Facebook Scam Alert

You may think of Facebook as a safe haven for sharing, posting and conversing with friends, but it should never warrant dropping your guard from scams and phishing attempts. There are several Facebook scams out there that try to capture personal information or infect your computer with Malware, so protecting yourself can be challenging. The following can help you detect a scam and provide insight on what you could do to prevent falling into common traps.

Friend Requests

Be wary of friend requests even if you recognize or know the person. If you know the person, check to see if you are already friends with them. If you are, the request is most likely a scam. Scammers will re-create someone's existing profile using their profile picture and "About" information and send requests to that same person's friends.

- If you get a request from an existing friend, verify that the request is real.
- Always be suspicious of friend requests form people you do not know.
- Edit your privacy settings to "Friends" in the "Who can see your friend list?" dropdown, rather than "Public".

Fake surveys and coupons

A lot of scammers can steal personal information just from your Facebook user name, so it's important to always be wary of special offers or tempting surveys. Be wary of surveys that mention a discount on your next purchase or coupons from well-known stores that appears too good to be true.

- Don't believe what you see. Scammers can make links and logos appear legitimate.
- Most legitimate businesses will not ask for credit card numbers or personal information on surveys.
- Search the web to see if the coupon or survey is a scam.

Viral videos and photos

Keep an eye out for videos or photos that seem shocking, indecent or racy. If you click on one of these links or videos, the page you are taken to will ask you to update or install a video Flash player. If you agree to do so, malware could be installed instead.

- Search for the video in YouTube or Google. If the video does not appear, it is most likely a scam.
- Never agree to update or download something after clicking on a link from Facebook. This is a scam and if you agree to the download, malicious viruses will be installed onto your computer.

Always be cautious on Facebook and while browsing the web. Scams continue to increase and are getting more convincing, but as long as you stay skeptical and do your research, you can avoid falling into traps.

As always, if you have any questions or concerns about emails, websites or unsolicited calls related to Universal 1, please email our Compliance department at **compliance@u1cu.org**. You can also call our eCommerce representatives at **800-543-5000 option 0** or **937-431-3100 option 0**.
We're available **Monday - Friday 8:30 a.m. to 6:00 p.m.** and **Saturday 8:30 a.m. to 12:30 p.m.**