



**AITKIN**  
18 First Street N.E.  
Aitkin, MN 56431  
218-927-3789  
FAX: 218-927-2586

**DULUTH - MILLER HILL**  
1600 Miller Trunk Hwy  
Duluth, MN 55811  
218-625-8500  
FAX: 218-727-1459

**CLOQUET**  
101 - 14th Street  
Cloquet, MN 55720  
218-879-3304  
FAX: 218-879-0018

**DULUTH - SPIRIT VALLEY**  
215 N. 40th Ave. W.  
Duluth, MN 55807  
218-625-8500  
FAX: 218-624-1571

**DULUTH - CENTRAL**  
630 E. 4th Street  
Duluth, MN 55805  
218-625-8500  
FAX: 218-727-4426

**McGREGOR**  
149 W. Hwy 210 • PO Box 457  
McGregor, MN 55760  
218-768-3607  
FAX: 218-768-4348

## **COMPUTER VIRUS ALERT**

March 9, 2010

Members Cooperative Credit Union has been informed that a member has been infected with a Trojan virus. This particular virus typically targets an audience, thus it is critical for us to educate our members on this threat.

Recently, a number of financial institutions utilizing online banking systems have reported incidents of browser-based viruses infecting end-users. In the last year, Symantec alone has detected over 154,000 computers as being infected with the Zeus Trojan and 70,330 unique variants of the Zeus Trojan binary. These incidents are on the rise. These viruses are causing online banking websites to display a pop-up screen asking users to submit additional information for verification. The viruses do not change the URL line, making them even less conspicuous.

The Zeus Trojan is designed to steal login credentials to bank sites, social networks and email systems. The malware is typically installed on a computer by a person clicking on a link that looks like something they are familiar with and then it downloads to their computer.

The virus essentially takes over the Internet browser that the member is using and captures data as information is entered as well as routes the member to websites where the thief requests further information. The Zeus Trojan has a capability that allows criminals to add fields to the form, such as fields for additional authentication information for a financial institution website which are routed back to the criminal. Fraudsters also can alter the display to fool users into thinking all their money is still in their accounts.

It is critical for our members to keep their anti-virus software up to date. If our members are being prompted additional questions such as debit card number, PIN number or any information that is out of the ordinary, they are likely infected with this virus and should no longer use the computer to do any type of online transaction activity. The computer is at risk and they will need to work with a vendor to extract the virus before using the computer further.

Members should take every precaution to know with whom they are dealing with whether online or via the telephone. If any activity seems suspicious, members should cancel the online session immediately. Please contact MCCU with any questions or concerns regarding the information provided in this alert.