A Tale of Authentication

Click this link to make a copy of this handout.

Act 1: The Attack

In the vast landscape of the internet, you are a tech-savvy teenager. You navigate social media, online games, and school assignments with ease. There's a popular new gaming platform, Arcade Nexus, and you create an account so that you can play games online with your friends. Arcade Nexus asks you to create a password so that you are the only person able to access your account. A password is a form of **authentication.**

> **Authentication** is the process of identifying a user and granting them access. Authentication is proving that someone is who they say they are.

You pause for a moment and decide to use a version of your standard password: k@reL45. This password passes all of the website's password requirements: lowercase letters, uppercase letters, symbols, and numbers.

Even though Arcade Nexus says your password is strong, a hacker thinks otherwise. Hackers are pretty sophisticated these days, and they can use a variety of attacks to crack your password. Copy and paste your password into PasswordMonster's Password Test. How long does it take the hacker to crack your password?

Yikes, that is no time at all! So, the hacker gets in. They find your email address because it is associated with your Arcade Nexus account. The hacker then tries to sign in to your email account using your Arcade Nexus password. What do you know - it worked! Why? Because you use the same password for almost all of your accounts. It's easier to remember that way, right?

Now that the hacker is in your email account, they discover they can access your social media account. They send mean emails and nasty messages to everyone in your network.

Was playing games online with your friends worth all of this trouble? Let's rewind and take a look at how this could have played out differently.

Act 2: The Power of Length

One of the ways hackers can crack passwords is by using a **brute force attack.** A brute force attack is when a computer attempts all possible password combinations until it finds the correct password. Supercomputers can attempt billions of passwords per second! This means that the strongest password isn't necessarily the one with a combination of symbols, letters, and numbers, especially since most people tend to replace letters with predictable symbols (i.e. "@" for "a" or "3" for "E"). The strength of a password lies in its **length**.

> The strongest predictor of a good password is its **length**. Each additional character makes a password exponentially harder to crack.

With this in mind, you decide on a longer password: k@reLthedog45.

Copy and paste your password into PasswordMonster's Password Test. How long would it take the hacker to crack your password now? How does this compare to your previous password?

Act 3: Passphrase

Another way to approach creating your password for Arcade Nexus is to use a **passphrase.**

> A **passphrase** is a password, but it's longer. It can be a sentence or a series of words. Just like a password, it should avoid personal information and be as random as possible.

The benefit of a passphrase is that it is much easier to remember than a password. Without looking back, can you remember the longer password you chose a second ago? Was the "T" capitalized or the "L"? Did the "4" or the "5" come first?

One way to create a strong passphrase is to use a method called "Diceware." This method rolls dice to select words from a long list of words, 7776 words in fact.

With this newfound security knowledge, go to this Diceware Password Generator to generate your Arcade Nexus password. Play around with the number of dice to use, and generate multiple passphrases until you find one you like. Write your passphrase below:

Now, copy and paste your password into PasswordMonster's Password Test. How long would it take the hacker to crack your password now? How does this compare to your previous passwords?

The key to this passphrase is to develop a memorization strategy to help you remember the words. Here are a few strategies:

- Create a meaningful sentence that finds a relationship between the words
- Create an acronym with the first letter of each word
- Visualize the words as a picture or scene

In the space below, describe how you will remember the passphrase that you generated:

Act 4: Multifactor Authentication

Alright, at this point, your password is extremely strong. However, there is always the chance a hacker will get lucky and crack your password. Once they have your password, they can easily access all of your account information. That's not good.

You can add an additional layer of security by using **multifactor authentication.**

> **Multifactor authentication** is an extra layer of authentication that requires two or more factors for authentication. Typically, these factors fall into three categories: something you know (password), something you have (such as a phone), or something you are (such as your fingerprint).
>
> **Two-factor authentication (2FA)** is a subset of multifactor authentication which requires two factors of authentication.

This means that once you enter your password correctly, there is at least one additional step to ensure that you are trying to gain access to your account instead of a hacker. 2FA typically works by sending a random code to your phone via text message or app after you have correctly entered your password. Once you enter the correct code, you are granted access to your account. Some additional forms of 2FA include using a hardware token as the physical requirement or using biometric authentication,

such as a fingerprint or facial recognition. Multifactor authentication works the same way, except there are two additional factors required for authentication. For example, you may be required to enter a password, scan an ID badge, and scan your fingerprint to be granted access.

Now, when you create your Arcade Nexus account, you go to the privacy settings. You're excited to see that there is an option to enable 2FA. Naturally, you choose to enable 2FA. Now, whenever you try to log in, a random code will be sent to your phone as part of the authentication process.

How will this additional security layer impact the hacker's ability to get into your account?

Act 5: Biometric Authentication

While you are in the privacy settings of your Arcade Nexus account, you notice an option called **biometric authentication.**

> **Biometric authentication** uses an individual's physical or behavioral characteristics to verify their identity.

Some common forms of biometric authentication include fingerprints, facial recognition, iris scans, voice recognition, or palm scanning. Biometric authentication is extremely secure because a user does not have to remember a password and it is unique to the individual. One thing to note is that biometric data is sensitive and needs to be stored in a very secure way. Additionally, just like passwords, it can still be stolen or compromised.

Your phone uses your fingerprint to unlock it, so you have the option to enable biometric authentication when you log in to Arcade Nexus on your phone. Do you choose to enable this feature? Why or why not?

Act 6: Epilogue - Password Manager

As a last step in your authentication journey, you stumble across **password managers.**

Password managers attempt to make it easy to have strong, unique passwords for all of your accounts by managing your passwords for you. Instead of having to remember all of your passwords, you just have to remember the “master password” to access your password manager.

The most important benefit of a password manager is that it ensures that you have unique passwords for all of your accounts. Think about the number of accounts you have - bank accounts, social media accounts, school accounts, email accounts, online store accounts, gaming accounts, etc. - that’s a lot of accounts! Most people tend to reuse passwords even though they know it’s not very secure because it’s just impossible to keep track of so many passwords.

As you consider the potential benefits of a password manager, you remember how you use a similar password for all of your accounts - a version of k@reL45. Even though you now have a super strong passphrase that is combined with 2FA, if you use the same passphrase for multiple accounts, you’re decreasing your online security.

You don’t have to decide whether or not to use a password manager now, but if you want to learn more, check out this article from Cybernews about the security of password managers.