

Online Safety Notice

Be on the lookout for suspicious activity.

What 's Going On?

Some members have reported seeing extra security questions when they attempt to sign in. These questions ask for personal account information, and are not the usual security questions asked by Florida Credit Union. Florida Credit Union (and other financial institutions) will not ask for this information as part of the login process. Online criminals are about to steal information from you right on your computer. Installed on your computer is a newer breed of malware (Trojan) called crimeware, and more than likely a trojan called Zeusbot (or Zbot, depending on the antivirus manufacturer). This malware sits locally on your computer and waits for you to log into your home banking using your multifactor credentials. It gathers information such as login, password, and any other information that you may share in the login process.

These criminals are not only looking to compromise your ATM/Debit/Credit card, but ways to siphon money out of your account as well. This crimeware is sitting on your computer attempting to gather home banking information that they will encrypt and send to themselves to login later and gather information about your account to attempt to get wired or otherwise withdrawn from your account and forwarded to a "money mule" in an attempt to get it out of the country.

We have much more detailed information at www.flcu.org. Click on "Security Update" to see samples of crimeware in action.

What should I do?

If you are asked for "new" security questions or card numbers, stop right away. Do not enter any data. For proper precautions, we recommend the following steps for the security of your accounts and private information.

1. Contact your financial institutions. Not only should you contact Florida Credit Union, but other financial institutions as well. This crimeware is notorious for capturing online credentials.
2. Download anti-malware software from sites like www.malwarebytes.org, www.safer-networking.org, or another source other than your general antivirus program for removal. In addition, many of the antivirus providers will give you instructions on how to remove it manually.
3. Consider dedicating a machine exclusively for your financial transactions. As prices for computers continue to drop, one can inexpensively dedicate one machine for sensitive financial transactions such as online banking and/or bill payment. Alternatively, using software to create virtual machines (such as VMWare or Parallels), a virtual machine can be dedicated to your home banking transactions, reducing your risk online. (cont. on back)

Online Safety Notice

Be on the lookout for suspicious activity when you sign on to your FCU Home Banking.

How do I know the crimeware is gone?

By following the advice of antivirus companies and by using multiple anti-malware products, one can be fairly certain that the crimeware is eradicated from their computer, as long as the restore points that are known to be infected are removed as well. To obtain 100% certainty, one should back up personal files (such as documents, music, etc) and reinstall the computer's operating system. This is the most destructive and time consuming method, but also the most certain method of eradication as well. That being said, you should be able to gain a fair degree of confidence that the malware is eliminated by taking the first suggestion.

How can I block this in the future?

Modern banker malware, also known as crimeware, is now fully capable of bypassing the two-factor authentication obstacle by doing a simple thing - patiently waiting for the crimeware-infected victim to authenticate himself in order to abuse the access in real-time. This crimeware is written with support of organized crime in order to perpetrate financial crimes and identity theft. Writers of the software will oftentimes use services (not unlike legitimate organizations) to verify that their software is robust and will remain effective for some time. Many security personnel believe Eastern European mafia is likely involved (at least financially) in the crimeware.

How can I block this in the future?

One of the best ways to reduce your chances of being infected is to not click links in emails. This is one of the major methods to propagate most of this crimeware, though it has also been known to be delivered via compromised web ads. In many cases, user interaction is still required for installation. Finally, avoid surfing the Internet from an administrator type account. Many modern operating systems (Windows XP, Vista, and 7, along with Mac OSX and the other Unix based systems) will allow you to have multiple accounts, including what is called a limited account. Use your limited accounts for most of your day to day work, but use the administrative account to install programs on your computer when you need to, and from good known sources.

Should I close my account?

This is a decision that you may want to consider. This is dependent on whether or not there is an indication that online criminals are attempting to access your account. At a minimum, we should work with you to change your online credentials and monitoring for further signs of unusual activity.

*For more information, visit www.flcu.org/security_alerts.asp
or call (800) 284-1144.*