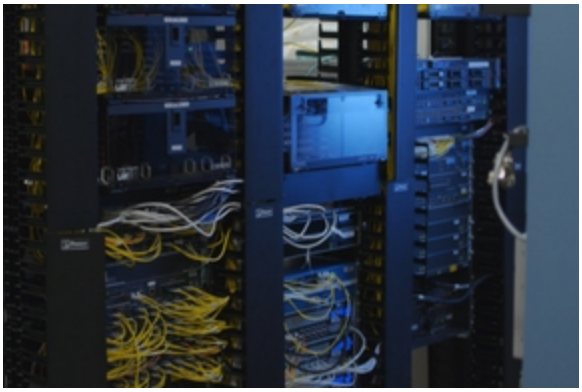
3-7-2018

What a Student Can Teach You About Cybersecurity

Rachel Smith

What a Student Can Teach You About Cybersecurity

udayton.edu/blogs/cybersecurity/2018/2018-03-07-rachel_cyber_class.php



Wednesday March 7, 2018

By Rachel Smith, UD Graduate, 2017

Have you ever walked into a room fearful and anxious because you had no idea what to expect? Well, that's exactly how I felt walking into my Cybersecurity and Communication course during my senior year. As someone with no background in computer science, I was terrified of the class and the challenges it would bring. Despite beginning the class with a "just get through it" mentality, I ended up discovering a new passion.

Cybersecurity is increasingly relevant in our society, yet the average person doesn't know enough about it. Every day, new stories break about companies -- big or small -- being compromised. Hacking with ransomware, phishing, brute force, and denial of service attacks are increasingly common and serious.

The consequences of hacking can be extensive. Businesses can be set back years from damaged reputations, and depending on the severity, they could go out of business. While hacking is often seen as something only big organizations should worry about, it can impact everyday citizens, as well.

From the course's start, my professors (Dr. James Robinson and Dr. Thomas Skill) illuminated how at risk the average person is to cybersecurity hacks -- myself included. Because we're attached to our devices *all of the time,* we're both connected *and* vulnerable. Today, virtually everyone has at least one smart device, as well as email, social media, and online shopping accounts. These connections subject us to potential weaknesses that a hacker can exploit.

Think about it:

If hackers can break into some of the most secure systems (e.g., the Pentagon), they can probably get into your accounts, too.

Each account you have has personal information about yourself. To a hacker, your personal information is financial gain. With just your name, address, phone number, and email, they can open credit cards and trash your credit. Your accounts may also give them access to your social security number, health insurance information, credit card information, and other sensitive data, as well.

As members in a culture that values connection, people must understand the risks that come with online connectivity while learning to protect themselves from potential threats.

Alas, cybersecurity efforts are not hopeless, and hacks are not inevitable. People can do many small things to protect themselves.

Consider:

-Using multiple passwords for your multiple accounts that you regularly change. Pick a time interval and write it down in your planner so that you remember to update them.
-Making stronger passwords. Having the password “1234” or “password” will not keep the hackers out. Use capitalization, lowercase, special characters, and numbers. Don’t just do the bare minimum that web pages require.
-Avoiding clickbait. Hover over links before clicking to verify where they lead.
-Not logging into sensitive accounts when using unsecure WiFi. Other people can easily view what you are doing on public WiFi.
-Deleting suspicious emails and never connecting to an unknown device. Unknown devices, such as a foreign USB drive, can encrypt your computer and hold it ransom.

Summary:

Cybersecurity shouldn’t seem like an irremediable feat. Instead, it’s about being knowledgeable and recognizing that *you have the power and agency to mitigate threats*. Be smart and logical with your information, and if you feel suspicious about something, tread with caution.

Rachel Smith graduated Cum Laude from the University of Dayton in May 2017. As a communication major, she was in the first-ever section of the Cybersecurity and Communication course.