Protecting Your Donor’s Information in the Cyberworld

DonorSnap
Donor Management Made Easy

As with many forms of technology, the advent of the computer and unlimited access to information afforded by the internet, has proven to be both a blessing and a curse. Our society’s heavy reliance on computer technology for every day interactions, transactions, communication and data storage mandates increasing emphasis on cyber security. News coverage on data breaches, identity theft and hacking personal information are commonplace today. Cyber thieves have not only kept pace, but are often a step ahead of the latest advancements in cyber security measures.

With the explosion of personal data and interactions stored in cyberspace, most of us are more vulnerable than ever to having personal data accessed by a malevolent third party. Data is now in a format that if someone can get access it, they can then replicate it in seconds. However, getting the data is not the real issue, it is the nature of the data and how it can be used that is important.

With that in mind, the following information is usually stored in your Donor Management system, and might be of interest to cyber thieves :

- **Name & Address:** This is basically a starting point, and alone of little value to cyber thieves. A name and address is easily obtained from White pages (or an online equivalent).

- **Donation History:** Again this holds little value for a cyber thief. It may be of interest to data mining organizations (i.e. Cambridge Analytics) that use information to create a composite view of an individual’s interests and leanings.

- **Phone Number/Email:** Also of little value as it is so easily accessible. In addition to social, school and work directories, or even loyalty memberships, this information may be on social media accounts and readily sold by reputable organizations (ie. Experian – yes the Credit Checking organization will sell you this information).

- **Credit Card Number/Bank Account and Routing:** This is of great value to cyber thieves, the key to monetary gain. Once thieves have access to credit card information, banking accounts and routing numbers, they are able to purchase items, make ACH withdrawals, or even sell the information to other thieves.

- **Passwords:** Also of great value to thieves, in particular, because people tend to reuse the same password on all their sites. With the amount of accounts and devices requiring passwords today, the average individual uses the same few passwords as a sheer survival mechanism. The problem with this is exemplified by the Yahoo security breach years ago; user IDs and passwords associated with Yahoo accounts are still being sold to criminals in the dark web.

How DonorSnap approaches the security of your data:

- First, we have controlled physical access to our data servers. The servers are in a dedicated “Server Farm – building” with access limited to those with security cards.

- We employ added layers of security through firewalls and scanning software, and limit access to our database to only DonorSnap programs.

- As specified in our terms of service, we do not allow the storage of sensitive information, including Drivers License, Social Security Number, Bank Number and Credit Card numbers. Without this data, the overall risk to donors of their information being compromised is minimal, as there is nothing of real value for the hackers to exploit.

Despite DonorSnap’s security precautions, an important vulnerability remains: your username and password. Almost all data breaches are accomplished by accessing the data through approved channels. Make sure you have a unique password for every user, deactivate the user when they leave your organization and make password requirements more sophisticated (longer length, combination of numbers and characters, etc.). It is also helpful to require passwords to be changed periodically, at least yearly, an additional safeguard that is not always well received. The above precautions are necessary for being a good steward of your donor’s information, however your donors’ data may need protecting offline as well. It is common practice for copies of checks to be made, shared amongst departments and filed along with relevant donor information. These checks are often also scanned and stored on computers, providing an additional reference for accurate record keeping and accounting. However, donors’ checks display sensitive information, beyond the list of donors and amounts of their donations, that is then easily obtainable within physical office files or electronic database.

If it is important for record keeping functions to retain check copies, cover the account and routing number on the bottom before scanning or copying, the information needed to perpetrate identity theft and simple frauds. It doesn’t take particular skill or imagination to create and pass fraudulent checks or do automatic ACH withdrawal on an individual’s account, once the accurate name, bank routing and bank account is obtained. This simple practice is an easy way to further protect valued donors from having their sensitive information end up in the wrong hands. -- Dennis Mueller