

## How to Backup and Protect Your Bankcard Pros CRM Database

Your CRM database is one of your most critical business assets. By putting the right security measures in place, you can protect your CRM database and avoid problems that could negatively impact your ability to deliver a quality customer experience.

You can also get more detailed information on backup information from this website

<http://en.wikipedia.org/wiki/Backup>

Your CRM database is a valuable asset that stores large volumes of highly confidential customer information, and houses the vital intelligence that sales, marketing, and support staff need to effectively interact with existing and potential clients.

In order to achieve your CRM-related goals, you need to put the right procedures and technologies in place to protect your CRM database from security breaches, performance problems, technical failures, and other issues.

### **24 x 7 Availability**

If your CRM database goes down, your ability to perform routine customer-facing activities will be severely hindered. The keys to ensuring that your CRM database is accessible - and operating at its peak - at all times are around-the-clock monitoring and system redundancy.

By continuously tracking the performance and availability of your CRM database, you can maximize uptime by instantly identifying any problems and taking immediate corrective action. Mirroring and redundancy can help you avoid downtime in the event of a major system failure, by providing you with an exact duplicate of your CRM database that can be rapidly "brought up" when needed.

### **Data Security**

The information contained in your CRM database is one of your most important competitive resources. Additionally, your customers need to feel confident that their private and personal information - such as credit card numbers, social security numbers, or any other data they share during business transactions - won't fall into the wrong hands. Therefore, maintaining the integrity of your sensitive and confidential customer data is crucial.

While there is no way to create a completely failsafe environment, there are plenty of measures that can be taken to dramatically enhance CRM database protection.

For example, multiple levels of login authentication can help you prevent unauthorized access. Role-based security, which enables users to view only certain portions of the data based on their job function, can help ensure that all customer information is handled correctly.

And, securing your CRM database with data encryption and firewalls can significantly minimize the risks caused by hackers other cyber-criminals.

If your company has chosen an on-demand CRM system, you'll need to work closely with your service provider to ensure that, even though your CRM database may not be physically separated, there are plenty of safeguards in place to keep other clients from getting to your information. Additionally, you'll

need to make sure that the service provider promptly installs any application, database, or operating system patches to keep security optimized.

**Here are a few questions to ask yourself as a business owner when it comes to your Bankcard Pros CRM data backup and security:**

**Q: How will I know to back-up my CRM software?**

Answer: As a system administrator user, when you login to your Bankcard Pros CRM software, you will see a red blinking box that says “Backup Database”. This will appear if the system recognizes that you have not backed up your data for 2 or more days. It is highly recommended that you **DO NOT** ignore this warning, or disable this feature in the configuration section of the CRM. Always perform the backup procedure on a daily basis.

**Q: What exactly should I backup?**

Answer: First of all, you must backup your data from your MySQL database program on a **DAILY** basis, which can be done on your own in the setup/configuration section of your CRM software, using the Database Backup tool. The system will save all your data into a text file like “backup\_yourcompanyname.txt”

Secondly, you need to back-up all the physical files from your hosting account. This can easily be done using a file transfer program called CuteFTP software program for example. You can get instructions on doing this from this website <http://www.globalscape.com/support/genusage6.aspx> .

The main folder that you always want to back-up on your hosting account is the /corp folder. This should be backed up on a **DAILY** basis. This folder contains all the files, marketing materials, docs, contracts, etc. that you uploaded in the leads section, document download library, status section under each merchant, and so on. But it is a good idea to back-up your entire CRM site at least on a monthly basis.

**Q: How do I backup my database?**

Answer: This video will teach you how to manage your daily backups of your CRM data: <http://www.youtube.com/watch?v=Ra1fx8vSLlc>.

It will teach you how to back-up your data from your MySQL database program on a **DAILY** basis, which can be done on your own in the setup/configuration section of your CRM software, using the Database Backup tool.

**Q: Where do I store the files of my database?**

Answer: The system will save all your data into a text file like “backup\_yourcompanyname.txt” and will probably be around 10MB and up to 50MB in size. If you have been using your CRM software heavily for 1-2 years, the file could easily be 200MB or more. It just depends on how much data you import and add each month.

When you backup your database, you need to save the file to your computer desktop, preferably in your “My Documents” folder under a new folder called “CRM Database Backups”

**Q: How often should you backup your database?**

Answer: It should be a strict company and employee policy to back-up your database on a DAILY basis. Make sure the employee responsible for this task understands that failing to perform this task can be subject to termination.

**Q: How many copies of the backup should I store?**

Answer: Depending on how valuable this data is and how many employees rely on your CRM on a daily basis, it would be recommended to always have 3 copies of your database and CRM files. (1) On your computer in your documents folder, (2) another copy on a USB drive that you can store in a safe, and (3) a copy you should burn on a DVD disc.

**Q: Where do I store the backup files?**

Answer: The CRM software allows you to download the text file and save the data file on your computer in your “My Documents” folder. Make sure your computer requires a password to login. Also, make sure your computer will automatically log out after 10-30 minutes of inactivity. Make sure your computer is in an individual office and you close the door and lock it with key when you leave your office at all times, like lunch or when you leave for the day.

