'I thought it was my sister': Woman loses $2,000 to Facebook scam

By Bob Sullivan

Now, you can't even trust your sister on Facebook.

Edythe Schumacher logged onto the social networking site recently and a picture of her sister popped up immediately, inviting her into a Facebook chat. After a bit of small talk, Schumacher's sister – Susan Palmer – egged her on to apply for a government grant, saying she'd just received one. For an up-front fee of $2,000, Schumacher was assured, she'd get access to up to $500,000.

Schumacher trusted her sister — and lost $2,000.

Apparently, Facebook impersonation scams have reached a new level of duplicity. Palmer's account had been hacked, Schumacher says, by an impersonator skilled enough to pretend to be her own flesh and blood. The fake Palmer eventually talked Schumacher into wiring $2,000 to an address in Massachusetts.

"Turns out I was not chatting at all with my sister," Schumacher told authorities, according to a report filed with the Ohio state attorney general's office. "I would never have sent the money if I didn't think it was my sister."

Facebook account hijacking has been around as long as Facebook itself. While it often amounts to little more than childish pranks, the theft of someone's identity on Facebook can lead to real harm. Imposters have successfully tricked victims into wiring money before — a common scam involves contacting friends and writing an email with dramatic claims of muggings, accompanied by desperate pleas to wire money. See this earlier report.

'More and more sophisticated'

But impersonating a sibling in a real-time online conversation represents a crime that's bold even for Internet scam artists.

"Scammers are getting more and more sophisticated as the technology ramps up, so people have to really be on guard," said Lisa Hackley, spokeswoman for Ohio Attorney General Mike DeWine.

Schumacher filed a report with Ohio authorities last month detailing the elaborate scam, which also invoked the name of a former high-ranking FBI official and a Massachusetts nonprofit devoted to helping troubled children.

"I just feel so stupid," said Schumacher, 58, who works as a teacher's aide working with autistic kids. Her husband is retired, so the couple is basically living on a fixed income. "But this one blew my mind."

The chat invitation arrived immediately when Schumacher logged on to her computer on Aug. 9. Palmer had sent an -mail blast, warning friends and family that her Facebook page had been hacked, but Schumacher didn't have time to read her email before the online conversation began.

"I was so mad at myself when I finally did read the email," she said.

After bragging about getting a grant herself, the fake Palmer urged Schumacher to contact Sgt. Chris Swecker for more details. Swecker said he was with the Federal Government Humanity & Empowerment Program.

"He informed me I need to Western Union $2,000 to acquire the grant," Schumacher told authorities. And of course, she had to do it immediately.

Chris Swecker is the name of a prominent FBI agent who specialized in electronic crimes during the Internet's early years. He later went on to be chief security officer at Bank of America before retiring recently to do consulting work.

It's unclear whether the criminal intended to use Swecker's reputation to aid the scam, but it's common for computer crooks to use names plucked from online sources to fill in the blanks while composing a scam scenario.

Swecker told a reporter that he hadn't heard that his name was used to dupe an innocent victim.

"There's an epidemic of this kind of thing happening on the Internet," said Swecker. "I speak about online crime all the time, so it's ironic my name is caught up in this."

The fake Swecker told Schumacher to wire the money to a woman named Patricia Casella in Springfield, Mass. The ruse was thorough. When he called her cell phone, and the caller ID read "Empowerment GOV54." Persuaded, she wired the money.

"He waited (on the phone) till the transaction was completed," Schumacher said.

Even after the money arrived, the imposter contacted her again, looking for $800 more. But by then, she was wise to the scam.

"He did contact another one of my sister's friends, too, but she didn't fall for it," she said.

Innocent bystander

The address where Schumacher wired the $2,000 is that of a nonprofit named The Children's Study Home, which says on its website that it caters to the psychological needs of children who have suffered abuse and neglect. The agency is an innocent bystander in this scam, and probably others.

Criminals who receive stolen funds via Western Union don't have to visit the destination address. They merely show up at the nearest Western Union facility with some identification and walk out with the money.

Steve McCafferty, executive director of The Children's Study Home, said this isn't the first time criminals have used his agency's address as a destination for stolen money.

"We know this has happened before," he said. Criminals have, at least once before, picked up cash labeled with his agency's address at a Western Union in a nearby grocery store, he said. The agency has received suspicious packages, also. Springfield police have been notified but so far have been able to do little to stop the crime.

"We're just a nonprofit agency, we don't want to be a part of this ... and it's unfortunate that people are falling for it," he said.

This newfangled Facebook impersonation scam is just an elaborate narrative designed to distract victims from a variation on an old-fashioned "advance-fee loan scam," said Hackley, of the Ohio Attorney General's Office. Criminals tell victims they can qualify for a loan by paying a small up-front fee, but -there is no loan, she said.

The new Facebook scam is also reminiscent of a traditional grandparent scam, she said, where a criminal calls a victim pretending to be a grandchild and makes a desperate plea for bail money or emergency cash.

"Don't tell my parents" is often a part of that storyline, Hackley said. Elderly parents can often be tricked into sending money, she said, particularly now that many of them list their grandchildren on their public Facebook page.

"The criminals can look at their pages and use the correct names. They are easy to find online," Hackley said. Facebook pages and pictures can also help criminals flesh out their narratives – "Grandma, we had fun at your 80th birthday party, didn't we?"

'Vulnerable niche'

That's why it's a good idea for children and grandchildren to aid older Facebook users with privacy settings. There's no need to make family member names available to strangers.

Swecker said he's very concerned about the growing numbers of older Americans who have begun to use social networking tools but have yet to develop the necessary skepticism for the online world.

"They are a vulnerable niche, the age group that didn't grow up with the Internet," he said. "Sometimes, the older generation has no idea how to protect themselves. For them, (using Facebook) is like giving the keys of a Ferrari to a 14-year-old."

Schumacher recommended that Facebook users drop a personal question or two into every chat, just to help positively identify chat participants.

She’s currently working overtime at school, trying to replace the lost funds.

“When you are counting every penny, it hurts. … I can't believe I did that. I’m not a risky person with money,” she said. “But I learned my lesson with Facebook.”