Haekka

Lesson 6 | Securing Your Computer

Updated 2020-09-14

Securing your software accounts and your online identity, as we covered in the last lesson, is only the first aspect of your digital security. Your computer, whether you use your own or are issued one by your company, and whether you use it from home, in the office, or at a coffee shop, needs to be secured.

If an attacker gains access to your computer, they can use that access to escalate privileges or to access data stored on your computer. Even if you are using a virtual, shared hard drive, often files are stored locally.

Your company may install and run some form of endpoint protection on your computer. This software monitors your computer to detect threats or other forms of attacks, successful and unsuccessful. In most cases, these attacks can be remotely mitigated.

Your IT department may provide you with a pre-configured computer in which they are responsible for the following security services. In that case, you may not have permission to set up or configure any of the below security services. It's still a good idea to consider these for your personal computer.

- **Firewall**. A host-based firewall is a software program that runs on your computer and controls incoming and outgoing traffic. It acts as a barrier between your computer and your computer network connections. There are third-party firewalls as well as built-in firewalls for both Windows and Mac, though you need to turn them on and configure them.
- **VPN**. A common way to protect the security and privacy of your Internet and remote network connections is through a VPN. A VPN routes all of your Internet traffic through a remote server. VPNs essentially mask your identity from your Internet Service Provider, or public wifi provider if using public (coffee shop) wifi, and encrypt all traffic between you and your Internet destinations. VPNs have been in use for a long time for secure, point to point connections, like connecting to a data center or remote computer; but, more recently VPNs have been made available and easy to use for personal use - on both computers and phones. NordVPN and TunnelBear are two common VPN services that have apps for computers and mobile devices.
- **Encrypted hard drive**. If your computer is stolen, or you leave it on a plane, in an Uber, or at TSA, you want to make sure the data that is stored on the hard drive is secure. The

easiest way to do this is by encrypting your hard drive. Both Windows and Mac offer easy ways to do this.

- **Updates**. You should download and install patches and operating system installs in a timely manner. One of the most commonly exploited vulnerabilities is unpatched operating systems. It is usually best to turn on automatic notifications of updates. You can then choose when to install them.
- **Company message**. Your company may have a message that is loaded on your computer to be displayed on the login screen. Or you may want to provide a simple message on your computer stating you are the owners of the device and how it is supposed to be used. This is easy to set in both Windows and Mac.
- **Screen protector**. This is covered in the section on remote work but, suffice it to say, preventing people from reading your screen is important, especially if you travel or work in public places like coffee shops.

Your computer is one layer of defense that needs to be secured in concert with your accounts and mobile devices.