Common Tax Scams Every Business Should Know About

Criminals use tax scams to obtain employee and business information for financial gain. While the peak time for these scams is tax season, scammers can strike at any time. This article discusses common tax scams businesses face and how to avoid them.

Common Types of Business Tax Scams

As businesses become increasingly vulnerable to cybercrime and scammers become more sophisticated, it can be difficult for businesses to keep up with the evolving threat landscape. The following are some of the most common business tax scams business owners currently face:

- **W-2 scams**—In a W-2 scam, a scammer contacts a company's HR, payroll or accounting department, posing as an employee or contractor in order to obtain a W-2 form. They can then use the form to file a false tax return to claim a refund.
- **Phishing scams**—Phishing scams involve scammers sending emails or text messages designed to trick taxpayers into thinking they are communicating with officials from the IRS or others in the tax industry. Once the scammer obtains personal or financial information, they can commit identity theft or fraud.
- **Telephone tax scams**—Scammers may call business owners claiming to be an IRS employee and request payment via wire transfer, gift card or another unusual method. While on the phone, scammers may threaten business owners with arrest or suspension of their business license if the payment is not completed.
- **Charity fraud**—This type of scam entails a fraudster setting up a fake charity whose name or website URL is similar to that of a legitimate charitable organization. Businesses may make what they think are tax-deductible donations only to realize that the charity does not exist.
- **Fraudulent tax preparers**—Criminals may masquerade as tax preparers to obtain a business's information to commit fraud.

How to Avoid Business Tax Scams

In order to mitigate the risk of falling victim to tax scammers, business owners should take the following precautions:

- **File early.** When scammers target a business, they may file a fraudulent tax return early in the hopes of obtaining a refund before the legitimate taxpayer files their returns. Since the IRS doesn't necessarily alert taxpayers when a return has been filed, business owners may not realize fraud has been committed for weeks or months. The longer business owners wait to file, the broader the window is for scammers to carry out this fraud.
- **Be selective with whom company information is shared.** Anyone involved in business deals, opportunities or transactions should be vetted before receiving information related to the company.
- **Verify information requests.** Any request for company information should be treated with suspicion until credentials are verified.
- **Dispose of sensitive information properly.** While the disposal of sensitive documents—such as financial statements, legal reports or tax information—may be time-consuming, tedious and expensive, it's imperative to destroy this information properly. Otherwise, business owners may find themselves in jeopardy.
- **Establish policies to keep information safe.** Businesses should implement and develop companywide policies to make protecting company information a priority. This can benefit not only employees and customers but also the long-term health of a business.

Conclusion

Tax scammers may use a variety of tactics to deceive and steal from businesses. By being cautious and having effective policies in place, businesses can minimize the risk of becoming a victim of a tax scam. For more risk management guidance, contact us today.