InterVarsity
INTERNATIONAL STUDENT MINISTRY

Top 5 Easy Ways to Increase Your Internet Security

1. Beef Up Your Passwords

Use good passwords and change them with regularity. Without good passwords, it doesn't matter what platforms you use – they will only be as secure as your weakest password. Go here to read more on setting up good passwords. Did you know that if you use a 10-letter password with a symbol it could take up to 54 million centuries to crack your password? If you are concerned about remembering such a long password, consider using a password manager such as LastPass which works on Windows, Mac and mobile devices. This not only stores your passwords securely, but it also generates complicated passwords for you.

2. Become Hack Proof(ish)

- 2-step verification can prevent any casual attempt to hack into your documents and data. What this means is that if you enter the password for Google Drive, then Google Drive will send you a message to your phone or computer with a code. Once you enter the code, you can access your information. In this way, someone who could hack into your account by figuring out your password would also need to be in possession of your personal phone or computer.
- Client-Side Encryption can prevent the website or application host from "eavesdropping" on your written, verbal, or videoed conversation. This is encryption that you need to add and isn't provided for you. The downside is that if your account were hacked, your provider would not be able to restore your information since they would not have access to your decryption information.

3. Limit Access to Your Devices and Apps

- Password lock your computer. Many of us have passwords automatically saved in our web browsers and computers because it speeds up our day-to-day communications considerably and it is difficult to remember so many passwords. This means, however, that anyone who gains the use of your computer also has access to some of your most sensitive data. If you simply password lock your devices, you can nip this problem in the bud without losing significant convenience.
- Do not sync apps between your computer, phone, and tablet. This prevents information from leaking between devices or becoming susceptible if one device is less secure than another. When Google Drive isn't linked to your computer or phone, it can only be accessed with a password when one is on wifi. In this way, anyone who has your computer (such as a customs agent) cannot see that information or even know that it exists. If this is unrealistic for everyday purposes, consider selecting an app, such as Dropbox, which can be dedicated to just the most sensitive information. This reduces your daily inconvenience while still protecting valuable data, privacy and security.

4. Don't Break Any U.S. Laws

The U.S. cannot legally access your information unless they have reasonable proof of an action considered a crime in the U.S. For instance, if the China government were to request information about you from the U.S. because you are breaking the Chinese law regarding sharing the Gospel, the U.S. will deny the request because sharing the Gospel is not a crime in the U.S.

5. Only Browse Secure Sites

Many browsers scan the websites you browse in order to provide you with security information such as that a site contains malicious malware or tracking cookies. Symbols such as  or  will explain to you how secure a site is. When exchanging information such as credit card information or personal data, be sure to be on a site beginning with "https://" as those communications are encrypted. Otherwise, someone may be able to grab your information while in transit between your computer and the website's server.