The Cybercrime Arms Race

If you've ever cleaned your computer of a virus, opened an email from your "bank" asking for your username or password, or been offered software that you were sure was not legitimate, you're one of the billions of people each year who are touched by the growing epidemic of cybercrime.

Cybercrime is typically characterized as an online offense committed by hackers, crackers, and other malicious types that use the internet to steal identities, hijack PCs, and pursue other types of fraud such as illegal spam, phish, and pharm schemes. Software piracy, another form of cybercrime, is when individuals or businesses illegally copy software to distribute or keep for personal use.

Though its hard to quantify an exact amount, the leading computer security company McAffee and other research estimates that cybercrimes cost businesses as much as $1 trillion globally in 2008 by way of lost intellectual property, data recovery efforts, and repairs.

The use of technology has contributed to huge economic losses for businesses and individuals through the fraudulent and criminal use of the internet, telephones, and credit cards, says John Shupper, chair and Legal Studies program director at South University – Columbia. And many schools, including South University, are trying to equip students with the tools necessary for the daunting task of fighting cybercrime.

"Hackers access your Internet files and steal your passwords so they can access your bank accounts or obtain your credit card data. Thieves steal credit card offers from your mailbox in order to steal your identity and run up bills in your name," says Shupper, who supervises paralegal externships in Columbia and teaches courses that cover aspects of cybercrime. "Criminals have gotten to the point where they can take a photograph of your credit card with their cell phone while you are paying your bill at a cash register."

All hope for a safe and secure digital future isn't lost, though. In their newly-released threat predictions for 2010, McAfee says that law enforcement will see many more successes in the pursuit of organized cybercriminals. With hundreds of groups and agencies dedicated to getting ahead of the cat-and-mouse game, and with the growth of the IT industry, there's reason to believe that instances of identity theft and security breaches could decrease in the near future, McAfee says.

The Business Software Alliance (BSA) is a multi-national group that creates policy for IT companies and specializes in tracking, reporting, and reducing the threat of software piracy and its effects on security. Peter Beruk, director of compliance marketing with BSA, reports that cybercrime, especially piracy, can translate into fewer jobs and less tax revenue.

"Software piracy affects all businesses, both large and small, " Beruk says, adding that U.S. software companies lost $9.1 billion dollars in 2008 due to software piracy alone. "A comprehensive approach from technical, legal, and policy experts is necessary to help create solutions to this problem."

Getting ahead of criminals by taking proper security measures and prosecuting perpetrators may be the key to success, especially for the legal profession, which alternately must fight against and protect itself from cybercrime.

The Internet Crime Complaint Center (IC3) – a partnership between the FBI, a nonprofit called the National White Collar Crime Center, and the federal government's Bureau of Justice Assistance – was created to receive, develop, and refer criminal complaints regarding the rapidly expanding arena of cyber crime. On a smaller, more concentrated scale, state attorneys general typically lead cybercrime and cyberfraud task forces.

In addition to increased governmental policy, the Business Software Alliance promotes education about the problem in businesses, schools, and universities, so that security and piracy issues occur less often. At South University, Shupper said, increased emphasis is being put on course work that teaches the implications of cybercrime to legal studies majors.

The Legal Studies department has adopted textbooks where publishers have added chapters dealing with changing business practices and new laws related to the use of the internet, electronic signatures, and privacy laws. In addition, South University recently added a new cybercrime course to deal with

various forms of electronic communications and business transactions, including electronic discovery in federal courts, so that students majoring in Legal Studies will know the latest trends and developments in the law, Shupper says.

"Students are routinely given assignments designed to teach them how to maintain confidentiality of their communications with clients especially when they use electronic communications like e mail and faxes," Shupper says, and they also are informed of emerging trends in real estate, business law, and other areas.

Faculty members also keep up with trends by attending professional conferences, as evidenced by the attendance of Legal Studies program directors at the AAFPE National Convention in Portland, Oregon in October, 2009. There, paralegal educators from across the nation provided training sessions and presentations related to the latest trends in paralegal education and American Bar Association Guidelines, Shupper says. Many of the sessions dealt with electronic communications and specialized software for use in the classrooms.

"The electronic age has dramatically changed the way attorneys practice law and the way courts operate," Shupper says. "We are continually evaluating and changing our programs as needed to stay abreast of the rapidly changing practices in our courts and modern law offices."