

Using Safe2Login

How do I use Safe2Login?

On your first visit to a Safe2Login protected banking server, you will go through a quick registration process. Part of the registration process will identify your computer with a short name like "My Laptop" or "Work PC." Once you are registered, Safe2Login uses a browser cookie to do its job with no further interaction from you, unless you clear your browser's cookies or use a different computer. In some cases the browser cookie will clear automatically.

How will I know that I am on secured PCU Online Banking login page?

Since each banking server protected by Safe2Login is known to the Safe2Login system, you are alerted by the safety image when the address of the banking server changes.

Will my web browser prevent me from using Safe2Login?

The Safe2Login system is compatible with most web browsers and does not use third-party cookies, which most browsers now block due to advertising abuse.

How does Safe2Login protect me?

Safe2Login acts as a third-party trust authority, verifying the user and the banking server through the use of a mutual authentication protocol. It does this by creating secure communication channels between the banking server, your computer, and the Safe2Login.com server, and by providing a dynamically-generated graphical image containing the special word or phrase chosen by you during Safe2Login registration. This "SafeCode" is stored securely at Safe2Login.com.

Safe2Login does not alter the website's existing login process. It serves as a first line of defense for the login page itself and simply notifies you if the "coast is clear" to enter your PCU Online banking account's user ID and password.

Registration

Am I required to register with Safe2Login before I can log in to PCU online banking account?

Yes, to assure your login security, your financial institution will require you to register with Safe2Login before you can access your online banking account. This extra step will provide security and help prevent accidental login to an authorized site masquerading as your usual online banking site.

What are the steps in the Safe2Login registration process?

First you complete the Safe2Login registration form, and then you check your email for the Safe2Login confirmation. Once you've received the confirmation, you will need to activate your account. Once your account has been successfully activated, you will be able to identify the computer by giving it a name. After those steps are all completed, you can use the Safety Stamp whenever you want to log in to your online banking account.

What information will I need to register with Safe2Login?

You will need your email address where you'd like to receive any Safe2Login-related information and your date of birth.

Should I use the same password for Safe2Login as I use for my online banking account?

No, creating a different password for your Safe2Login account will help ensure that your online banking password is kept safe.

How will I use the SafeCode that I create?

The SafeCode will appear in the Safe2Login Safety Stamp on the PCU Online Banking login page. You will be challenged to select your SafeCode from a list of SafeCodes before you are able to log in to your online banking account.

What makes a good SafeCode?

A good SafeCode is a word that you can easily remember and must be between 6 and 12 characters in length.

How will Safe2Login use my registration information?

Your registration information will only be used to contact you for the purpose of providing information relating to your Safe2Login account. Any information that identifies an individual user will never be sold or distributed. Safe2Login uses a cookie set by your financial institution's server to identify your computer. This cookie will not be used for any other purpose and contains only an encoded key that identifies the computer on the Safe2Login system.

The Safety Stamp

What is the Safe2Login Safety Stamp?

The Safety Stamp is the face of the Safe2Login product and presents a sequence of individual security checks, all of which must succeed before your personal security code, or "SafeCode" is displayed. You are challenged to select the correct SafeCode from a list of SafeCodes, before access to the PCU Online banking login fields is granted. The Safety Stamp lets you know when you are safe to log in.

What information can I find on the Safety Stamp?

The Safety Stamp is your guide to safer online banking. You can look to it to find out what server you are logging into, which authorized computer you are using, and where you are in the login process. It will also let you know when all the Safe2Login security checks have been passed and you are safe to log in.

What if I am already a member of Safe2Login, but the Safety Stamp doesn't recognize me?

When the safety stamp doesn't recognize you, it will look like this:



Simply click on the link on the Safety Stamp and log in to Safe2Login. Once you've done that, you will be returned to your online banking login page where you will be able to verify your SafeCode and then log in to your online banking account safely.

What if I don't see the name of the computer I am using on the Safety Stamp?

If you don't see the name of the computer you are using on the Safety Stamp, do not proceed with your online banking login and notify your credit union immediately. Seeing the name of your computer on the Safety Stamp is your assurance that you are safe to continue.

What if my SafeCode is not listed on the Safety Stamp?

