FIDELITY Charitable℠
Make more of a difference

Four Things You Can Do To Protect Against Cyber Threats

Technology allows our organizations to advance our missions while working from home due to COVID-19. However, this doesn't come without risk. Here are some cybersecurity tips for you and your team to help protect your organization, your donors and those you serve.

01 Monitor All Money Movement—Even More Than Usual

- **Seek additional security on money matters.** Ask your financial institutions and any digital fundraising tools about multi-factor authentication or donor validation for all money movement.
- **Sign up for digital statements and monitor your accounts.** Many financial institutions offer proactive notifications so you can monitor account activity in real time and identify any suspicious activity.
- **Opt for digital-only donations.** Receive funds as quickly as possible—and eliminate checks being sent to an office where employees are not regularly checking mail.

More information on signing up for Electronic Funds Transfer from Fidelity Charitable®: fidelitycharitable.org/nonprofits.html

02 Protect Your Devices

- **Install antivirus software on every device.** Choose one that scans your PC on a regular basis to catch and remove potential threats.
- **Stay current with digital updates**, like operating system patches, software updates and major software releases. Vulnerabilities in popular applications—for example, most web browsers—can be targeted by hackers.
- **Avoid public WiFi, and protect your device and accounts** with strong, unique passwords, including multi-factor authentication. Change your passwords regularly. You can also contact your internet provider about stronger encryption.

Learn more: chrtbl.org/NCSApasswords

03 Ensure Digital Tools Are Secure—And Limit High Risk Information

- **Review security protections for all digital tools.** You can find these in the contract or terms of use, or by contacting your vendor.
- **Evaluate where you store high-risk information**, like personally identifying information. Ask yourself: is it necessary to store it in each location? What would happen if it became public?

04 Look Out for Suspicious Emails

- **Be vigilant when opening all email from outside sources**, especially those from an unknown source asking for urgent action. Even legitimate-looking emails can contain fake web links, phone numbers and attachments from cyber criminals.

Learn to recognize cues and clues in this video from McAfee©: youtube.com/embed/Jkt0zFbin90

Remember: Regardless of role, every member of your team can contribute to keeping your organization safe.