



Nonprofit Tech Circle

3 Ways to Protect Your Donor Data



Who Am I?

- 13+ years in the nonprofit tech industry
- Passionate about understanding what donors want from the nonprofits they support (and what orgs can do about it)
- Writer, speaker, and marketer with Neon One





PCI Compliance

Support



SSO



Housekeeping

1

Ask questions. This should be as useful as possible for you and for your organization, so please use the Q&A box!

2

Please talk to me! I love seeing what you have to say during the session. Use the chat box to talk to me and each other.

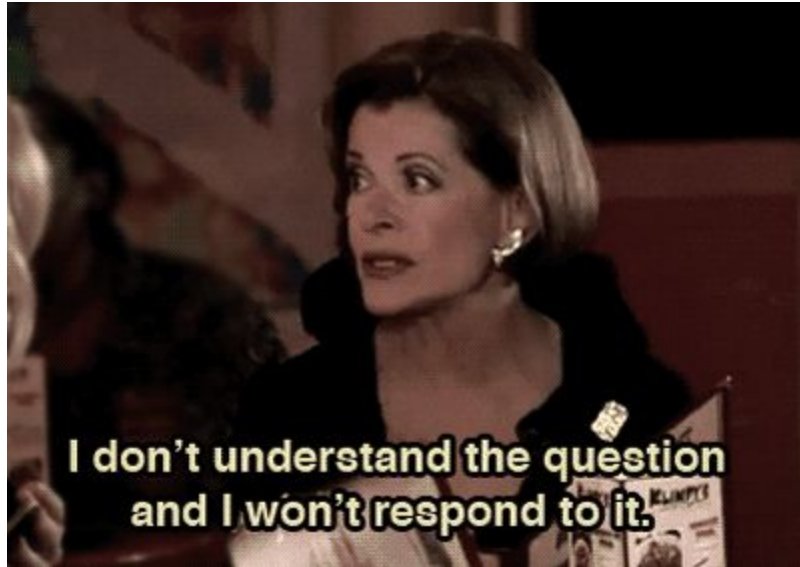
3

Yes, we are recording this webinar! You'll receive an email tomorrow containing a link to this session, the slides, and a transcript. It'll also include links to some helpful resources!



How Confident Are You About Donor Data Protection?

How confident are you about donor data protection?



I'm pleading the fifth 🙄



I'm basically Fort Knox



Why Is This Worth Discussing?

According to a recent study of data from the Nonprofit Cybersecurity Incident Repository (NPCIR):

"Up to 60% of nonprofits have experienced a cyberattack or data breach in recent years"

Data leaks can be expensive for nonprofits and a pain for donors. It's important to protect yourself!



There is always at least a *little* risk any time you store donor data.

Simple steps can help protect your nonprofit and your supporters!

Here are some straightforward ways you can make sure donor data stays safe.





1. Evaluate Your Tools

All tools are not created equal

You can safely store and use donor data in:

- ★ A CRM
- ★ A spreadsheet (probably)
- ★ Protected drives

You cannot safely store and use donor data in:

- ★ Free or personal AI tools
- ★ Openly accessible drives
- ★ Physical locations (probably)



Neither is all data

Some data is safer to store than others.

The more sensitive the data, the more careful you need to be about how and where you store it.

Some data, like payment information and other very sensitive info, shouldn't be stored at all.



Be careful with "safe" tools

Even the safest tools can be compromised by:

- ★ Outdated permissions
- ★ Leaked passwords
- ★ Improper use

Store and use donor data only where it's safe to do so, and make sure you keep those programs protected.



CRM → Protected bookkeeping platform ✓

CRM → Personal ChatGPT account ✗

Spreadsheet → Protected email platform ✓

Spreadsheet → Email to board member ✗





2. Ask the Right Questions

Evaluating your current tech tools is one thing. What about finding new tools?

Asking current or potential vendors the right questions now can save you some headaches in the future!

