

INTERNET BANKING SERVICES SECURITY BAC | CREDOMATIC NETWORK

Our customer's biggest concerns are the security of the information that gets transferred over the Internet. BAC | CREDOMATIC Network has taken measures to secure and protect the information of its clients, using several security mechanisms.

Our Online Banking services use a 128-bit certificate granted by VeriSign, to encrypt data being sent over the internet. Internationally, the use of 128-bit SSL certificates is accepted as the standard for online financial services. Information such as: personal information, passwords, account numbers or credit cards are encrypted so that they cannot be seen by third parties and also the certificate gives the user the certainty that he is communicating with our server and not with an imposter server.

User access passwords in the Online Banking site are encoded using a special encryption hash mechanism based on DES technology. The information stored on our databases is a specific subset of that hash. The process of authentication or access to the Online Banking site takes the password typed by the user and compares it using the hash algorithm against the registry of keys in the server. Using this method we ensure that neither the password, nor the complete "hash" result is stored anywhere in the system.

Another Security mechanism we use in the Online Banking is the maximum number of failed attempts to login. When a user tries to enter the Online Banking system, the system will lock the user if the number of failed attempts is exceeded. This prevents the use "brute force" attacks, since the user cannot be unlocked until the authorized account holder or user authorizes to activate it again.

The Site's security is not only setup with software solutions; we also have designed our network to prevent unauthorized access. Customer information and their accounts are stored in databases within a protected area of the network that is not visible externally. The web servers are in a single public area known as demilitarized zone (DMZ) and are the only visible servers on outside networks, they do not store any type of sensitive information, plus they also have a strong level of protection.

The servers are protected by Industry Recognized Firewalls in 3 tiers and have Intrusion Detection Systems that alert and block all unauthorized activities with minimum impact to the network performance. The Internet servers play a mediating role between the client and the systems that maintain the information databases; since they only give the information that the client is authorized to see. Our firewalls and IDS's are oriented to reinforce a safe access between the internal network of company and the Internet. In addition they are extremely stable and have high availability.

To ensure the quality and security of our service we have highly specialized people working to design, maintain and constantly reinforce our site security. Our personnel are trained not only in the administrative tasks of maintaining the sites but also in security risks and actions needed to mitigate these risks. Our personnel are up to date on security, technical vulnerabilities and techniques to combat intrusive actions, and periodically receive training on new techniques and best practices.

Our personnel have taken these and many more measures to strengthen the security of the Internet sites, nonetheless to not fall in subjective criteria; we periodically contract external audits to test our site's security, using internationally recognized leaders in Internet Security Consulting.

BAC | CREDOMATIC Network strives to make the Online Banking system, friendlier and easier to use, oriented to companies with multiple banking operations with the BAC Financial Network. This permits a single user to have all product groups under a same interface. The system permits Multi-accounts and Consolidated Accounts, also companies can assign a single master user and grant privileges to sub-users.

The Online Banking system provides still greater levels of security. The capacity to grant specific privileges to each user ensures a greater level of control of the banking operations that each user of the system can execute. A set of online logs, detail the actions made by users while logged in to the system. In addition the Online Banking system offers use of alphanumeric passwords and Passwords expire after a certain time period. The Online Banking system also offers a service which allows users to send emails to the participating financial institutions while logged into the system, providing authenticated communication between customers and our company.

The Online Banking system also controls user sessions that time out having the user retype the password to continue, thus improving security by logging off users who leave their sessions open. These sessions are held on the server side and are not transmitted to the user thus preventing session hijacking, and are erased as soon as the user logs-off or closes the internet browser. This way, no stranger can conduct operations without previously identifying himself.

As an additional safeguard our employees are not authorized to ask for customer passwords.

These are just some examples of the efforts made by our team to give an efficient, safe and reliable service to you.

Sincerely,

Internet Team
BAC | Credomatic Network