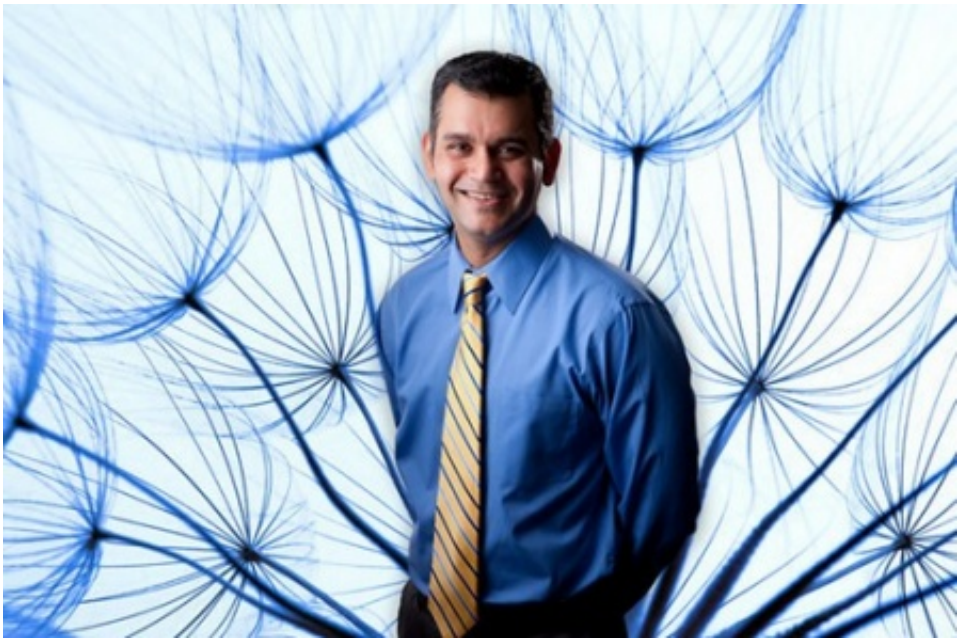
Online phishers are 'farcing' your brains out

July 31 2014, by Pat Donovan



Be careful when making friending decisions on social media, says UB's Arun Vishwanath. Credit: Doug Levere

"Phishers," the crafty perps who scam us via email, are trolling social media sites to steal vast amounts of personal data and then use it to fleece us.

Whereas Facebook recently manipulated our emotional states in service to an online study, phishers exploit us by using the emotional influence of others in our social networks.

"Farcing" is what researchers call it and it's on the rise.

The attack may not end with you, however. Once the phisher friends you, each of your friends may receive a request and think the phisher is a real person—a "friend's friend." In this way, such attacks become virulent in a very short time through a process of upward contagion, in which the phisher steals information from your real online friends, then their online friends, and so on.

These findings are published in a new study by Arun "Vish" Vishwanath, UB associate professor of communication.

"Farcing takes place on popular social media platforms like Facebook, Twitter, LinkedIn and Google Plus," says Vishwanath, "and has been used for online bullying, identity theft, organizational espionage, child pornography and even burglary."

One way to protect yourself, he says, is to be much more careful when you make friending decisions—phony, even felonious, characters will present themselves as great new friend possibilities. Another is to limit the amount and types of personal information you share on social media sites.

"These scams are on the rise and will continue to increase with the popularity of social media, exponentially increasing the number of farcing victims worldwide," he says.

Imagine the wealth of information available to an online "friend," the phisher: your name, your nicknames and the names of friends and relatives; your schools and employment background; your address and pet's name, favorite vacation sites plus when you're leaving and how long you'll be gone; your kids' names and schools; favorite sports teams, entertainment venues and online shopping sites; your church, favorite

charities, what you fund on Kickstarter, and so on and on.

Using this information, it is easy to learn your phone number, email address, maybe your salary and account numbers. Multiply that data by 50 (the number of your real online friends) and then by their 2,500 friends (at 50 each) and you can see that sneaking into your account can be quite lucrative.

"This is how the Hollywood 'bling ring' operated," Vishwanath says. "The scammers used information freely provided through social media profiles, updates and tweets to locate addresses of celebrities, find out if they were home, and rob them.

"Another farcing case, which was attributed to espionage by the Chinese government, tricked senior military officials from the UK and U.S. into becoming Facebook friends with a fictional U.S. Navy admiral," he says. "The phishers then collected a good deal of information about the officials from their profile pages and posts."

To ascertain how the phisher hooks a victim; learn how many victims, once ensnared, are likely to continue to provide information to the invader; and determine the extent of the danger posed by farcing to the social media marketplace, Vishwanath set up a simulated farcing experiment on Facebook and watched it unfurl.

"We established four fake characters with Facebook profiles for the study: one without a photo or friend connections, one with a photo but no friends listed, one with 10 friends listed but no photo, and one with a photo and 10 friends," he explains. "All the characters were male and the photos had previously been rated average for attractiveness."

Study subjects were 150 Facebook users recruited from the UB student body. In stage 1 of the attack, each subject was sent a friend request

from one of the Facebook accounts.

"One in five subjects okayed the fictional farcer's initial friend request, thus falling victim to the first stage of the attack," Vishwanath says.

"While a farcing attack could stop at this point and use just the information already made available to him—including the victims' friend list," he says, "a motivated phisher can go on to the second stage, requesting more information directly from the victim by using messaging functions within the social media platform. Messages can be crafted to take advantage of the asymmetries between the information mined from the victim's page and the deceptive intent of the phisher."

Vishwanath offers the example of a well-publicized farcing attack that took place recently in a school district near Buffalo. A substitute teacher created a false identity and fake Facebook profile in which he presented himself as a female student. He used that identity to entice minors—some of whom were his students—to send him explicit sexual photographs. He is now serving 30 years in prison.

In this study, a further 13 percent of subjects who befriended the phisher responded to his message requesting additional personal information. Although at study's end, 46 percent of the original 30 who had befriended him had decided not to provide additional information, 41 percent were still considering the request.

What did the Vishwanath study learn about how subjects become victims?

"We found that many victims of the stage 1 attack said they relied primarily on the profile and/or photo of the requester as cues and then made snap judgments in 'friending' him," he says, "while in stage 2, victims said they were influenced by the phisher's long list of contacts.

So a fake person with a fake photo and a fake contact list can be handed a lot of data without expending much energy.

"It is the ready availability of personal information on social media profiles and feeds that give the phisher material with which to work," says Vish. "One way to protect ourselves is by limiting what we disclose.

"Second, farcing spreads through social contagion. Think through decisions as to whom to 'friend.' Don't rely on cues like a photo or a list of contacts," he advises. "Paying a lot more attention to who is making friend requests and who is messaging you for further information is likely to further protect you—and your real friends—from these online pickpockets."

The study appears in an upcoming issue of the journal *Information Systems Frontiers*.

More information: "Diffusion of deception in social media: Social contagion effects and its antecedents." Arun Vishwanath. *Information Systems Frontiers*, June 2014. DOI: 10.1007/s10796-014-9509-2

Provided by University at Buffalo