
Mitch Morrissey,
Denver District Attorney

FRAUD ALERT!

From the Office of Denver District Attorney
Mitch Morrissey

Facebook Friends Might Just Take More Than Your Time

Social networking Web sites like Facebook and MySpace are a great way to find old classmates, stay connected with friends, or make new friends. Unfortunately, hackers are using Web sites like these to infect computers and steal identities.

The BBB has identified the following common social networking schemes:

Friend in Distress Scam
One scam that has made the transition from phone and e-mail into Facebook is the "friend in distress" scam. Facebook users may receive a message in their inbox from a friend saying that they are in a dire situation – such as stranded in a foreign country – and need money wired to them. The recipient of the message doesn't realize that their friend's account has been hacked and that the message was actually sent by scammers. If the Facebook user wires money to the scammers, they have no way of recovering the money after they learn that their friend is actually safe and sound.

Phishing Friends
One particularly destructive computer virus, called Koobface, has made the social networking site rounds via MySpace and most recently on Facebook in December. In Facebook, the victim receives a message from a friend saying "You look awesome in this video" or "You look funny in this video" and includes a link to an outside Web site to view the video. Clicking on the link will open a window that claims the victim needs to download an updated version of Flash. Agreeing to the update actually installs the virus onto the victim's computer. The virus is designed to monitor the user's Internet activity and potentially steal personal information. Victims of Koobface have had a particularly difficult time removing the virus and in some cases just decided to scrap their computers completely.

Viral Wall Post
Another recent Facebook scam takes advantage of a social networker's fears that the pictures and information they post on Facebook could be made very public. The user receives a post on his or her wall from a friend saying something like, "hey do u realize your Facebook picture is all over <link to Web site>". The wall posts vary, but all invariably link to an outside Web site that supposedly has the user's photos. Facebook warns that clicking on the link will allow hackers to gain access to the user's personal account and

post the same message – seemingly coming from the victim – on their friend's walls.

Prevention Steps:

- Be extremely wary of messages from friends or strangers that direct the user to another Web site via a hyperlink.
- Before wiring money to a friend in a jam, users should attempt to contact their friend outside of the social networking site, such as over the phone or via e-mail to confirm the situation. If that's not possible, ask them a question to which only they would know the answer.
- Users should always make sure their computer's operating system's antivirus and firewall software are up to date.
- Social networking sites are about sharing information, but it is best to keep information like phone numbers and addresses private.
- Be selective when choosing friends. While a user might not want to be rude, it's best to decline a request for friendship if the user doesn't actually know the person.

Need help or have a question? Call the Denver DA Fraud Line: 720-913-9179

February 2009 – Special Edition