IOWA DEPARTMENT OF JUSTICE | OFFICE OF THE ATTORNEY GENERAL | ATTORNEY GENERAL TOM MILLER

# Consumer Focus

SEPTEMBER 2017

## Watch for Facebook Crooks!

Facebook is a popular site to share photos and stay connected with friends and family. The social media giant now has more than a billion users. With so many users, Facebook is also a popular site for scammers looking for potential targets. Here are some of the most common Facebook scams:

1. **Friend request from an imposter**
   Scammers can copy legitimate accounts to create imposter Facebook accounts that may look authentic. The cloned accounts use the same name, profile picture, photos, and information as the original account to ensure the imposter account is convincing. The imposter will pose as a friend or family member and send you a friend request. If you accept, they might ask you to send money or provide personal information. Scammers might also send you link that will direct you to dangerous sites and malicious software (malware). Or, they may send friend requests from "you" to people on your friends list, and then try to target them through your fake profile. (If you receive a friend request from someone you know is already on your friends list, contact them directly via phone, email, or in person to confirm that this is truly their new account.)

   Make it harder for Facebook imposters by hiding your friends list so they can't contact them if they clone your account. To do it through a web browser, open your Facebook profile, click on the "Friends" tab, click the pencil tab ("Manage"), click "Edit Privacy" and then select "Only me" on the "Who can see your friends list?" drop-down menu.

2. **Like this page and win!**
   When you "like" a page that claims, "*Like this page and win a free trip*," you could get contacted by a scammer who claims you won, but asks for money upfront for shipping costs, taxes, or handling fees.

Legitimate sweepstakes never ask for anything more than your name, address, and telephone number. A sweepstakes asking for bank account information, Social Security number, or money is a scam.

3. **Your account will be disabled**
   You receive a message from a Facebook "employee" stating that your account will be disabled unless you click the link and provide or "verify" your login credentials. This is a phishing attempt from a scammer who will use Facebook login credentials you provide to access your account.

   Facebook will never ask you for your password in an email or a message. If a Facebook message looks strange, including a link that doesn't look right, wording that seems odd, or typos, don't open it or click on links or attachments. You can report the fake messages to Facebook.

4. **Look at this video of you!**
   One of your Facebook friends sends you a message stating, "*Oh my gosh! Look at this video of you!"* with a link to a video. Don't click! Your friend's account has been hacked or impersonated by scammers. Following the link typically requires you to enter your Facebook login credentials in order to view the video and the video usually contains malware. Follow the link and your Facebook account can be hacked, and your computer may have a malicious program installed.

**General Tips**

Be wary of anyone who asks you for money through Facebook (including money card or gift card numbers), even if it seems like a legitimate way for you to claim a prize/winning, government grant, or take part in a money-making opportunity. And be wary anytime someone asks for your password or login information—even if the person claims he or she is a Facebook employee who threatens to shut down your account unless you "verify" it. Lastly, keep in mind that Facebook does not have a public customer service/technical support phone number, so don't get tricked into calling one!