Donor Database Security: Best Practices

As published in The Nonprofit Times – Volume 22 Number 4

With the recent outbreaks of security breaches in the news, it's more important than ever to ensure that your data is safe. While no system is ever 100% secure, there are many steps and industry best practices you can follow to significantly lower your risk of becoming the next victim of a security breach, data corruption, or loss of mission-critical data.
Whether your donor database is stored on your own computers or uses a hosted solution provider (such as DonorPerfect Online), here are some important practices to use or look for:

Backup, Backup, Backup

The greatest risk to your data is not really hackers; it's data loss due to computer failure, fire or other accidents. Not having a comprehensive backup plan can spell disaster for your organization. Complete backups should be performed every day, and copies of the backup itself should be stored securely offsite. There are countless examples of data loss due to fires, floods, etc. where the organization dutifully backed up their data, but unfortunately stored the backup tapes next to their computer. Hosted software providers handle daily offsite backup storage for you, but if you're not good about making backups yourself, consider an online backup service such as mozy.com or carbonite.com.

> The greatest risk to your data is not really hackers; it's data loss due to computer failure, fire or other accidents.

User ID & Password Security

Some of the most stringent data security requirements are used by the healthcare industry under the guidelines of the Health Information and Patient Privacy Act (HIPAA). HIPAA spells out many requirements for password security, including:

- Passwords should be at least 7 characters in length, contain at least one non-alphabetical character, and not be words found in a dictionary.
- Passwords should never be displayed onscreen and always stored with a high level of encryption. You should never be able to download the password file – it must be individually reset for each user.
- Passwords should expire and be changed every 60 days and User IDs should automatically expire after a predetermined date. This safeguard ensures that users who are no longer authorized do not have access to the data.

- No more than 3 unsuccessful login attempts are allowed. Once 3 attempts have been made, the User ID is inactivated and the user cannot access the system unless the password is reset by the system administrator.
- You should be able to limit data access to only certain subsets, such as Name and Address, and not include financial transactions. You should also be able to limit access for certain users to business hours Monday-Friday. Or you may want to limit access to just certain designated IP (Internet Protocol) addresses.

Audit Trails

A database system should be able to provide a security audit trail of user logins. In DonorPerfect Online, for example, we track the user id, time/date, and IP address of every single login to any of our systems. These security logs are then reviewed periodically, and any suspicious behavior is identified. Don't make the mistake of ignoring the audit trails until after you know of a security breach – in almost all cases you can stop a breach if you pay close enough attention to these logs regularly.

Physical Security

A weak link in many organizations is the physical protection of their property and databases. This not only includes protection of your servers and computers, but also protection from unauthorized access to the printed records of your database. All paper records should be destroyed (cross-cut shredding is best), including any correspondence (including the envelope) from your donors. Data identity thieves know that it is often much easier to sort through your trash looking for information than to successfully hack your systems or decrypt your password files!

User Security Awareness Training

Some of the greatest threats to your data are from hackers who can use social engineering to access your systems. Also known as 'Phishing' schemes, these unscrupulous hackers can trick your users into revealing their security credentials. That's why it's important to make sure users are aware of such schemes, and to always be on the lookout for 'official' looking email that redirects them to a rogue website to enter their credentials.

One of the easiest ways to identify a phishing attack is to be mindful of where the perpetrator redirects your web browser. For example, while an email link may display an official looking website address, hovering the mouse over the link will reveal the actual HTML address in the bottom left hand corner of the browser. In fact, this type of phishing scheme is so prevalent, that many service providers will NEVER include a link to a login page in email communications.

Securing your database systems should be a mandatory part of every organization's overall contingency planning, and in many cases it is necessary to ensure the organization's very survival. Both physical and software protections are required, and while out-sourcing your database systems to professionals can provide added security, it's still necessary to teach greater security awareness among all your users to ensure that your data is as safely protected as possible.