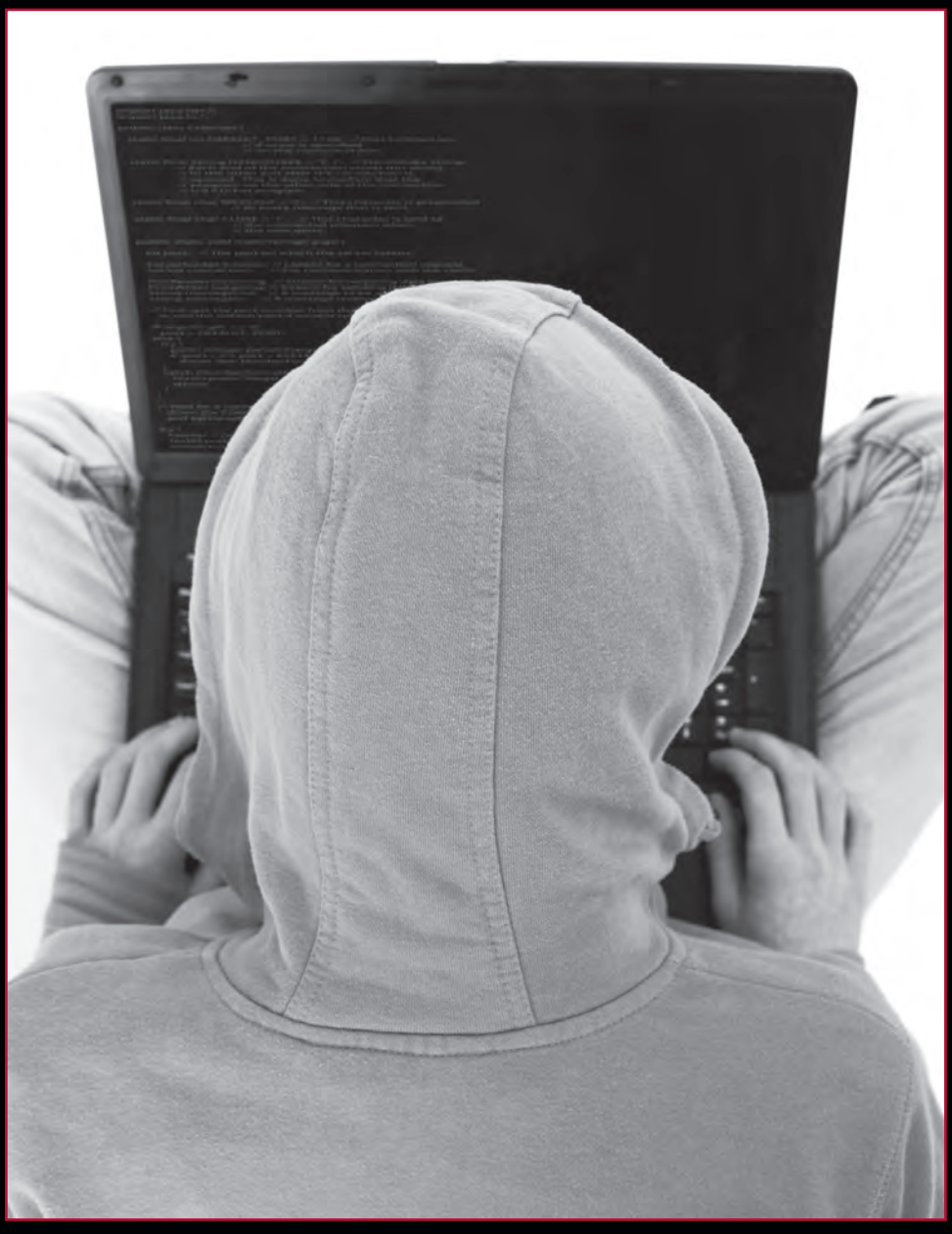

Portrait of the Cybercriminal as a Young Man

Computers have given juveniles the ability to engage in the same kind of white-collar offenses as adults, says Henry Pontell

In 2000, 15-year-old Jonathan Lebed made headlines — and financial history, of sorts — when he became the first minor ever charged with stock market fraud by the U.S. Securities & Exchange Commission.

According to the SEC, the New Jersey teen used his computer to execute a classic pump-and-dump scheme. He snapped up cheap penny stocks, spread false rumors about them on financial message boards under various aliases, and then sold them for a tidy profit. His investments, ranging from an importer of Italian cheese to a manufacturer of bendable toy figures, netted him hundreds of thousands of dollars — as much as $74,000 in a single day. The SEC dropped the charges against Lebed after he agreed to hand over $285,000 in ill-gotten gains.

Shady stock trades are nothing new to Henry Pontell, UC Irvine professor of criminology, law & society and sociology. An expert on white-collar crime, he's studied Wall Street rip-offs and other forms of financial fraud for three decades, even testifying on the subject before the U.S. Senate in 2010 (PDF). What's changed isn't the scam but the artist: In this digital age, the criminal mastermind is often a mere child.

It's something Pontell hadn't seen before the widespread use of the Internet. Elaborate stock swindles, identity thefts and other big-money heists have been orchestrated online by adolescents, some not even old enough to drive. The perps have pimples.

