Additional Fraud Alerts

Home and Office Router Security: VPNFilter Malware

(June 14, 2018) The United States Computer Emergency Readiness Team (US-CERT) recently sent out an alert identifying that foreign cyber actors have compromised thousands of home and office routers worldwide. The actors used VPNFilter malware to target small office/home office (SOHO) routers. The malware is able to collect intelligence, exploit local area network (LAN) devices and block actor-configurable network traffic. Read the full article here.

Equifax Cybersecurity Breach

(September 8, 2017) Due to the recent breach of Equifax Cybersecurity, we encourage all members to closely monitor their accounts for suspicious activity. If you notice anything irregular, please contact our eCommerce department at 937-225-6800, option -0-, or 800-762-9555, option -0-. For more information on the Equifax breach you can visit equifaxsecurity2017.com, as well as consumer.ftc.gov.

Ransomware Cyberattack: Petya/Petrwrap malware

Preventive measures for ransomware

(June 30, 2017) The current ransomware outbreak associated with the Petya/Petrwrap malware family is similar to the recent "WannaCry" cyberattack that will encrypt files on a computer, rendering them inaccessible unless a ransom is paid. You should continue to be aware of email phishing and non-reputable websites. Read the full article here.

Ransomware Cyberattack: "WannaCry"

Preventive measures for ransomware

(May 16, 2017) The serious cyber threat called "WannaCry" has impacted many organizations worldwide, so it's important to be aware of this issue and watch for malicious activity to mitigate the risk of an attack. Read the full article here.

Google Docs Phishing Scam

Phishing Scam Targets Gmail Accounts

(May 4, 2017) A phishing email attack targeting Google users impacted organizations and individuals across the country. Reports indicate that Google has shut the attack down, but not before as many as 1 million users were affected. Read the full article here.

NCUA Warns of Fake Check Scams

Consumers Should Be Vigilant and Avoid Depositing Checks from Unknown Parties

ALEXANDRIA, Va. (April 10, 2017) - Consumers should be on the lookout for fake check scams, the National Credit Union Administration warned today after receiving numerous inquiries from consumers. Read the full article here.

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.**