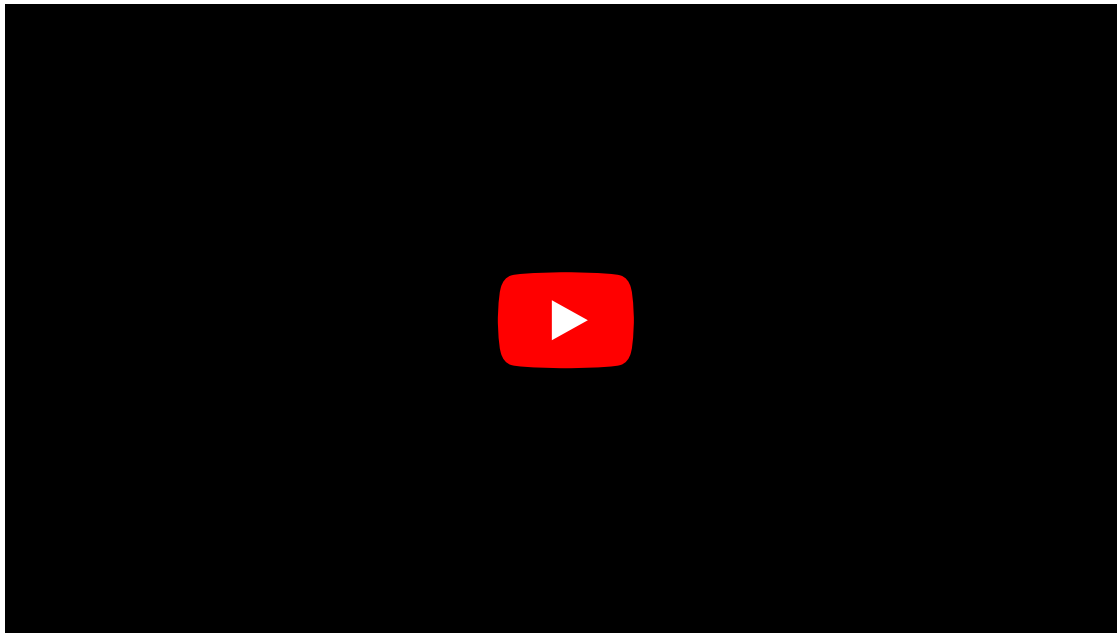# Tip 6: Internet Safety and Privacy

Text

People sometimes think of security as a technical issue, and it can be. But a big part of online safety involves simple, smart practices like selecting good passwords. You can think of your password like the code to a vault where you keep your most valuable documents and information. Make sure your password is strong and don't share it with others.

To create a strong password, use a mix of lower and upper case letters, numbers, and symbols, and make it between eight and nine characters long. Avoid using any identifiable information such as your name, address, phone number, or personal information that is easy to guess, like your pet's name, the name of your school, your favorite team, etc. Choose a different password for each of your important accounts, like your email, social network, and online banking accounts. Reusing passwords is risky. If someone figures out the password for one of your accounts, it's possible they could get access to your personal information or other online services that you use.

But how can you create a different password for each account that meets all this criteria and that's easy to remember? The answer is simple. You can create a passphrase. To create a passphrase, first think of a sentence that's easy for you to remember. For example, "I met Alice in San Francisco in 2011." Now, take the first letter of each word in the sentence and use it to create your passphrase. Where possible, convert words into symbols to make your passphrase stronger.

There you have it. You can add an extra layer of security by enabling two-factor authentication, the security process where logging into a service requires two steps. For instance, you could have to enter your password as usual, followed by a code that was texted to your phone. Two-factor authentication protects your account with something that you know, your password, and something that you have, your cell phone. This means that if someone steals or guesses your password, they still can't sign into your account because they don't have your phone.

Now you know how to sign in safely into your account. But it's equally important to know when to log out. If you're using a public or shared computer, such as a computer at a library, internet cafe, or even a friend's house, sign out of your account before leaving the computer. Otherwise, the person who uses the computer after you may have access to your account.

Great. Now let's talk about privacy and security settings. Forgetting your password or getting locked out of your account can be a frustrating experience. No one wants to lose access to their emails, documents, or photos. To make sure you can get back into your account quickly and easily, it's important to set up password recovery options. Most online services will give you the option of adding a recovery phone number or email address to your account. This way, you can receive a numeric code or link to reset your password and regain access to your account. It's important to set up your recovery options before this happens.

Take some time to explore other privacy and security settings on the online services that you use. Change your password if you suspect unusual activity in your account. And become familiar with the privacy policy, which will tell you what information about you is collected and stored and for what purposes. When using social networks, make sure to review the privacy and security settings to decide what information is visible in your profile, who can view your posts, photos, videos, or other content that you share.

Now, you know how to take care of your personal safety and your account when you're online.