### Time Estimate: 45 minutes

**1. Cyber Security and User Authentication**



Cyber Security is one of the fastest growing IT fields. It is essential to every organization to keep their computer systems and data safe.

Passwords are currently the primary way to protect devices and information from unauthorized access. A **strong password** is something that is easy for a user to remember but would be difficult for someone else to guess based on knowledge of that user. In Unit 5, we saw that it is very difficult to guess a long complex password (which can be tested in sites such as [https://howsecureismypassword.net](https://howsecureismypassword.net/)). Luckily, brute-force password cracking algorithms take exponential time. However, passwords can also be compromised (stolen) through phishing attacks and data breaches.

Many organizations now use **two-factor authentication (2FA)** or **multi-factor authentication (MFA)** which asks for additional authentication in addition to the password, just in case the password gets compromised. Users are asked to present several separate pieces of evidence such as:

| **Something You Know Something You Have Something You Are** |
| --- |

* **Something You Know**: for example your password or the answers to security questions that you have set up;
* **Something You Have**: for example a code texted to the user’s phone or a USB security token;
* **Something You Are:** for example **biometrics** such as fingerprints or face recognition.

Multi-factor authentication requires at least two steps to unlock protected information. Each step adds a new layer of security that must be broken to gain unauthorized access. Watch the following [video](https://www.youtube.com/watch?v=0mvCeNsTa1g) on multi-factor authentication:

[](https://www.youtube.com/watch?v=0mvCeNsTa1g)

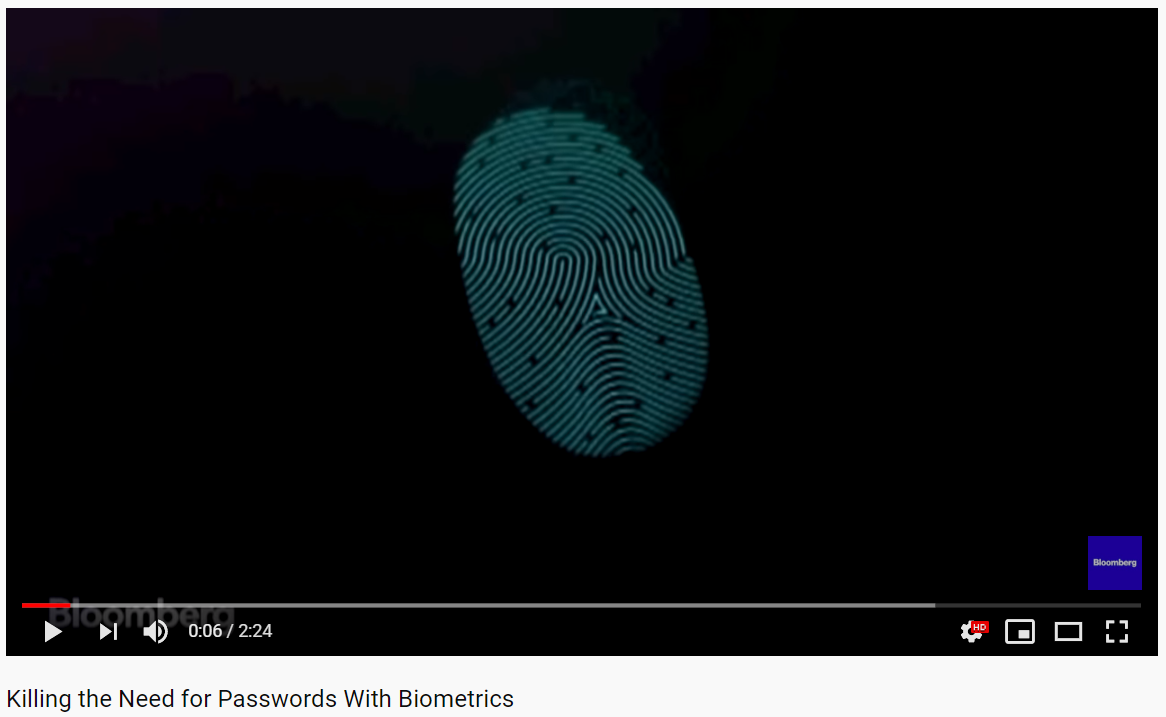
**Self-Check Exercise:** After watching the video, which of the following would NOT count as 2FA in addition to entering a password?

1. Your fingerprint
2. Entering a token that is sent to your phone
3. Entering a token that is emailed to you.
4. Entering your password twice.

**Biometric Authentication**: uses unique physical characteristics such as fingerprints for identification.

* **Discuss with your class:** What different types of biometric authentication have you seen in real life or in movies?

Biometrics became popular with fingerprint scanners, and now facial recognition technology has exploded in use for biometric authentication and surveillance. However, the problem with static biometrics like fingerprints is that if it is compromised (stolen), you can’t change your face or fingerprint to a new one. Dynamic biometrics like heartbeats or behavioral biometrics like walking gaits are more difficult to hack. Watch the following [video](https://www.youtube.com/watch?v=88Rjg8gM_DI) on biometric authentication:

[](https://www.youtube.com/watch?v=88Rjg8gM_DI)

**2. Malware**

**Malware** which stands for MALicious softWARE is software intended to damage a computing system or to take partial control over its operation. A computer **virus** is a type of malware that can copy itself and gain access to a computer in an unauthorized way. Computer viruses often attach themselves to legitimate programs and start running independently on a computer.

* **Discuss with your class:** Have you ever had a virus on your computer? What happened and how did you get rid of it?