Here are some questions to ask any company who might touch donor data.



- ★ Is your system PCI compliant? What level?
- ★ What measures do you have in place to protect your customers' data?
- ★ How does your company handle security incidents?
- ★ How much control do I have over user permissions?
- ★ Do you have zero-retention agreements in place for any in-app AI tools?

What would you add?





3. Train Your Staff

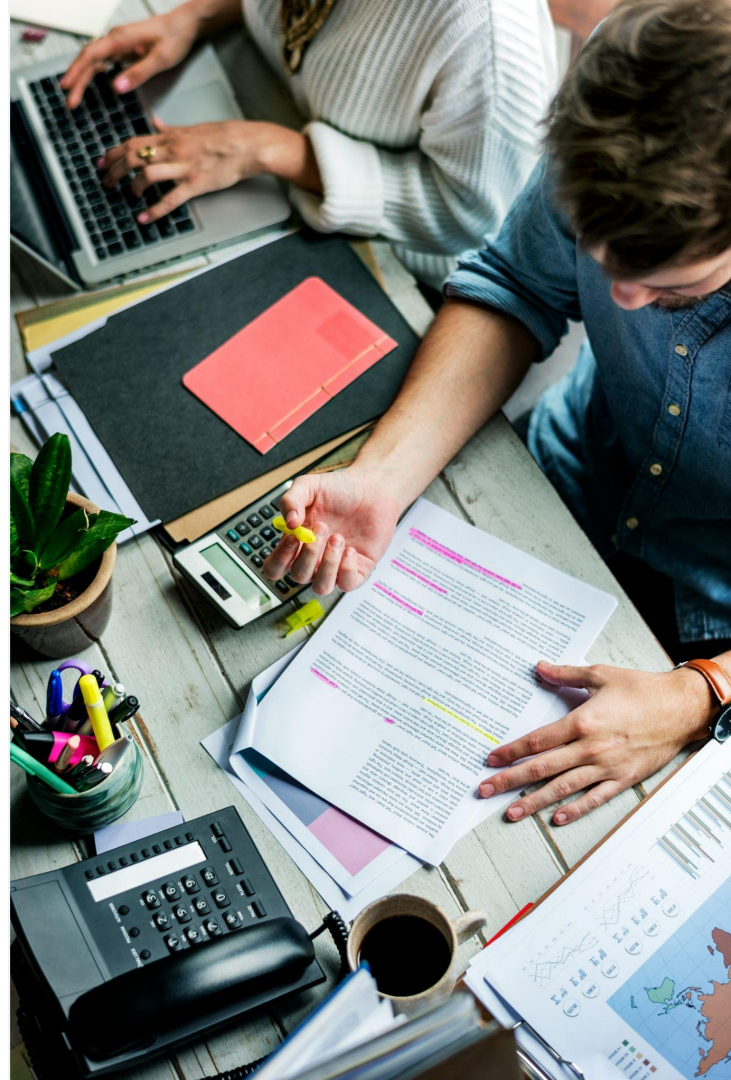
The biggest security risks aren't in tech platforms. They're humans.

Teach people at your org to minimize risk!



Simple Steps:

- ★ Update old passwords
- ★ Use a password manager (especially for shared passwords!)
- ★ Lock computer screens when away
- ★ Use file sharing links instead of emailing donor data



Intermediate Steps:

- ★ Review user permissions for your CRM and other platforms
- ★ Create an off-boarding process for departing staff
- ★ Spend time learning about phishing and other online shenanigans
- ★ Write up a simple incident response plan



Advanced Steps:

- ★ Purchase and complete an online security training course
- ★ Adopt a data governance policy
- ★ Create a schedule for regular security audits and ongoing training





The #1 Thing to Remember



There is always risk associated with storing and using donor data. But simple steps can protect your nonprofit and the people in your community.

You don't need to be an IT expert to keep everyone safe!



Questions?