Multi-Schools Federal Credit Union

FAQ concerning our newly updated website:

When I select On-Line Banking and a few other links on the Credit Union newly designed webpage, I receive a message that says I am leaving the MSFCU's website. The message further states that I am linking to an alternate website not operated by MSFCU. Who is operating the home banking if it isn't the credit union? Is it safe to click OK?

The Credit Union Core Processor (MY CU Services) operates the home banking for our credit union and many other credit unions. They have handled all of our processing, including our on-line banking, for almost 20 years. ***Rest assured it is definitely safe to click OK and proceed to Home Banking***. My CU Services that designed and services our new web page is following federal regulation guidelines to protect you.

When you click on OK to confirm that you want to open the Home Banking page, notice the URL: https://creditunionhomebanking.com/hbv3/hb146/

Secure Sockets Layer (SSL) certificates, sometimes called digital certificates, are used to establish an encrypted connection between a browser or user's computer and a server or website. The SSL connection protects sensitive data exchanged during each visit, which is called a session, from being intercepted from non-authorized parties. Nearly all current browsers are set up by default to accept SSL certificates from most established certificate authorities, and to notify you when you are entering or leaving secure sites, including secure areas of comprehensive sites.

When the URL of any website begins with "https" instead of "http" it means the site is secured using an SSL Certificate (the s stands for secure). SSL Certificates secure all of your data as it is passed from your browser to the website's server. To get an SSL Certificate, the company must go through a validation process.

However, there are a few different levels of validation—and some of them are easier to get through than others. The lowest level of validation, Domain Validation (DV), simply validates ownership of the domain and not the legitimacy of the organization requesting the certificate.

The highest level of validation, Extended Validation (EV), is the safest and most extensive. With Extended Validation the company requesting the certificate has to prove their identity as well as their legitimacy as a business. You can tell if a site has an EV certificate by looking at the address bar. Browsers show a ***green address bar*** with a lock icon for websites with EV certificates, as shown in the picture below.