# Network and The Internet Cybersecurity

**K-2.NI.5** Explain why people use passwords.
**K-2.NI.6** Create patterns to communicate a message.

**3-5.NI.5** Describe physical and digital security measures for protecting personal information.
**3-5.NI.6** Create patterns to protect information from unauthorized access.

## Creating Strong Passwords

You'll need to create a password to do just about everything on the Web, from checking your email to online banking. And while it's simpler to use a short, easy-to-remember password, this can also pose serious risks to your online security. To protect yourself and your information, you'll want to use passwords that are long, strong, and difficult for someone else to guess while still keeping them relatively easy for you to remember.

## Why do I need a strong password?

At this point, you may be wondering, why do I even need a strong password anyway? The truth is that even though most websites are secure, there's always a small chance someone may try to access or steal your information. This is commonly known as hacking. A strong password is one of the best ways to defend your accounts and private information from hackers.

## Tips for creating strong passwords

A strong password is one that's easy for you to remember but difficult for others to guess. Let's take a look at some of the most important things to consider when creating a password.

- Never use personal information such as your name, birthday, user name, or email address. This type of information is often publicly available, which makes it easier for someone to guess your password.
- Use a longer password. Your password should be at least six characters long, although for extra security it should be even longer.
- Don't use the same password for each account. If someone discovers your password for one account, all of your other accounts will be vulnerable.
- Try to include numbers, symbols, and both uppercase and lowercase letters.
- Avoid using words that can be found in the dictionary. For example, swimming1 would be a weak password.

## Security measures for protecting personal information

### 1. Use Passcodes for your Devices

If you were to leave your smartphone in a coffee shop or taxi, would the person who found it be able to access what’s on it? That’s a scary scenario. Losing your smartphone is one thing, but giving the finder access to everything from your email and social media accounts to all the personal information you may have stored on the device could play havoc with your life. Make sure to use a passcode to help keep your apps, accounts, and personal information protected. Do the same for your laptops and even desktop computers.

### 2. Create strong & unique passwords.

If you have an online account with a company that suffered a data breach, ideally, that one account is your only concern. But if you use the same login credentials on other accounts, then that single breach incident could give hackers access to your other accounts, as well. That’s why it makes sense to use a unique password for each of your online accounts.

If you’re like me and have way too many sets of online credentials to commit to memory, consider using a password manager to keep track of those many, unique passwords. There are several out there with different prices and plans, but it shouldn’t take you too long to figure out which one works best for you. Just do an Internet search for “password managers” and see what suits your needs.

3. **<u>Don't overshare on social media.</u>**

   Limit social media sharing. Sharing too much on social media may put your personal information in the wrong hands. Pay attention to not only the pictures and posts you share, but also to your privacy settings, as well, so that you're limiting the number of people who can see what you're sharing.

4. **<u>Use free Wi-Fi with caution.</u>**

   You get what you pay for, right? Free public Wi-Fi is a good example. Sure, it's convenient, but in terms of security, most free public Wi-Fi networks don't offer much. That means, with the right tools, anyone else on the same Wi-Fi network could be "eavesdropping" on your online activity. Given that, would you want to log in to your bank account or enter a credit card number while on public Wi-Fi? The answer is, no!

   Even a password-protected Wi-Fi network is only as safe as the people who have the password. Save transactions for when you're on a secure network, perhaps at home. If you must log in or transact online on public Wi-Fi, use a VPN (virtual private network), which encrypts your activity so that others on the same network can't easily see what you're doing.

5. **<u>Watch out for links and attachments.</u>**

   Do not open emails or attachments that is not in your contact. Delete them immediately.

6. **<u>Check to see if the site is secure.</u>**

   A secure URL should begin with "https" rather than "http." The "s" in "https" stands for secure, which indicates that the site is using a Secure Sockets Layer (SSL) Certificate. This lets you know that all your communication and data is encrypted as it passes from your browser to the website's server

   Look for a lock icon near your browser's location field.

7. **<u>Consider additional protection.</u>**

   Use Anti-virus programs.

## Create patterns to protect information from unauthorized access

### Five Best Practices to Prevent Unauthorized Access

1. Strong Password Policy. ...
2. Two Factor Authentication (2FA) and Multifactor Authentication. ...
3. Physical Security Practices. ...
4. Monitoring User Activity. ...
5. Endpoint Security.