United Church Funds®
Investing Together for a Sustainable World

FIDUCIARY FOCUS, APRIL 2026

SAFEGUARDING CYBERSECURITY AS A FIDUCIARY DUTY

By Matt Wagner, Vice President, Institutional Relationships

In today's environment, cybersecurity is no longer simply a technical issue; it's a core component of fiduciary responsibility.

Customer and employee personal identification information, financial and banking data and confidential trade secrets are just three examples of areas of concern for business leaders who face daily pressure from professional hackers and cybercriminals bent on stealing and profiting from cracks in the armor of cybersecurity.

Raymond Daoud, Senior VP and Chief Security Officer at CGI, a leading business IT consulting firm, noted that "With every new wave of technology, innovation tends to move faster than security. The opportunity for leaders is to innovate responsibly – moving quickly, but with intention."[1]

The nonprofit world is not immune to these security risks. In fact, nonprofit organizations have become common targets for phishing attacks, data breaches, ransomware and other threats from both external and internal sources.

In a recent article published by the Non-Profit Leadership Center, author Kadien Douglas, Managing Partner at Douglas CPA & Consulting, LLC, offered several tips for non-profit leaders who are seeking to build and maintain an effective cybersecurity program to protect sensitive information. You can read Kadien's article here.[2]

The National Council of Non-Profits has also weighed in, offering additional resources built specifically for non-profit leaders. We encourage you to learn from their expertise here.[3]

Put simply: protecting your organization today requires attention not only to financial stewardship but also to digital stewardship.

As fiduciaries with access to sensitive financial information, you have an obligation to both grow and protect the assets of your organization as well as to protect donors, employees and other stakeholders.

Whether you are on staff for a large national non-profit or a volunteer in a leadership capacity at a local church, the conversation about cybersecurity can start with:

ACKNOWLEDGE that you are a potential target of cybercriminals, and that your individual actions contribute to the overall security of the organization's assets.

EDUCATE yourself and those around you with resources and tools to protect your organization and the mission and ministry you value.

IMPLEMENT actions, procedures and best practices to limit the amount of risk to your cybersecurity infrastructure.

EVALUATE your methods and strategies to seek continual improvement in the changing landscape of cybercrime.

UPDATE your software, hardware, login information, certificates and other online tools you regularly use to access sensitive information.

The team at United Church Funds, our custodial partner, BNY, and our vendors take our cybersecurity seriously.

UCF regularly works to follow these and other steps to shield your assets from those seeking to harm your mission and ministry.

We are grateful for the opportunity to be of service to your organization and will continue to be vigilant in response to cyber threats.

Matt Wagner
Vice President, Institutional Relationships

1 Jepma, W. (30 October 2025). Cybersecurity Awareness Month Quotes and Commentary from industry Experts in 2025. SolutionsReview.com https://solutionsreview.com/cybersecurity-awareness-month-quotes-and-commentary-from-industry-experts-in-2025/

2 Douglas, K. (undated) A Best Practice Guide to Cybersecurity for Non-Profits. Non-Profit Leadership Center https://nlctb.org/featured/best-practice-guide-to-cybersecurity-for-nonprofits/

3 (Uncredited) (Undated) Cybersecurity for Non-Profits. National Council of Non-Profits.https://www.councilofnonprofits.org/running-nonprofit/administration-and-financial-management/cybersecurity-nonprofits