Cyber scams are getting more personal, thanks to social media

June 19 2012, By E. Scott Reckard

Old high school classmates aren't the only ones making connections on Facebook. The crooks are too.

There's the Osama bin Laden death video that downloads a virus into your computer. A sting known as the grandparent scam in which fraud artists plead desperately for money, pretending to be young relatives. And last week a new one surfaced that steals your personal information by advertising a 20 percent cash rebate for users who link debit cards to their Facebook account.

People are used to con artists pitching them via email. Who hasn't received a sketchy alert that they've won an African lottery, inherited millions from a long-lost relative in Eastern Europe or had a security breach of their bank account?

But Facebook, with its network of "friends," has a way of making people let their guard down.

"We've all been dealing with email spam for 10 or 15 years now, and we've gotten darn good at it," said Chester Wisniewski, a senior advisor at Sophos Ltd., a provider of corporate data security systems. "But it's a lot more convincing when you think you're hearing from your cousin than getting something filled with spelling errors from a random stranger in Russia."

Sophos calculates that straight email scams have dropped 30 percent

over the last year or so, and Wisniewski said widespread anecdotal evidence shows social-media scams have surged.

The exact scope of the new-wave schemes is unclear because online companies don't disclose numbers and many victims are too embarrassed to report problems to law enforcement. But there's plenty of trouble out there: In 2011, a federal Internet crimes center logged 314,246 complaints with losses totaling $485 million, the third straight year of more than 300,000 complaints.

Some scams involved emails that appeared to be from Facebook itself, or popular games such as "FarmVille" or "Mafia Wars." And, armed with user names and passwords, thieves will hijack Facebook accounts to target people on their friends list.

A simple scheme might use a template from a genuine Facebook email to ask millions of people to update their security questions because of unauthorized access attempts against their accounts. Then the scamsters snatch your personal information.

Still more vulnerable are the many users who accept all friend invitations, along with those having low or no security settings on their accounts.

"Even if you don't friend someone, if you post things publicly or share lots of information with a compromised friend, your information is still available," Wisniewski said. "If something is truly sensitive, it is best not published on the Internet."

Schemes in which criminals pretend to be a desperate relative in need of help appear to be among the most brazen.

The so-called grandparent scams gather information about the target

person, their family, friends, even dogs and cats. Then comes the appeal, laced with personal details, typically in a muffled and distraught phone call saying a young loved one needs cash quickly to get out of a jail or a scrape in Eastern Europe, Asia or Latin America.

"I prefer to call them 'relative in distress' scams since that's the general scenario," said FBI spokeswoman Laura Eimiller in Los Angeles. "We have one victim who is middle-aged, (and the) scammer pretended to be her son who is fighting in Iraq."

The scams can draw in even sophisticated financial minds, such as a Ventura County, Calif., financial advisor who is working with the FBI after losing nearly $5,000 to a young man impersonating a nephew.

The scam artist said he was calling from the U.S. Embassy in Mexico City after a wrongful drug arrest. The victim, who sent the funds via Western Union in two installments, called back at one point to check how things were going.

"I called the number that they left me down there, and a woman answered 'U.S. Embassy,' " said the victim, who asked not to be identified because it would hurt his professional career.

A scammer pretending to be a Marine sergeant advised him that money was the only swift way to deal with the Mexican legal system.

"Try flushing 50 hundred-dollar bills down the toilet if you want to know how I feel," the man said.

In another common scheme, the criminal hijacks a Facebook account's friends list to send emails pleading for money on behalf of a person who supposedly has been robbed in a foreign country and left without even a passport.

"It looks like it's coming from a friend," said Jenny Shearer, an FBI spokeswoman and cyber crime expert. "You'd hope the targets would check first to see if the friend really is in London, but sometimes they're really worried and wire the money first."

The problem is serious enough that Facebook Inc., Google Inc., Microsoft Corp. and other big tech companies teamed up this year to fight the scams through an alliance called Domain-based Message Authentication, Reporting & Conformance.

Fraud artists have "a tremendous financial incentive" to steal passwords and information about bank and credit-card accounts from social media and e-commerce sites, according to the group.

"Simply inserting the logo of a well-known brand into an email gives it instant legitimacy with many users," the alliance said in announcing its counterattack.

Facebook also has been active in fending off cyber thieves. Protecting users from scams "is a top priority for us," the social media giant said in a statement. Facebook said it uses "enforcement mechanisms to quickly shut down malicious pages, accounts and applications."

"As always, we advise people not to click on links in strange messages, even if those messages have been sent or posted by friends," a spokeswoman said.

Wisniewski said Facebook is adept at shutting down scams, but some of them move so fast that hundreds of thousands of potential victims can be reached before that can be accomplished.

A malicious software program called the Zeus Trojan horse last week attacked Facebook, along with Google Mail, Hotmail and Yahoo,

offering rebates and new security features. The Facebook version used a pop-up form to offer a fraudulent deal that supposedly linked MasterCard or Visa debit cards to Facebook accounts, online bank security provider Trusteer Corp. reported last week.

It said that users who registered their card number, expiration date, security code and PIN would earn 20 percent cash back when they bought Facebook credits, which are used to play games on the social media site.

Of course, the real aim was to make debit purchases using stolen information, which can be easy to obtain, said George Tubin, a senior security strategist at Trusteer.

"Those of us in the security industry are always concerned with the large amount of very personal information that people put out on Facebook," Tubin said. "It's the perfect target for criminals because a lot of the Facebook audience are people who share their entire lives and don't think about security."