Huntington Welcome.®

Help prepare your business against fraud this tax season.

Tax season is an ideal time for your business data or employee information to be stolen. Stolen business EINs have long been used to perpetrate tax fraud by creating false W-2 or 1099 documents or to fraudulently claim certain benefits, such as fuel tax credits. However, in the past couple of years there has been an upswing in the filing of fraudulent Forms 1120 and 1120S[1].

Safeguarding your EIN number and filing your business taxes early are your best defenses against tax fraud and identity theft.

☐ W-2 Phishing Scams

- Fraudsters send an email pretending to be from a high-level corporate employee requesting information about employees' Form W-2. The emails typically ask for Form W-2 information and an earnings summary of all W-2 employees. They might also ask for an updated list of employees with their personal details including social security number, home address and salary.

☐ Other Phishing Scams

- Email phishing scams are designed to trick taxpayers into thinking these are official communications from the IRS or others in the tax industry, including tax software companies.
- Be alert to emails from the Taxpayer Advocacy Panel (TAP), which is a volunteer board that advises the IRS on systemic issues affecting taxpayers. TAP never requests, and does not have access to, any taxpayer's personal and financial information.
- Phone calls and text messages purporting to be from the IRS. The IRS does not initiate contact with taxpayers by email, text messages or social media; it sends letters by U.S. mail. Officials say there are very few circumstances when the IRS will come to a business, and even then, such a visit would be preceded by several notices via mail.

☐ How to Report Tax Fraud

- To report theft of W-2 information and/or social security number, visit https://www.irs.gov/individuals/form-w2-ssn-data-theft-information-for-businesses-and-payroll-service-providers.
- Forward any suspicious tax-related email to phishing@irs.gov with "W2 Scam" in the subject line.
- File a complaint with the Federal Trade Commission at identitytheft.gov.
- Contact your financial institutions and close any financial or credit account that might have been opened without your permission or compromised by thieves.

Over 200

employers were victims of the W-2 phishing scam in 2017.[2]

$46 million

dollars in fraudulent refunds caught by the IRS as of February 24, 2018.[3]

23%

of reported identity theft complaints in 2017 were employment and tax–related.[4]

[1] Source: Internal Revenue Service, *Identity Theft Guide for Business, Partnerships and Estates and Trusts*

[2] Source: Forbes *Tax Time Is W-2 Scam Time*

[3] Source: *Treasury Inspector General for Tax Administration, Interim Results of the 2018 Filing Season*

[4] *Federal Trade Commission, Consumer Sentinel Network Data book 2017. Last Modified March 2018. https://www.ftc.gov/system/files/documents/reports/consumer-sentinel-network-data-book-2017/consumer_sentinel_data_book_2017.pdf*

Turn over for additional tips.

☐ How to Help Avoid Tax Scams

- File your business taxes as early as possible during tax season. Fraudsters using stolen identities tend to file false returns early hoping to obtain refunds before the legitimate taxpayer files their return.
- Only give out company information when absolutely necessary —especially on websites and social media sites—and keep track of who you give it to. This could be helpful in determining the source of a breach of personally identifiable information if you become a victim.
- Before giving out information, verify email or other requests that appear to come from your tax professional and payroll/ human resource personnel.
- Properly dispose of any documents that contain sensitive business and customer information.
- Secure your networks and protect company computers and devices with firewalls and the latest anti-virus software.
- Establish and enforce security policies to protect company and employee information.

Contact Huntington

If you think you may be a victim of fraud related to your Huntington credit or debit card, or your card has been lost or stolen, please let us know right away at **(800) 480-2265.**

If you receive a suspicious email claiming to be from Huntington, please let us know at **ReportFraud@huntington.com.**

Visit **huntington.com/Security** for more tips on protecting yourself and to learn more about how we help protect your privacy and keep your information secure.

How the IRS Contacts Taxpayers and Businesses.

- **The IRS will not initially contact you by phone call, text message, social media or e-mail** to ask for personal or business financial information or to obtain payment for a tax bill. The government loves a paper trail. The IRS will write to you first, possibly multiple times. If you are unsure about a tax bill, call the IRS at (800) 829-1040.
- **The IRS will not give you an ultimatum** to pay up immediately or demand that you wire money.
- **The IRS will not demand** that a business pay taxes without the opportunity to question or appeal.
- **The IRS will not threaten** to send police or other law enforcement to your place of business.
- **The IRS will not ask you** to pay your debt using iTunes gift cards or any other type of gift or debit cards. They also will not ask you to pay with alternative currency, such as bitcoin.
- **In the case of a personal visit from someone claiming to be from the IRS or other government entity,** check for official credentials in the form of a pocket commission and HSPD-12 card. No one making a personal visit will demand immediate payment, especially to a source other than the U.S. Treasury.

For more information, go to **huntington.com/Privacy-Security.**