Cyber attacks are deadly to businesses, and the working world is fighting back. To that end, more and more colleges now offer courses, degrees and programs to help stop online predators in their tracks. It is an option that businesses are using to gain knowledge critical to safeguarding their networks from viruses and hackers.

“We are an Internet-enabled world, where everything we touch has a component for online access,” said Bill Dafnis, dean of the School of Information Systems and Technology at Strayer University. “It touches every industry — for instance, health care [and] … manufacturers with worldwide distribution and data in many countries.”

Strayer University, which has a corporate office in Virginia and a location in Center Valley, recently launched an Internet-based master of science in information assurance degree to combat online terror. Graduates are essentially taught about what makes an online device a good target for a hacker and what steps to take to protect from a cyber attack. During the program, students are placed in live labs and given roles as both hacker and potential victim.

Dafnis said it is important for everyone to lock their “cyber doors.” The university started the MSIA degree to educate on cyber attacks while meeting employer demands for cyber security personnel. The goal is to equip grads with the educational tools necessary to combat online warfare at home and in the workplace.

“It is obvious that prevention and detection are key. This course is about risk management and developing policies and procedures” for online attacks, Dafnis said.

**MASTER’S IN CYBER SECURITY**

Penn State University, which has campuses throughout the state, also offers undergraduate and graduate programs on cyber attacks, including a master’s degree based on cyber security.

David Hall, dean and professor at Penn State’s College of Information Sciences and Technology, said cyber security jobs are in high demand. Penn State hosted an expo this fall that drew 400 students. More than 85 percent of attendees left with job offers in hand and many had multiple offers for cyber security positions with pay ranges starting at more than $60,000, according to the university.

“Organizations are interested in our students because they have a combination of technical skills, understanding regarding working in team environments and an understanding of the use of information systems in real-world environments,” Hall said.

At Lehigh University in Bethlehem, information security and policy officer Keith Hartranft visits schools and businesses to give seminars on cyber attacks. October is National Cyber Security Awareness month, a program created with the assistance of the U.S. Department of Homeland Security. Hartranft is scheduled to give a talk at Northampton Community College about cyber attacks.

In a recent newsletter distributed by Hartranft, he details the many forms of cyber attacks from emails that promise fortune or threaten an immediate action to elicit a faster response, to an advertisement that pops up on your computer that offers a free version of an expensive software program.

**TARGETED THROUGH SOCIAL MEDIA**

Cyber attacks also will arrive through social media, where hackers use networks such as Facebook to gain account and credit card information.

A 2011 survey by a company called Symantec reported that Web attacks cost businesses $114 billion each year, and according to the U.S. Department of Labor, the information technology field is projected to grow 22 percent by 2020, creating about 65,000 new jobs for cyber security analysts.

While employers want to hire people who can spot bad malware or a nasty Trojan aimed at taking one’s personal information, it is safe to say that cyber attacks at businesses are underreported each year. Paul Mazzucco is chief information security officer at Xand Holdings, based in New York with a data center in Lehigh Valley. He said the biggest thing that leaves businesses open to cyber attacks is employees who click on the wrong website or receive phishing emails or malware.

In addition, there are security groups that do not follow proper online security measures, and this is why there are specific certifications established for the federal government, hospitals, credit card companies and insurance companies.

“Most business attacks are kept very quiet, especially attacks on large corporate networks that are openly traded on stock exchanges or that house financial data,” Mazzucco said. “So any numbers used to show how many businesses are hit each year are usually quite incorrect.”

In Trexlertown, Spokeswoman Debbie Bauer at Air Products and Chemicals Inc. said the company, like all other businesses connected to the Internet, is always under attack. It has a cyber security department dedicated to finding new techniques and controls to combat cyber attacks.

“Cyber security, like safety, is of utmost importance to Air Products. We take our responsibility as a critical infrastructure of the United States and beyond very seriously,” Bauer said. “We understand the reality that cyber security breaches or successful hacks could potentially become physical concerns without the proper layers of defense to minimize this risk.”

**HACK-PROOFING ONLINE DEVICES**

Keith Hartranft, information security and policy officer at Lehigh University in Bethlehem, uses 10 tips from www.stopthinkconnect.org to educate others about cyber attacks:

1. Keep a clean machine by running recent versions of mobile operating software to fight against malware, viruses and online threats.
2. Don’t lose track of your device.
3. Protect personal information by choosing passwords that have lowercase and uppercase letters and a few numbers.
4. Connect with care by turning off and logging out of your online device.
5. Secure your device by putting a key lock or password on it.
6. Back up your online device by syncing your info to another device or cloud service on a weekly basis.
7. Provide contact info by attaching a name and alternative contact number to your device.
8. Download a secure, free app that will allow you to locate your device in the event it is stolen or missing.
9. Only download apps from reputable sources.
10. Record the serial number on your online device.