      - All these methods have strengths and weaknesses.
  - Two-factor Authentication
    - Two-factor Authentication (2FA) tries to overcome weaknesses of just one way of identifying yourself by requiring two components that operate independently and avoid a common point of compromise.
      - This could be something physical that you have and something that you know.
      - Common examples are smart cards and login number generators such as the RSA SecurID, and Yubikeys.[1]
      - You need to prove yourself in two ways before you can log in or use a service.
        - For example, when you withdraw money from an ATM, you need to enter a PIN (personal identification number) and insert your card.
        - On the Internet, your password is like a PIN. It is a secret that only you know, so 2FA combines your password with something else only you have, such as a phone number or a unique device.
      - Someone else needs to do the same if they are pretending to be you.
    - SMS Code
      - A code is sent to your mobile device as a text message (SMS – Short Message Service). When you receive the code, you enter it in the field provided and the login proceeds.

1 For more detail see: https://nakedsecurity.sophos.com/2014/11/14/understanding-the-options-2fa/

    - Authenticator apps
        - Authenticator apps perform the same type of service as the SMS code but instead of the login codes being sent to you, they are generated locally on your smartphone or tablet.
- Passwords
    - Currently, passwords are the least worst option for most of the Internet and the main way of proving who you are.[2]
        - Passwords are sometimes referred to as passphrases.
            - Passphrases differ from passwords only in length.
                - Passwords are usually short, six to ten characters.
                - Passphrases are usually much longer; typically 20 to 40 characters, sometimes more.
        - Passphrases are considered better for encrypted things because they are longer and take much more time to guess.
        - Encrypted things are often sent into a public environment where criminals could copy them and have many attempts to guess the passphrase.
        - Using a very long password means they will have to spend more time trying different options.
    - Criminals can get passwords by:
        - Gathering enough information about you to guess your password;
        - Tricking you into revealing your usernames and/or password;
        - Capturing your passwords, e.g., by looking over your shoulder or with spyware;
        - Cracking passwords using a software program that makes many guesses;
        - Capturing usernames and passwords from one service, and attempting to use them on other services.

- Bad habits
    - Reusing passwords
        - We have so many accounts, it is has become difficult to remember all the passwords. Some of the ways we try to make this easier work against us.[3]
            - Reusing passwords has direct security implications as leaks at one website can compromise security at another.

2 An in-depth review of 35 proposed password alternatives using a framework of 25 comparison criteria found no proposal beats passwords on all front.

3 Many people cope with the large number of accounts by reusing password, sometimes with slight modification; for example, a 2007 telemetry study estimated the average person has 25 password-protected accounts but only six unique passwords

    - Concentrate on never reusing passwords for important accounts (bank, email etc.).
    - Don't worry as much about your many accounts of little value to an attacker; (i.e. no personal information or financial assets on the account).

- Forgetting Passwords
    - You can write down passwords for use at home.
        - Written-down passwords kept in a safe location not available to others are quite safe from most of the ways that people steal passwords.
        - It is not a good idea to stick passwords on your computer or on the computer desk, but a non-descript book in a drawer is quite safe.
        - Be aware that banks and other financial institutions may consider that if you write your password down or keep a poorly disguised record of it you are contributing to possible unauthorized use of their system. Check with your bank before keeping a written record.
    - The suggestion to write down your passwords does not apply for a shared computer or in an office environment where people you don't know have access to the computer and the desk.
- Bad or weak passwords
    - Computer experts love to warn people against bad or weak passwords.
        - A weak password is one that a person or machine can guess easily.
        - Weak passwords include:
            - Names of family members or pets, or significant personal dates.
                - For example, felix56 is a bad password because everyone knows your cat's name is Felix and you were born in 1956.
            - Key combinations that are easier to type.
                - For example; 1234, 123456, aaaa, qwerty, are all very obvious passwords, because these words are in the lists used by password guessing programs.
            - Dictionary words of common short phrases.
                - For example; password, iloveyou, Mississippi and sesquipedalian are all in the dictionary and in the list of words guessed by password-guessing programs.
            - Password sequences
                - Even if you have not reused the exact same password, attackers can guess small variations.

