It's ID theft, but money's not the goal

by Dana Littlefield

It began innocently enough. A college student studying in southern Spain snapped photos of herself in a bikini and e-mailed them to her boyfriend in the United States.

ID THEFT - Keith Burt, a deputy district attorney in San Diego, says his office gets two to three calls a week from people who claim they were harassed or impersonated online. CNS Photo by Nelvin Cepeda. In the months that followed, she didn't give the images much thought. That is, until early last year, when they popped up in her inbox attached to an ominous e-mail. It read:

"I think these belong to you? I have accessed all your e-mails and files on your computer. These pictures are very nice. It would be bad if these got out.

If you tell anyone about this, even your boyfriend I will e-mail everyone you have ever e-mailed with these pictures.

This is not a joke. Do you understand?"

The sinister missive - signed "Jon Smithhacker" - frightened the 22-year-old from San Diego. Who was Jon Smithhacker? How did he get the photos? Would he make good on his threat?

She notified police at her Northern California university and consulted computer technicians. They told her there was no apparent problem with the school's Internet security and that the photos must have been stolen by someone she knew.

Her photos also had been posted, along with her name, on various adult Web sites, a friend discovered. Some of the images had been doctored - cropped so that she appeared to be nude.

"I couldn't believe it. I could not believe it," she said in an interview. "I don't know why I thought it was an empty threat."

Because she is a crime victim and the images are still accessible on the Internet, the student asked that only her first name, Christine, be used in this article. She told family members what had happened, and they were supportive. Her sister's fiance, Michael Fletcher Norris, offered to contact the Web site operators and ask them to remove her photos.

But soon afterward, as Christine's university was about to launch an investigation, Norris confessed to being the person who had posted the photos and sent the threatening e-mail.

He later pleaded guilty to a felony charge related to identity theft and was sentenced in February to a year in county jail.

"How dare he do this to me?" Christine said, firing off rhetorical questions.

"How can I be a teacher if my pictures are all over the Internet?

"How am I going to explain myself?

"How am I going to maintain a job if people find this out about me?"

What happened to Christine is difficult to categorize. Although Norris used her personal information without her knowledge - effectively stealing her identity - this wasn't identity theft in the traditional economic sense. And even though she felt scared and harassed, it wasn't cyberstalking as most states define it.

Some experts say laws should target people who impersonate others online and do irreparable damage to their reputations. Often, the perpetrators are angry with their victims, and they exact revenge by humiliating them personally and professionally.

"This is not a lesser crime," said Keith Burt, a San Diego deputy district attorney. "The harm is enduring. Some of the harm you may suffer, you may never be able to prove."

Burt is part of a multiagency Computer and Technology Crime High-Tech Response Team.

Under California law, it is a misdemeanor to contact a person by phone or by computer device to annoy or threaten injury.

Federal cyberstalking laws could apply if someone threatens, harasses or causes "substantial emotional distress" to someone in another state by means of a computer or electronic device.

Victims may also sue for defamation, or obtain a restraining order, but only if the perpetrator's identity is known.

But some say that's not good enough.

Burt, who prosecuted Christine's case, said the District Attorney's Office receives two to three calls a week from people who claim they were harassed or impersonated online.

The cases are usually time-consuming and expensive, because investigators require specialized training and perpetrators are hard to track down.

Adding to the difficulty is the fact that sometimes the offender doesn't harass the victim directly, but prompts others to do it.

California state assemblyman Guy Houston introduced a bill this year that seeks to punish people who use Internet sites such as Craigslist and MySpace to intentionally incite a third party to harass or intimidate a victim. Such acts would be prosecuted as misdemeanors.

Houston cited two recent incidents. One involved a 17-year-old girl whose photo and cell phone number were posted online without her consent, causing her to receive dozens of lewd voice mails and messages.

In another case, a tenant evicted from a rental home in Tacoma, Wash., posted a phony classified ad on Craigslist encouraging people to take what they wanted from the property. When the landlord returned to the house, she found many items missing, including the kitchen sink.

San Diego prosecutors have charged defendants in these types of cases with using the personal identifying information of another, which can be handled as a felony or a misdemeanor.

At Norris' sentencing hearing in February, Superior Court Judge Timothy Walsh called the defendant's actions "evil" and commended Christine and her sister, who broke off her engagement immediately, for speaking up in court.

"There's going to be a time - and it's unfortunate - that some employer of yours is going to Google you, your students are going to Google you," the judge said. "Things are going to happen and this isn't going to go away.

"I'll tell you I'm shaking, because these kind of things really bother (me) because they're new and, frankly, the system doesn't know how to handle them yet," the judge continued.

"And I don't think it will be long before we see the punishments significantly increased in this area legislatively."

Norris' family maintains that he is remorseful and is paying for his crime. They say he is a changed man.

In another recent case, William Richter, 53, of Alpharetta, Ga., was accused of using a San Diego woman's personal information to set up e-mail accounts, a blog and a MySpace Web page in her name.

Investigators learned that Richter had used the woman's information to apply for jobs and post phony resumes on the Internet. He also exchanged messages with MySpace users, even prompting a man to show up for a lunch date at the woman's job.

Richter's blog, which was set up to look as if the woman had posted the entries herself, stated that she was a recent "post-op male to female transsexual" who liked cross-dressers, according to court documents.

He pleaded guilty to an identity-theft charge and was sentenced May 1 to a year in jail, after which he'll be placed on probation for three years.

"It was the most embarrassing and humiliating experience of my life," the victim wrote in a letter to a judge, adding that she believed Richter targeted her because she rejected his friendship.

"This crime is not finite like a purse being stolen, or a credit card being misappropriated, this crime strikes at the core of who you are," she continued. "It distorts your reputation and uproots everything you worked for to be a good person, a good worker and a good community member."

Christine, now 23, is studying for her teaching credential. She e-mailed the webmasters at several Internet sites asking them to remove the pictures Norris posted, but a few keystrokes on a search engine reveal that the images are still out there on the Internet.

Experts say that even if photos and files are removed from some Web sites, little can be done to be sure they won't resurface. The person who has the original image can upload it on a different site. Images posted online for just minutes can be copied and distributed around the world, said Christian Desilets, a research attorney with the National White Collar Crime Center in Richmond, Va.

"Realistically, one can never be sure that an image has 'died' online," he said.

It's ID theft, but money's not the goal by Dana Littlefield