In [computing](https://en.wikipedia.org/wiki/Computing), hardening is usually the process of securing a system by reducing its [surface of vulnerability](https://en.wikipedia.org/wiki/Attack_surface). Hardening exists on every level from the end user, to the local network, to the Internet service provider, and on every node in between.

Cybersecurity can seem like an endless process with many factors at play. These factors include not only the securing of the computer itself via hardware, software, and mobile devices, but also for the end user. The “human factor” or the end user, is often considered the weakest link in cybersecurity. Organizations must address the human element if they want to prepare and protect themselves against cyber threats.

As IT professionals, part of our job is to educate end users on how to recognize a potential threat. In this module, we’ll identify common system vulnerabilities and review best practices on hardening.