        - For example, changing the number at the end of your password does not make it as good as a new password.
    - A computer program is more likely to be doing the guessing than humans. Outsmarting machines is different. Something that seems complex to a human may not be so to a computer.
    - Words that are difficult to spell are not more secure.
    - Rare or obscure words are not more secure.
    - A word that nobody would associate with you is not more secure.
    - The program will have more trouble with misspelt words.
- The program will have more trouble with a random combination of words (without a sentence structure).
    - It is very difficult to give an example of a good password because they are unique, random and secret. Once you give out a password, it isn't secret anymore and becomes a bad password.
    - The criteria for a good password are:
        - Complexity; the more types of letters or characters that it uses (letters, capitals, numbers, punctuation), the better.
        - Uniqueness; the probability that the particular combination of characters has never existed anywhere else.
        - Randomness; the probability that the combination will not exist anywhere else.
        - Entropy; the difficulty of guessing the password by trying all possible combinations (basically length).
        - Memorability: the ease of remembering the password.
        - Usability: you should be able to type the password into the computer using the available keyboard without errors.
            - Unfortunately the last two criteria compete with the other requirements.
            - We need to strike a balance between them in order to have a password that is good because we can remember it, and good because it is strong.

1.3 In Practice

DO consider two-factor authentication.

DO make conscious decisions about security when choosing passwords.

2 Mnemonic Passwords

2.1 In Brief

Phrases can be easier to remember than complex passwords. Take advantage of this by using a phrase to remember a password.

2.2 In Detail

- Mnemonics (memory aid)
  - Choose a password that is hard to guess but easy for you to remember by abbreviating a memorable phrase:
    - Think of a memorable sentence or phrase containing at least ten words or more. It doesn't matter what this phrase is about, just that you find it easy to remember.
    - A phrase that is obscure or unique is better.
    - Select a letter, number or special character to represent each word in your password. A common method is to use the first letter of every word.
    - Ideally, choose a mix of lower-case and upper-case letters, numbers, punctuation, and special characters (such as ^ or %).
    - Use punctuation where it makes sense to you and is easy to remember; use '&' instead of 'and', '?' where there is a question, etc. or substitute numbers for letters ('E' = 3) or combine numbers and letters over the syllables (2day).
    - Remember the phrase.
  - You can devise your own way of doing this—as long as you remember your method, so you can remember your password.
    - Examples:

Phrase	***Password***
I love to ski with Derek at Banff in winter	Il2swD@Biw
Purple Haze all in my brain. Excuse me, while I kiss the sky.	PHaimb.Em,w1kts.
Don't make me repeat myself twice.	D'tmmrm2ice.D'tmmrm2ice.

2.3 In Practice

DO use mnemonics to make passwords that are both memorable and strong.

3 The Diceware Method

3.1 In Brief

The Diceware method can create a password that is random, unique, long, and memorable by using dice rolls to choose words from a list to make a password.

3.2 In Detail

- Longer passwords are more secure than shorter passwords
- A long phrase from a book or song would be easy to remember, but would be easier to guess because it follows a set of rules (grammar and syntax).
- Although a very long string of random letters would probably be best, it would also be very hard to remember.
- A string of random words would be very long and still difficult to guess.
- A computer-generated string of random letters would not be completely random because computers follow a set of instructions that could be duplicated.
- Humans are not very good at being random either. We tend to be predictable even when trying not to be.
- Dice are designed to be random and are very good at it.
- The Diceware method uses dice and a list of words to come up with a truly random collection of words to make a passphrase.
    - The randomness of the phrase makes it hard to guess as it defies standard syntax and grammar rules.
    - The Diceware list is a list of numbers and words. Here is a short excerpt:

