



PRESS RELEASE

Common Goals, UNCOMMON SERVICE.

Contact: Gloria Thomas
502-564.4775 / 800.228.6420, Extension 5578
Email: gthomas@cwcu.org
Date: June 19, 2008

Commonwealth Credit Union Responds To Phishing/Vishing Attacks

As you are no doubt aware, Commonwealth Credit Union has been targeted by a steady stream of Identity Theft scams over the past few weeks. These have taken the form of both phishing (email based) and vishing (phone based) scams and have been in the form of \$100 offers for completing surveys to phone messages indicating that accounts have been (or will be) closed unless the person goes to a website to enter certain financial information. Kentucky Attorney General Jack Conway has issued a statement concerning these attacks, which are being investigated by the Attorney General's cybercrimes unit.

Commonwealth Credit Union's Records Have NOT Been Breached

It is VERY IMPORTANT to note that these attacks are NOT the result of your information being obtained or stolen from Commonwealth Credit Union. Our records have NOT been breached, hacked or stolen.

Why Are People Getting Phished or Vished?

When it comes to phishing scams, credit unions in general are much easier targets than banks because of field of membership. The phisher needs their scam to appear as legitimate as possible. Part of that is to target potential victims as accurately as possible. It's nearly impossible to know who does business with a bank, but it's relatively easy to determine who is a potential member of Commonwealth Credit Union. We serve participants in Kentucky's government retirement systems. Therefore, scammers have figured out that people who work for Kentucky state government are likely to belong to our credit union. They have used this information to determine that anyone with an email address that ends with "ky.gov" is probably a credit union member or potential member. Therefore, most of the attacks have targeted state employees or individuals within their email lists. As you may know, state employee names are available via various sources, including the internet (such as whitepages.com). It is not difficult to use this information to develop a database with all the email addresses of state government employees. This list is now apparently in the hands of many different phishers, each of whom is sending fraudulent emails in the hopes that someone will respond and reveal their personal financial information.

What Is Commonwealth Credit Union Doing To Fight This?

First, we are using multiple procedures to ensure that your financial records are kept safe and that no unauthorized people have access to your files. Per federal regulations, Commonwealth Credit Union has implemented all the best practices issued by the National Credit Union Administration (NCUA), the federal government agency regulating credit unions, and the Federal Trade Commission to fight the battle against identity theft.

Second, we have ongoing employee training and mandatory independent auditing of our procedures to ensure the highest security standards are in place. We have invested multiple resources and utilize the latest technology and expertise to ensure your safety and security.

Third, we are working with appropriate agencies to shut down all fraudulent web sites and phone numbers that are being used for phishing or vishing. These efforts are ongoing as we learn of new attacks against our members. We encourage you to contact us at our published phone numbers (800.228.6420 or 502.564.4775) if you receive a suspicious email or phone call so that we can work to shut down these fraudulent web sites and phone numbers.

Fourth, we are among the first financial institutions anywhere to have a Fraud and Loss Prevention Department (and the ONLY financial institution in this area) that works specifically to help members who have had their identity stolen or been victimized by a phishing or vishing scam. Our staff also utilize the latest early fraud detection software to stop fraud as soon as it is detected.

Finally, we are working to EDUCATE YOU so that YOU can protect yourself if you receive an email or phone scam.

For more information, go to our website at www.ccuky.org and click on the Scam Alert icon.

###