BLACKHAWK COMMUNITY CREDIT UNION

ONLINE BANKING SECURITY

Protecting You and Your Account

Your visit to our Online Banking site is safe and secure. We employ a 'layered approach' of multiple barriers between your account information and the outside world rather than just a single level of security.

We utilize such measures as multi-factor authentication, encryption, firewalls, intrusion prevention systems, around-the-clock proactive monitoring, routers, demilitarized zones and antivirus protection.

Below is a general overview of what we do to protect you and your account.

Multi-Factor Authentication

Multi-Factor Authentication is a system used to further identify Online Banking users beyond the Username and password.

In order to use our online banking service you must have an Online Banking Username and Password. BHCCU employees do not have access to your Password. If your Password is entered incorrectly three (3) times at the login page, your account will be frozen. You will then need to contact the Credit Union at 1-800-779-5555 to be authenticated and unlocked.

When enrolling to use the Online Banking product, you will be prompted to choose a Username, Password, and Watermark Image. A Watermark Image is a user-selected image that is used as an anti-phishing device and also assures the user that they have logged into the legitimate Online Banking site.

When you login, your Online Banking Username and Password are transmitted via a secure session between your browser and our servers. Your information is 'scrambled' (please see Encryption below) and then sent to our online banking servers where it is 'descrambled' using a unique and temporary key.

One of the first times you access your accounts, you will be asked to choose and answer three (3) Personal Verification Questions. During future online sessions, we'll ask you some of these questions if we feel there is a possibility that someone other than you is attempting to access your information. You may be asked questions when you log into Online Banking from an unusual location, you complete a transaction that is outside the norm, or you exceed a certain dollar amount.

You will be allowed three (3) attempts at answering the challenge questions before you are blocked from the computer or phone on which you failed the question. You will then need to contact the Credit Union at 1-800-779-5555 to be authenticated and unlocked.

Encryption

We require the use of a secure browser to access your account online. Your browser must be equipped with SSL (Secure Socket Layer) with a 128-bit or higher encryption algorithm to communicate with our servers.

SSL protects against eavesdropping and data tampering during transmission. To check the security status of a web page, look at the URL in your browser window. You will see an "s" added to the familiar "http" (to make "https"). This indicates that SSL is in effect for the current page.

There are trillions of possible key combinations and each time you connect to Online Banking a new key is utilized.

The access to eStatements from Online Banking is secure. Not only is your account number masked (does not show full account number), but the query encrypts account information with the Advanced Encryption Standard (AES). This is the same standard that the Federal Reserve uses to transfer funds between member banks. eStatements, at rest, are fully locked up with AES and are never stored as plaintext files on the server.

Please note that BHCCU never transmits your information without it being encrypted beforehand.

Network Security & Monitoring

We utilize firewalls, routers, intrusion prevention systems, demilitarized zones and active monitoring of suspicious activity against our servers. All network activity accessing our business-critical systems is logged, monitored and reviewed on a continual basis.

Session Cookies

Our servers require session cookie technology to ensure account confidentiality and security. A session cookie is a single use security object that permits you to browse within password-protected areas of our web site. The session cookie is only valid during your current login session and is automatically discarded after periods of inactivity or a log off. Please note that we never use cookies to capture any personal information about you.

Anti-Virus

We use several layers of virus detection software to protect our environment. Our antivirus software scans our network equipment, our servers

and PCs to detect and react to any virus activity that may be introduced. Our email servers also provide the same protection, scanning each incoming document for malicious code.