16655 clause	16656 claw
16661 clay	16662 clean
16663 clear	16664 cleat
16665 cleft	16666 clerk
21111 cliche	21112 click
21113 cliff	21114 climb
21115 clime	21116 cling
21121 clink	21122 clint
21123 clio	21124 clip
21125 clive	21126 cloak
21131 clock	

- To use the Diceware method:
  - Download the complete Diceware list[4] or the alternative Beale list[5] and save it on your computer. Print it out if you like.
  - Decide how many words you want in your passphrase. You can use four, five, six or more. The more words, the better the passphrase.
  - Roll the dice and write down the results. Write the numbers in groups of five.
    - Make as many of these five-digit groups as you want words in your passphrase.
    - You can roll one die five times or roll five dice once, or any combination.
    - If you roll several dice at a time, read the dice from left to right.
  - Look up each five-digit number in the Diceware list and find the word next to it. For example, 21124 means your next passphrase word would be "clip" (see the excerpt from the list above).
  - When you are done, the words that you have found are your new passphrase.
- Some people try to connect the words in the phrase to make it easier to remember.
- There is no harm in writing it down on paper stored in a secure location.[6]
  - Example Diceware Passphrases
    - Rolling 36424,51644,64134, 54236 produces leekricowhiteskat
    - Rolling 33142,53132,14323,65622,53112,56456 produces nscaldblatz64savetardy

3.3 In Practice

DO use the Diceware method to create passwords that are long and memorable.

4 Password Managers

4.1 In Brief

Password managers are programs that remember passwords for you.

4.2 In Detail

- One solution to the problems of passwords is password managers.
  - They are programs that manage your passwords for you.

4 Download at: http://world.std.com/%7Ereinhold/dicewarewordlist.pdf
5 Available at: http://world.std.com/%7Ereinhold/beale.wordlist.asc
6 For more information: http://world.std.com/~reinhold/diceware.html

    - They can work by requiring one password to gain access to all of your passwords
    - They can work by using an easy-to-remember password to unlock a stronger password that is then used for the service.
    - They may also generate site-specific passwords that depend partially on the domain name of the site (protecting against some phishing attacks).

- Password managers exist in different formats: stand-alone applications (e.g., Site Password, browser plug-ins, and bookmarklets).
- As always, look for these applications at reputable sites such as Offline Retailers, the iTunes Store or Google Play to avoid downloading poor software or malware.
- Some banks and financial institutions may consider the use of a password manager as writing down a passphrase and contributing to an authorized access. Check with your bank before deciding to use a password manager.
- Password managers don't "travel" well.
    - They may not be available on every device when you need a given password—leaving you stuck trying to remember the password or waiting until you have access to the manager again.
- A solution to this is Cloud based password managers.
    - They are more portable.
    - They are less secure because the passwords are stored in the cloud.

4.3 In Practice

DO consider password managers if you access many accounts frequently.

Glossary of Terms

Diceware method	A method of creating long random passphrases using dice and a word list.
Encryption	A process of converting information to a form unreadable to untrusted parties that still contains the original information and is able to be read by the intended recipient.
Mnemonic	A system or pattern of ideas or associations which assists in remembering something.
Passphrase	A phrase used to identify a person as it is only known to them.
Password	A word used to identify a person as it is only known to them.
Password manager	An application that assists in managing passwords.
Phishing	A fraudulent practice or pretending to be a from a reputable company in order to induce people to give their personal information (a contraction of Phone fishing).
PIN	A Personal Identification Number, a secret code used to identify a person, usually for a bank transaction.
Smart card	A card with an integrated computer chip in it.
SMS code	A code is sent to your mobile device as a text message (SMS – Short Message Service) as part of an identification process.
Two-factor authentication	A system for identifying a person that uses two components that operate independently and avoid a common point of compromise.
Username	A unique name given to a computer system or service user. Used together with a password it can identify an individual.