If your SafeCode is not listed, someone else may have logged into Safe2Login on the computer you are using. If this is the case, you'll simply need to click on the link that says "Click HERE if your SafeCode is not listed" to log in to your own Safe2Login account.

How will I know that I am safe to log in?

You are safe to log in to your online banking account when the Safe2Login Safety Stamp indicates that all the security tests have been passed and that you are "Safe2Login." You will also see green lights for server, session, and computer. If you don't see three green lights on the Safety Stamp, you are not safe to log in yet.

What if I don't see the Safe2Login Safety Stamp on my online banking login page?

If you are expecting to see the Safety Stamp and it's missing, notify your financial institution immediately.

Logging in to Safe2Login

Once I am logged in, what changes can I make to my account information?

You may unlock your account, register a new computer, or update your email address. You are also able to change your password, SafeCode, or computer name.

What if I am using a different computer than usual?

You will be offered a chance to "Add a new computer" during the login process. You may name each computer anything you want, but are limited to 12 characters.

Why do I need to identify my computer?

The computer name you provide will appear on the Safe2Login Safety Stamp on your banking login page. Seeing the name you chose for your computer will assure you that you are safe to proceed.

Will I be locked out of my account if I forget my SafeCode?

If your incorrect attempts to verify your SafeCode on the Safety Stamp exceed the 3 attempts, you will be locked out of your account. Follow the instructions on the Safety Stamp to unlock your account.

What browsers can I use with Safe2Login?

Safe2Login is optimized for the newest versions of Microsoft Internet Explorer, Netscape, Firefox, Opera, Safari, and Camino. Safe2Login may not be compatible with text-based browsers for impaired or disabled users.

About the Safe2Login Product

What is Safe2Login?

Safe2Login complements a financial institution's existing online banking login process by employing mutual authentication and device authentication as a safeguard against malicious emails and fake websites. Safe2Login is a way to assure an online banking user that they are, in fact, logging into the correct website.

Why do web sites need Safe2Login?

Safe2Login prevents identity theft that can result from phishing and pharming attacks by verifying the identity of the online banking server, as well as the identity of the online banking user's computer. This verification process, called "mutual authentication" assures the online banking user that they are logging into the correct web server and therefore will not be putting any of their personal information at risk.

What are phishing and pharming?

"Phishing" is when a fraudulent email is sent to an individual that prompts them to log into a malicious website and provide personal information ranging from online banking usernames and passwords, to account numbers, to social security numbers. The "phisher" creates an email that looks like it is coming from a legitimate source, often a credit union or bank.

"Pharming" is when the fraudulent individual replicates the website of a financial institution or other organization in an attempt to collect personal information from users.

Used in conjunction with each other, phishing and pharming can be detrimental to online banking customers and to a financial institution's reputation. The malicious sites and emails are often indistinguishable from the sites they are mimicking and can fool even seasoned internet users.

How does Safe2Login defend against phishing and pharming Attacks?

Safe2Login.com acts as a third-party trust authority and verifies the identity of a web server. It does this by creating a secure communication channel between the banking server and the Safe2Login.com server and providing a dynamically-generated graphical image containing the special word or phrase chosen by the online banking user during Safe2Login registration. This "SafeCode" is stored securely at Safe2Login.com.

Why does my financial institution's web site need Safe2Login's multi-factor authentication?

According to the Federal Financial Institutions Examination Council (FFIEC), single-factor authentication (such as simple username and password) is no longer adequate to secure online information. Multi-factor authentication should be used to increase the level of security. Safe2Login employs mutual authentication and several layers of user authentication to prevent phishing sites from easily fooling internet users, as well as to prevent unauthorized account use.

Why does Safe2Login work?

The Safe2Login.com identity verification process consists of a sequence of individual security checks, all of which must succeed before the user's personal security code is displayed, granting accessibility to the banking login screen. Only the online banking user sees their personal security code, so a hacker can never accurately duplicate or simulate it.

Before presenting an accessible banking login field, the financial institution can verify a user's identity by comparing the online banking user's answers to varying challenges against information in a trusted database to see if the information supplied by the user matches information in the database.

Safe2Login's dynamically-generated Safety Stamp image has several layers of complexity that make it a lengthy hassle for a hacker to duplicate. The hacker will quickly decide to move on to an easier target. Safe2Login's multi-factor authentication process is also resistant to "keylogging."