PKF O'CONNOR DAVIES
ACCOUNTANTS AND ADVISORS

June 2020

Private Foundations Bulletin

Protecting Your Foundation Against Cyber Threats in the Age of Working Remotely

The COVID-19 pandemic caused private foundations to relocate physical offices to a “virtual office” without much preparation. This hasty change forced a rapid deployment of new technology to allow employees to work from home in order to carry on operations. This change has caused private foundations to be exposed to an increased risk of cyber threats as cybercriminals seek to take advantage of the vulnerable virtual workforce.

As private foundations continue to operate in this virtual world, necessary steps must be taken to evaluate and mitigate the risks associated with this new environment.

Cybercriminal Tactics during the Pandemic

The pandemic has granted cybercriminals an increased opportunity to compromise private foundations’ and their employees’ networks. We are seeing a large increase in the number of cybercrime reports as more individuals work remotely each day. The FBI has reported approximately 3,000-4,000 cybercrimes per day since the start of the pandemic. Prior to the pandemic, the FBI reported an average of 1,000 cybercrimes each day.

Cybercriminals have become more sophisticated over the years as they attempt to gain access to networks through malicious websites. According to SophosLabs, from February 8, 2020 to March 24, 2020, there were 42,578 newly-registered domain names using the words “covid” or “corona.” Cybercriminals are taking advantage of the pandemic because targets are likely to click on these domain names.

In addition to malicious websites, there has been an increase in the amount of malicious emails that have been sent by cybercriminals. In the month of March, there was a 667% increase in the number of malicious emails that were sent according to Barracuda Networks. Private foundations must remain attentive when reviewing any emails that are received to ensure no malicious content is attached. Gaining an understanding of the various tactics used by cybercriminals will help mitigate the risk.

Considerations for Private Foundations

Private foundations should consider the following to ensure virtual offices are secure:

- **Clear Communication and Awareness Training** – What can’t be controlled by technical mechanisms needs to be controlled by clear communication of expectations and awareness:

    - Revisit your remote access policy
    - Authorized applications – prevent shadow IT
    - Authorized storage locations
    - Authorized communication channels

- **Embrace Stronger Password Requirements and Multi-factor Authentication –** Weak passwords are one of the most common ways that systems are compromised by cybercriminals. Private foundations should require employees to have strong passwords and should implement multi-factor authentication to prevent cybercriminals from accessing information if passwords become compromised.

- **Data Control and Loss Prevention –** Define and enhance existing controls around the movement and potential loss of data:
  - Encryption
  - Restricting data storage locations
  - Security of printed documents

- **Endpoint Visibility –** Ensure devices you control are protected. For the devices you don’t control, communication of expectations is key.

- **Remote Conferencing**
  - Password protect the sessions
  - Zoom has come out with many best practice considerations and updates

- **Employee Verification –** Help Desk verification of employees and vice versa

- **EFT (Electronic Funds Transfer) Transactions** – Implement verification procedures on banking information and changes to:
  - Vendors
  - Employees

- **Continuously Evaluate IT Environment –** Although now is a great time for private foundations to evaluate their IT environment, this should not be a one-time occurrence. Private foundations should regularly evaluate their environment to help mitigate any risks imposed by cybercriminals, as the threat is continuously evolving.

Considerations for Employees

Employees should consider the following to ensure virtual offices are secure:

- **Bandwidth –** Employees should ensure their virtual office has sufficient bandwidth to continue with operations.

- **Secure Home Network** – Employees should ensure their network is secure. Steps that can be taken to help secure home network include:
  - Establish a strong Pre-Shared Key for Wi-Fi
  - Create separate Wi-Fi segments for personal use and for foundation use
  - Update router with the most current firmware
  - Ensure vendor default passwords are changed

- **Paper Protections –** Procure a shredder

- **Cyber Hygiene –** If employees are using their own personal devices, employees should ensure these devices remain patched with vendor security fixes and that these devices have the latest anti-virus installed and active.

During these challenging times, it is imperative that we remain vigilant on the links we click, the attachments we open, and the information we disclose.

Contact Us

We welcome the opportunity to answer any questions you may have related to this topic or any other accounting, audit, tax or advisory matters relative to private foundations. Please call 212.286.2600 or email any of the Private Foundation Services team members below:

Thomas Blaney, CPA, CFE
Partner, Co-Director of Foundation Services
tblaney@pkfod.com

Joseph Ali, CPA
Partner
jali@pkfod.com

Raymond Jones, Sr., CPA
Partner
rjones@pkfod.com

Anan Samara, EA
Principal
asamara@pkfod.com

Christopher Petermann, CPA
Partner, Co-Director of Foundation Services
cpetermann@pkfod.com

Scott Brown, CPA
Partner
sbrown@pkfod.com

Barbara Van Bergen, CPA
Partner
bvanbergen@pkfod.com

www.pkfod.com

About PKF O'Connor Davies

PKF O'Connor Davies, LLP is a full-service certified public accounting and advisory firm with a long history of serving clients both domestically and internationally. With roots tracing to 1891, twelve offices in New York, New Jersey, Connecticut, Maryland and Rhode Island, and more than 800 professionals, the Firm provides a complete range of accounting, auditing, tax and management advisory services. PKF O'Connor Davies is ranked 27th on *Accounting Today*'s 2020 "Top 100 Firms" list and is recognized as one of the "Top 10 Fastest-Growing Firms." PKF O'Connor Davies is also recognized as a "Leader in Audit and Accounting" and is ranked among the "Top Firms in the Mid-Atlantic," by *Accounting Today*. In 2021, PKF O'Connor Davies was named one of the 50 best accounting employers to work for in North America, by *Vault*.

PKF O'Connor Davies provides specialized services to not-for-profit organizations. Our dedicated industry practice serves over 3,000 not-for-profit organizations, including 375 private foundations (i.e., family, corporate, community and independent foundations) as well as grant making organizations. We are committed to the not-for-profit industry and continue to invest in our professionals by providing training, state-of-the-art technology and audit and tax guidance to meet the evolving needs of the not-for-profit community.

PKF O'Connor Davies is the lead North American representative in PKF International, a global network of legally independent accounting and advisory firms located in over 400 locations, in 150 countries around the world.

Our Firm provides the information in this e-newsletter for general guidance only, and it does not constitute the provision of legal advice, tax advice, accounting services, or professional consulting of any kind.