Watch the following [video](https://www.youtube.com/watch?v=XU8PHihT_P4&ab_channel=FTCvideos) about malware:

[](https://www.youtube.com/watch?v=XU8PHihT_P4&ab_channel=FTCvideos)

Malware can spread by email attachments, downloading from sites that are not reputable, network connections from infected computers, and copying infected files from computer to computer on portable memory. So don’t click or open anything where you don’t know the source. A computer that is infected may stop working, display strange messages, delete files, be controlled by others, steal personal information and infect other computers. Recent **ransomware** attacks encrypt and lock computer systems until a ransom is paid.

Computer virus and **malware scanning software** can protect a computing system against infection. Many operating systems like Windows come with their own free malware scanners like Windows Defender. It is very important to auto-update the malware scanning software with newly discovered malware signatures. Explore the malware scanner on your computer. Regular software updates help to fix errors that would compromise a computing system. All real-world systems have errors or design flaws that can be exploited.

**3. Unauthorized Access**

Criminals can gain unauthorized access to computing systems in many ways by exploiting the users and the staff of the system. They can gain access through malware or by stealing or cracking passwords or hacking in through unprotected areas.

**Phishing** is a common technique that is used to trick a user into providing personal information usually through email. That personal information can then be used to access sensitive online resources, such as bank accounts and emails. A malicious phishing or malware link can be disguised on a web page or in an email message. Watch the following [video](https://www.youtube.com/watch?v=eWS8cYoj2oA) on phishing.

[](https://www.youtube.com/watch?v=eWS8cYoj2oA)

Another technique for capturing passwords is **keylogging** software which secretly records every keystroke made by a computer user. This can be used to gain fraudulent access to passwords and other confidential information. Keyloggers can be installed through malware or hacking. Unsolicited emails, attachments, links, and forms in emails can be used to compromise the security of a computing system. These can come from unknown senders or from known senders whose security has been compromised. Untrustworthy (often free) downloads from freeware or shareware sites can contain malware.

Unencrypted information sent over public networks can also be compromised. Data sent over public networks can be intercepted, analyzed and modified. One way that this can happen is through a rogue access point. A **rogue access point** is a wireless access point that gives unauthorized access to secure networks. Network and system administrators protect their networks with **firewalls** which provide a barrier to attacks and scan their networks with network analyzers to prevent unauthorized access.

**Investigate:**

Select one or more of the following activities to complete after watching and discussing the videos.

1. Can you spot when you’re being phished? Do the Phishing Quiz working in pairs or POGIL groups: [https://phishingquiz.withgoogle.com](https://phishingquiz.withgoogle.com/)**.** See how many you get right. Answer the following questions in your portfolio:
   1. Post a screenshot of your summary page.
   2. What did you find to be the most challenging phishing technique to spot?
2. In pairs or POGIL groups, investigate this map (<http://cybermap.kaspersky.com/> (click on a country and more details or statistics) and <http://securelist.com/statistics/> which shows the current week’s infections and attacks. Answer the following questions in your portfolio:
   1. What are the top 3 attacked countries?
   2. What country has the highest rate of infections? What is the top infection (virus) currently?
3. Investigate a famous or recent malware, hacking, or security breach incident. Answer the following questions in your portfolio:
   1. Who was involved in the incident?
   2. What happened in the incident?
   3. When did the incident occur?
   4. Where did the incident occur?
   5. How did the incident happen?
   6. What were the consequences of the incident?

**Still Curious?**

* Try <https://www.hacksplaining.com/lessons> which describe hacking exploits and how to protect against them.
* Try PBS Cyber Security Lab <https://www.pbs.org/wgbh/nova/labs/lab/cyber/> where you protect a business against attacks.
* Try a Capture the Flag event where you solve computer security challenges to capture flags. A great one for beginners is <https://picoctf.com/> designed for high school students. Here are some other resources (<https://resources.infosecinstitute.com/tools-of-trade-and-resources-to-prepare-in-a-hacker-ctf-competition-or-challenge/>)
* More Cyber Security lessons available at <https://teachingsecurity.org/>.

**Vocabulary**

* **strong password** - a password that is easy for a user to remember but would be difficult for someone else to guess based on knowledge of that user.
* **multi-factor authentication (MFA) -** users are asked to present several separate pieces of evidence involving knowledge (something they know like a password), possession (something they have like a texted code), and/or inherence (something they are like biometrics).
* **biometrics** - using unique physical characteristics such as fingerprints, face recognition, etc. for identification
* **malware-**  software intended to damage a computing system or to take partial control over its operation.
* **virus**  - a malicious program that can **copy itself** and gain access to a computer in an unauthorized way.
* **ransomware** - malware that encrypts and locks computer systems until a ransom is paid.
* **malware scanning software** - software that helps to protect a computing system against malware infections.
* **phishing -** a technique that is used to trick a user into providing personal information usually through email.
* **keylogger -** a program to record every keystroke made by a computer user.
* **rogue access point** - a wireless access point that gives unauthorized access to secure networks.
* **firewalls** - barriers that protect a network from unauthorized access

**Reflection Questions** ([Google document](https://docs.google.com/document/d/1U7_tRzo2HTZvIRMbP30bwgtMjL094GQ8cVFyZwmRpi0/edit?usp=sharing))

1. (From Activity) Which activity did you complete? Record your answers/results from the activity you completed.
2. Describe the benefits of Multi-Factor Authentication.
3. Describe a phishing attack and how to protect against it.