Steve Zylius / UC Irvine

Henry Pontell, UC Irvine professor of criminology, law & society and sociology, says the anonymity of the Internet has prompted some teens to perpetrate major online swindles, fleecing their "faceless victims" of millions.

"Fifteen seems to be the magic number. I don't know why. It's something about hormones or not getting dates," Pontell says, half-jokingly. "They're not really grownups and not really kids, and they probably aren't dating a lot. They're stuck in their rooms with their computers. That plays into this. They're at the peak of their techno-geekiness. And they're really savvy."

One of the first in his field to study cybercrime, Pontell once summed up the threat such "geeks" pose this way: "There are kids out there today who can steal your identity, destroy your credit and empty out your bank account without ever leaving their computers. And they can do it as fast as unwrapping their birthday presents."

In the 2010 edition of *Profit Without Honor: White Collar Crime and the Looting of America,* an academic text he wrote with Stephen Rosoff and Robert Tillman, Pontell added research on Lebed and other juvenile cybercriminals.

Cases in which adolescents pull off sophisticated swindles are such a new form of deviance that he and Rosoff invented a term for it: white-collar delinquency.

In a 2008 study, Pontell and Rosoff reported that 24 percent of those charged under the federal Computer Fraud and Abuse Act between March 1998 and July 2005 were under age 20. The median financial loss was $59,000 per case – making kids' weekly allowance look like chump change. Before the Internet, one had to at least pass for an adult to score that kind of money.

"You had to do all kinds of physical things to commit a white-collar crime," Pontell notes. "A 15-year-old can't pose as a stockbroker."

Underage cybercriminals don't fit the traditional profile of juvenile delinquents, he says. They're not the typical troublemakers, the ones already on law enforcement's radar for truancy, drug use and gang behavior.

continued on next page

Among middle and high school students, those most likely to engage in illegal online acts had friends who did so, according to a 2011 study led by Michigan State University criminologist Thomas Holt. Other determining factors included the amount of time they spent on computers for nonacademic reasons, lack of self-control and having strong tech skills. Higher grades were not an indicator, and girls were highly unlikely to commit cybercrimes.

"It's a male-dominated activity," Pontell says.

To his classmates, coaches and friends, Cole Bartiromo appeared to be an ordinary high school student involved in the usual extracurricular activities: playing baseball, working at a local pizza joint and trading sports cards. But that wasn't all he traded.

From his Mission Viejo home, not far from UC Irvine, Bartiromo bilked at least 1,000 people of more than $1 million through an online Ponzi scheme, according to charges filed by the SEC against the then-17-year-old in 2002. The teen had promised investors returns of up to 2,500 percent for betting on sports events, paying off some but moving most of the money into an account he controlled in Costa Rica.

The SEC also accused Bartiromo of making false claims on the Internet to pump up stock he'd purchased in 15 publicly traded companies, then cashing in his inflated shares.

The government made the young wheeler-dealer pay back investors and fined him nearly $1.3 million, but there was more trouble. In 2004, at age 19, Bartiromo was sent to prison for 33 months for conspiring to defraud a Wells Fargo bank branch out of about $400,000 and for conducting fraudulent auctions on eBay, collecting payments from bidders and not delivering the goods.

Why would teens — or any person — who otherwise might not think of stealing someone's handbag or holding up a liquor store be lured into fleecing victims online? Pontell attributes it to the anonymity of the Internet.

"Cybercrime is characterized by diffuse victimization and rationalizations by offenders that allow them to maintain a positive self-image while engaging in acts they know are wrong," he says. "The Internet puts social distance between the perpetrator and the victim, so any guilt, sense of responsibility or appreciation of the harm and injury caused is diminished."

Lebed, he notes, showed no remorse for his actions, telling "60 Minutes": "I'm not aware of one investor that exists that I cheated." His father even told *The New York Times,* "I'm proud of my son."

"There's this idea that there was no injury to the victims, but there was," Pontell says. "Many investors lost money. Lebed's gain was someone else's loss. It's the fact that they're faceless victims – that's why some people don't see cybercrime as causing real harm."

In addition, many view it as more acceptable than other forms of deviance because they're doing it too.

"Some crimes don't elicit the same kind of response that others do," Pontell says. "People swap discs and buy pirated DVDs and think, 'Who am I hurting? I wouldn't have bought this [legally] anyway.' That's why they aren't up in arms about a lot of these crimes."

Discouraging cybercriminals calls for more than enacting tougher penalties, he says. It means changing social mores, so people stop seeing piracy and other illegal activity as somehow OK. Parents, in particular, need to do a better job of instilling values in their children and keep closer watch over their computer use.

"We have to solve the problem of white-collar delinquency in terms of producing ethical kids," Pontell says. "We need to ask, 'What is my son or daughter doing up there on the computer?' Many parents have no clue."

One voice kids might heed is Bartiromo's. In a bid to reinvent himself, the former teen swindler has visited schools to talk with students about the lure of cybercrime and its real-life repercussions, reports *The Orange County Register*.

"It's OK to be different, to exceed and excel over your peers, but only if you do it legally," Bartiromo, now nearly 30, told one group at California State Polytechnic University, Pomona. "Otherwise, you'll eventually be paying the price in all the ways I have." ■

Kathryn Bold, UC Irvine