Rebecca Henderson

Tracking Cybercrime

"I really like catching the bad guys. When I first start working on a case, I might not know who the person is behind the scam. It's a fun challenge to figure out who it is, especially if they are trying to hide their identity."

– Rebecca Henderson

A news release from the Washington State Office of the Attorney General pretty much summed up the facts of a computer scam case that affected hundreds of consumers. You can read it at **http://www.atg.wa.gov/pressrelease.aspx?id=19692.**

What the news release didn't highlight, however, is the behind-the-scenes work of specialists such as Rebecca Henderson, a digital forensic analyst.

"Originally I wanted to be a Web developer," she said. "While I was attending classes related to computer networking, I saw that computer forensic classes were also available. Computer forensics sounded very intriguing to me, so I signed up for the first class. I remember how excited I was when I learned how to recover a deleted file off of a floppy disc. That was really all it took for me to get hooked."

Computer forensics is a new and emerging field within the realm of law enforcement – which makes people like Henderson very valuable ... and very much in demand. It also requires her to be a "Jane of all trades."

"I am the only person in my division who does what I do, so I am expected to be the expert in several different areas," she said. "Someday I would like to see a team of forensic investigators in my division."

Henderson describes an average day as being anything but average.

"One part of my job involves tracking down businesses online that are using unfair and deceptive practices," she explained. "This might involve the use of deceptive advertising designed to trick people into downloading and/or purchasing software that they don't really need. This might also involve spam, phishing and spyware.

"Another part of my job involves performing a forensic analysis of a hard drive in search of evidence related to a case," she continued. "A majority of my time is spent performing online investigations. I have several undercover identities that I use to pose as a consumer online. If I know of a company that is scamming people online, I will participate in a transaction with them and document all of the evidence involved. If I don't already know who they are, I will then need to review the evidence so I can track them down."

It's fun, challenging and rewarding, all at the same time.

To get a job in computer forensics, specialized training or a bachelor's degree in computer science is recommended. Henderson graduated from the Digital Forensics and Information Security program at Edmonds Community College in Lynnwood, Washington.

But, she warns, be prepared to learn more than just computer skills.

"You should also be able to write reports to explain the evidence that you find," she said. "Good writing skills are a definite plus. Digital forensics and network security go hand in hand, so it is best to learn about both subjects. If you have skills in both areas, you should be prepared for a wider variety of jobs. This could include jobs such as a Computer Forensic Examiner, Data Recovery Specialist or Network Security Specialist."

Henderson foresees an increasing demand for forensic experts with advanced technical skills.

"Cybercrime continues to become more advanced, which means forensic experts need to keep up with current trends," she said. "Cybercriminals increasingly use better methods in order to hide their true identity, which makes it more difficult to find them.

"Forensic analysis is no longer something that is only done on computer hard drives," she said "Almost every type of digital equipment such as PDAs, cell phones and even an Xbox can be a source of evidence. Even the Internet is a source of evidence."