**Student Hackers Are Next Generation of Cyber-Security Experts**

[**VIDEO**](https://s3.amazonaws.com/pbs-ingest/newshour/video/2013/10/26/PNWE20131026_Cylab.mp4)

Protecting the digital integrity of corporate and government computers is becoming a major industry, with businesses and government spending around $46 billion this year to protect themselves from hackers. Carnegie Mellon University in Pittsburgh is at the forefront of training the next generation of good-guy hackers to do just that.

The skill sets to maliciously break into computers and to protect them from malicious break-ins are almost identical, and computer security students must learn to think like criminal hackers in order to do their jobs. This has raised concerns that Carnegie Mellon could be training hackers with bad intentions. However, graduate student Peter Chapman says not to worry.

“This isn’t hidden information. Someone who’s determined to break into a system, they can take normal courses and just add this, “How am I going to ruin the world mindset” to it,” he said. “It’s the same way a locksmith who knows how to fix locks can probably also break into them.”

“At some point they make the decision. You know, “Am I going to be– a good hacker or a bad hacker?” said Andrew Conte, an investigative reporter at the Pittsburgh Tribune-Review who’s written dozens of articles about hackers and cybersecurity. “And there’s not that much difference between them in terms of– their abilities. Huge difference in terms of their motivations.”

**Discussion questions:**

1. How can hackers be used to help protect the government and corporations from other hackers?
2. Is it moral to hack into another government’s information if it might save lives?
3. Is it moral to use hacking to protest things you disagree with?
4. What are the risks and benefits of teaching college students how to hack? Would you sign up for that class? Why or why not?