GARY R. HERBERT
Governor

SPENCER J. COX
Lieutenant Governor

State of Utah
Department of Commerce

FRANCINE A. GIANI
Executive Director

THOMAS A. BRADY
Deputy Director

DANIEL O'BANNON
Director, Division of Consumer Protection

May 11, 2017

MEDIA ALERT

<u>Consumer Alert: Mother's Day Facebook scam luring shoppers with bogus coupons</u>

"Scammers looking to profit off social media as consumers expected to spend 24 Billion on Mom"

(For immediate release…)

SALT LAKE CITY, Utah – Francine A. Giani, Executive Director of the Utah Department of Commerce, announced today the Utah Division of Consumer Protection is warning consumers to be aware of a Mother's Day phishing scam that seeks to steal personal and payment information online. The Division has learned that fraudsters are posting fake high dollar coupons on Facebook to popular retailers. These bogus posts include authentic looking coupons between $50.00 and $75.00 off purchases at Target, Lowe's, Bed, Bath and Beyond and other famous names. Consumers are asked to click through a link to sign up for the coupon offer in exchange for personal address, bank account and/or credit card information.

"Be aware con artists are looking to steal your information online with these convincing coupons," warned Francine A. Giani, Executive Director, "Don't click the link or enter any personal information. Instead call the retailer directly to see what deals are real."

According to the National Retail Federation, consumers expected to spend upwards of $24 Billion dollars on mom this year. State regulators are concerned that this coupon phishing scam could dupe many social media users.

"As Utah shoppers become more savvy online, fraudsters are constantly creating sophisticated phishing scams that look and feel authentic," stated Daniel O'Bannon, Division Director. "Protect your identity and your wallet by verifying the deal offline before you respond."

<u>Tips for Consumers: How to Avoid Phishing Scams</u>

- Be cautious about opening links or attachments from social media posts, emails, or texts regardless of who sent them. These files can contain viruses or other malware that can weaken your computer's security.
- Don't enter or email personal or financial information. Social media sites and email are not secure methods of transmitting personal information.

- Only provide personal or financial information through an organization's website if you typed in the web address yourself and you see signals that the site is secure, like a URL that begins **https** (the "s" stands for secure). Unfortunately, no indicator is foolproof; some phishers have forged security icons.

- Review credit card and bank account statements as soon as you receive them to check for unauthorized charges. If your statement is late by more than a couple of days, call to confirm your billing address and account balances.

For more information on how to protect yourself from scams or to file a complaint, log on to the Utah Division of Consumer Protection website at: www.consumerprotection.utah.gov

For media enquiries contact:
Jennifer Bolton
Public Information Officer
Utah Department of Commerce
(801) 530-6646 office
(801) 652-8322 cell
Follow us on Twitter @UtahCommerce