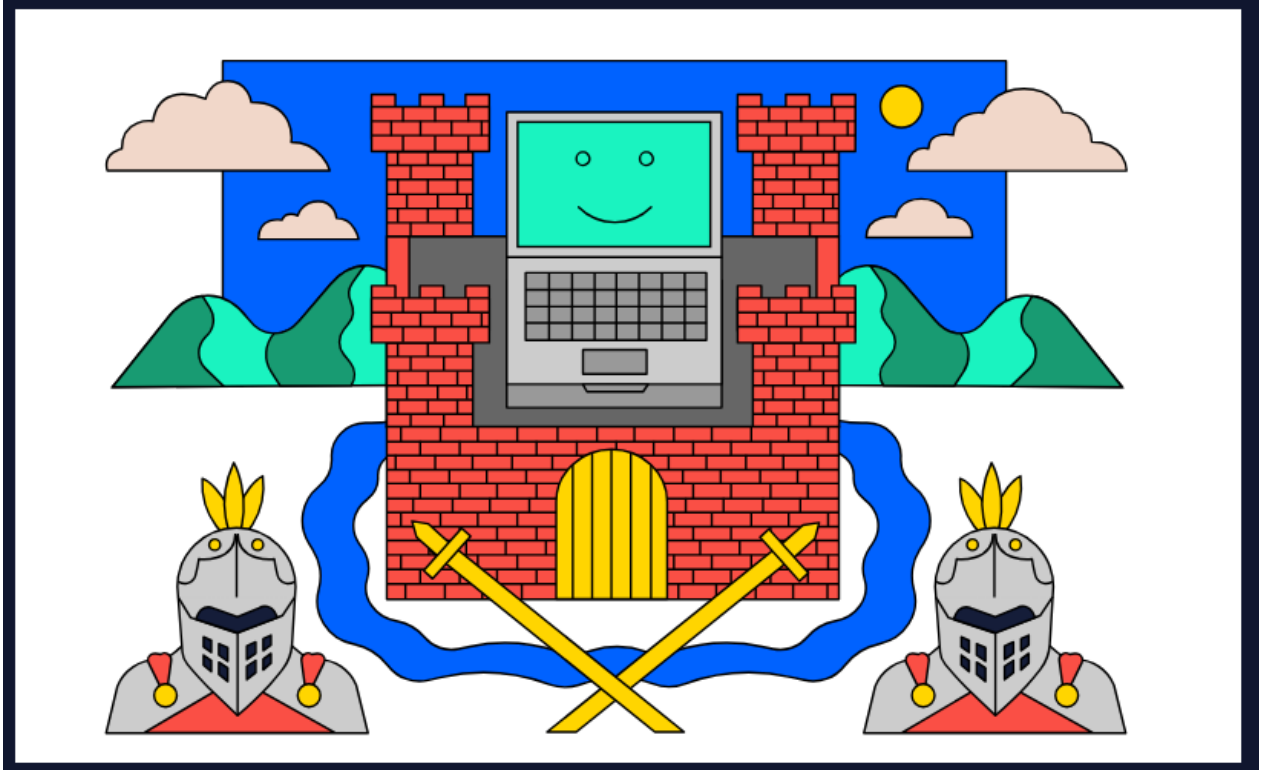
Personal Security: Hardening Your Device

Hardening your personal device is a huge part of security.

What is Hardening?

Hardening is the process of fortifying a system against attacks. When we harden computers, we are generally focused on fortifying the operating system, making sure that it is as secure as it can be.



Computers are complicated machines. If we had to communicate with the hardware directly, we would never get anything done! That's why computer scientists and engineers created *operating systems*. Operating systems (OS for short) are pre-loaded sets of software that handle the details of keeping a computer running, provide services to applications, and make it easy for us to interact with our computers.

If the hardware of a computer is its brain, the operating system is its consciousness and also its protection from cyber attacks.

A Balancing Act

Hardening is a balancing act: too little of it, and the computer is vulnerable to attacks, but too much hardening can make a computer impractical to use. For example, keeping a computer off is a sure-fire way to prevent it from being remotely compromised, but also dramatically decreases its usability.

Because hardening often has trade-offs, it's important to analyze what threats you could likely face before determining what hardening is necessary to protect yourself and your assets. Does this computer have access to sensitive data? Do lots of users access this computer? Is this a personal, public, or company computer?

Shared Personal Security Practices

No matter what OS you use, there are some shared practices between different types of devices. Some examples of shared practices might be:

- Requiring Account Passwords
- Limiting Administrator Access
- Utilizing Firewalls
- Using a Trustworthy Antivirus Software
- Keeping Your System Up-to-Date

There are other security practices that will differ based on the type of device you use. Many Windows processes will be unique to Windows machines. Linux and Mac OS might share some processes because the Mac terminal is similar to the terminal on Linux machines. Again, research, research, research!

As you research, remember: malicious actors might try to trick you with fake security tips in order to gain access to your machine. Don't download the first antivirus you see a link for. Be vigilant and careful.

What will you do to harden your personal device?