United Church Funds®
Investing Together for a Sustainable World

FIDUCIARY FOCUS, JULY 2026

CYBERSECURITY AS MODERN STEWARDSHIP

By Matt Wagner, Vice President, Institutional Relationships

In today's rapidly accelerating tech environment, cybercrime has become a complex, thriving and lucrative ecosystem. For individuals, businesses and nonprofit organizations alike, cybersecurity is no longer simply an issue of changing and protecting passwords; it requires constant and active vigilance to protect yourselves and your organization.

Customer and employee personal identification information, financial and banking data and confidential trade secrets are just some of the areas that professional hackers and cybercriminals around the globe are targeting by exploiting cracks in cybersecurity armor. Raymond Daoud, Senior Vice President and Chief Security Officer at CGI, a leading business information technology consulting firm, noted that "With every new wave of technology, innovation tends to move faster than security."[1]

As fiduciaries, dealing with the risks posed by a fast-moving technological world have become core to your duties to protect your assets — as well as the missions and ministries those assets support.

Churches and nonprofit organizations, as well as the staff and volunteers who lead them, have become increasingly vulnerable to phishing attacks, data breaches, ransomware and other threats.

In a recent Nonprofit Leadership Center article, author Kadien Douglas, Managing Partner at Douglas CPA & Consulting LLC, **offered several tips** for nonprofit leaders who are seeking to build and maintain an effective cybersecurity program to protect sensitive information.[2] The National Council of Nonprofits has also weighed in, **offering additional resources** built specifically for nonprofit leaders.[3] Lastly, we encourage you to review **educational resources** provided by the Insurance Board, a UCC-affiliated insurance provider, to protect against cybercrime.

Put simply, protecting your organization from bad actors online requires regular attention and discipline, core tenets of traditional fiduciary duty.

As new technologies like artificial intelligence are leveraged to commit cybercrime, fiduciaries must remain vigilant against new types of cyberattacks designed to steal your personal identification data, impersonate you in conversations with other parties and breach your login credentials to banking and other sensitive Internet sites.

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

Whether you are on staff for a large national nonprofit or a volunteer in a leadership capacity at a local church, cybersecurity starts with:

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

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

IMPLEMENTING actions, procedures and best practices to limit the risks to your cybersecurity infrastructure.

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

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

PROTECTING your institution by working with your insurance provider to mitigate cybercrime risk. (If you are not insured through the Insurance Board, learn how to protect your organization at www.insuranceboard.org.)

At UCF, we take cybersecurity very seriously. UCF is audited annually by an independent CPA firm on our financial reporting and procedures, as well as on our internal controls, information security and client data protection processes (System and Operations Control Report, or SOC1) to document effective layers of protection for our clients' accounts.

UCF also works with our custodial bank, BNY , and all of our investment managers, vendors and consultants on ensuring that their systems and processes have strong cybersecurity in place.

However, all these safeguards are only as effective as the precautions that our churches and clients also put in place. With cybercrime here to stay and only getting worse, it will take action from all of us to protect our assets from cybercriminals.

As always, our team at UCF is grateful for the opportunity to be of service to your organization.

In service,

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 Nonprofits. Nonprofit Leadership Center https://nlctb.org/featured/best-practice-guide-to-cybersecurity-for-nonprofits/

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