**Q: Who should be in charge of managing your database, hosting account, and server?**

Answer: It is highly recommended that you hire a certified IT person to manage your database backups, or hire a professional firm to manage this for you. This person or company should be a highly qualified, educated, and experienced to handle your IT needs. It is not recommended that you allow a manager, sales rep, receptionist, etc. to perform these tasks. If they do not know what they are doing, it could result in a loss of data and be devastating to your business, especially if you have a call center with dozens of sales reps or telemarketers calling on thousands of leads in your CRM software.

**Q: How do I trust the person managing and backing up your database?**

Answer: The two questions to ask is, “Can I trust this person?” and “Is this person capable of managing our company’s IT needs without making any devastating errors with the CRM, hosting accounts, or servers that could result in loss of data?” Even if you trust an employee, it is recommended you put in place business policies as if you do not trust anyone, just to be safe.

It is highly recommended that you perform a credit/criminal background check on the IT person to make sure they have no past issues like theft or felony convictions. It is also important this person has the education, experience, and training to properly manage computers and servers in the IT career field. Check their references as well as past employment history with other companies. Check to make sure they have High School diploma, college diploma, training certificates, and other certifications in their career field. Never go by what they tell you in the initial interview and what their resume says. They must provide you all the documentation, references, and so on.

**Q: How do I secure my computers at my office from unauthorized access?**

Answer: It is highly recommended that you add a password protection to your business email program, like Microsoft Outlook Professional 2010. In regards to all the computers in your company, it is highly

recommended that you treat each computer with the same security as a business server. Make sure all your computers are running Windows 7 and all computers are up to date with all Microsoft updates. Make sure all computers are running Microsoft Security Essentials antivirus and firewall software. This is free from Microsoft. Make sure your internet access routers or wireless routers are password protected with a new password other than the default password. Make sure all computers require password in order to login and get to the Windows 7 Desktop. You should also set the Windows option so the computers will automatically log out after 30 minutes of inactivity, and require a password to be able to access the computer again. This will insure employees are unable to access other employee computers at any time.

Make sure all your computers do not have USB ports or DVD writers installed making it easy for any employee to steal company data, especially via USB drives which are the easiest way to copy tons of data within minutes.

If an employee is no longer with your company, immediately change all passwords to the computer and his/her email so they will no longer be able to access anything. Make sure the employee does not have any keys to your office. Since keys can be duplicated, it is highly recommended you change your locks to your office with new keys immediately.

**Q: Should I store credit card info on any of my computers or servers?**

Answer: Never! This is in violation to the PCI security regulations. If you have paperwork faxed to your office via FAX or Email, these documents should be stored in a safe, or properly destroyed or shredded. These documents should be received and managed by 1 employee only as you should not allow sales reps and telemarketers to receive, handle, or store paperwork with customer's credit card info.

**Q: How can I prevent my employees accessing our CRM from home or any other location other than our office?**

Answer: Each user profile has a feature that will allow you to restrict the user from logging in from multiple locations. If you add the IP address of their computer at your office, then that user will only be able to login from their computer at work only. If they try to login from home which is using a different IP address, their access will be denied.

**Q: How can I prevent my employees from providing confidential login information to other individuals not associated with our company?**

Answer: Each user profile has a feature that will allow you to restrict the user from logging in from multiple locations. If this employee provides their username and password to another individual outside the company, they will never be able to login because the username is only allowed to login from a specific computer with a specific IP address.

**Q: My company has 12 computers, should I back all the computers as well?**

Answer: You should always backup all computers on a daily basis. You should have a server with a software program that will back-up all computers automatically on a daily basis. The backups should include all "My Document" folders on each computer as well as the Outlook email .pst files for each

employee. You should also backup the server as well. Any IT person or company you hire will be able to explain all this in detail and provide you all the options.

## **Back Up and Disaster Recovery**

Answer: The loss of mission-critical customer data could be detrimental to your business. Are you prepared for a major disaster?

A well-designed disaster recovery plan will allow you to retrieve the information stored in your CRM database if something happens. Back up your CRM database at least once a week (although most experts recommend a daily back up for the utmost protection). It is also preferable to back up to a server in an off-site location. While an on-site back up will enable you to quickly restore your data after a power surge or a system collapse, it will do you no good in the event of a fire or flood.

## **Why is Computer Backup Important?**

If you've ever been in a situation in which you've almost completed an important project, only to have your computer spontaneously crash seconds before hitting the "save" button, you understand how frustrating losing your data can be.

Now, imagine losing all your important files - everything from business files, to family photos, to your tax returns - permanently. Although many of us prefer to adhere to the mantra of "it'll never happen to me", the truth is, it could. And as computers continue to become the principle way in which many people conduct important transactions, this type of thinking is becoming increasingly risky.

What's worse, the modern computer is ever more vulnerable to the imminent threats multiplying on the Internet - everything from adware, to spyware, to viruses. In fact, in 2003 alone, the number of computer viruses increased by 11%.

## **Do I Need to Backup All of my Computer Data?**

The short answer to this question is no, you do not need to back up all of the files on [your computer](#). However, there are certain files you should definitely backup, so that in the event your computer decides it's time is up, you won't be at a total loss.

So just what files should you be backing up? Although the choice is ultimately a personal one, here are some suggestions:

- Information and files relating to banking or other financial transactions
- Digital photos
- Purchased/downloaded music from the Internet
- Purchased/downloaded software from the Internet
- Important work/school projects
- Email contact list
- Internet browser bookmarks