Drake Software®

PHISHING GUIDANCE FOR TAXPAYERS

Phishing Guidance for Taxpayers

As a taxpayer, it is crucial to be vigilant about protecting your personal and financial information. Cybercriminals often use phishing emails to steal sensitive data, especially during tax season. This guide will help you recognize phishing attempts and provide steps to protect yourself and your information.

What is Phishing?

Phishing is an email scam where cybercriminals pose as legitimate organizations to trick you into revealing personal information, such as Social Security numbers, bank account details, or login credentials.

Common Signs of Phishing Emails

Scammers may impersonate your tax return preparer by sending emails that appear to be from them, asking for additional information or prompting you to click on a link. If you are not expecting an email from your tax preparer, verify the sender by contacting your preparer directly using a known phone number or email address. Never use contact information provided in a suspicious email. Common signs of phishing emails include:

- **Urgency or Threats** – Many phishing emails claim that your account will be closed or you will face legal action if you do not respond immediately.
- **Unusual Email Addresses** – Look closely at the sender's email address. Phishing emails often come from addresses that are similar to—but not exactly—the official address of an organization like the IRS (Internal Revenue Service) or your tax return preparer. These differences can be as minute as spaces or hyphens.
- **Generic Greetings** – Legitimate communications usually address you by name. Phishing emails often use generic terms like "Dear Customer."
- **Spelling and Grammar Mistakes** – Professional organizations like the IRS do not send emails with spelling errors or poor grammar.
- **Suspicious Links or Attachments** – Be wary of links or attachments that ask you to provide personal information.

IMPORTANT The IRS will *never* initiate contact with taxpayers by email, text message, or social media to request personal or financial information. Phishing emails may claim to be from the IRS and ask you to update your account, check the

status of your refund, or verify your identity. Always go directly to the official IRS website by typing `www.irs.gov` into your browser rather than clicking on any links in an email.

Steps to Avoid Phishing Scams

- **Do Not Click on Links or Open Attachments** – If you receive an unsolicited email requesting personal information, delete it immediately from both your inbox and trash. Do not click on any links or open any attachments.
- **Verify the Source** – If you are unsure about the legitimacy of an email, contact the organization directly using contact information from their official website.
- **Use Strong Passwords and Multi-Factor Authentication (MFA)** – Protect your online accounts with strong, unique passwords, and enable MFA when possible.
- **Keep Your Software up to Date** – Ensure your computer and mobile devices are using the latest software and antivirus versions.
- **Educate Yourself and Others** – Stay informed about the latest phishing tactics and educate family members or colleagues to do the same.

What to do if You Receive or Fall Victim to a Phish

Phishing scams are a real threat, especially during tax season. By staying informed and cautious, you can protect yourself from becoming a victim. If you suspect a phishing attempt, or have fallen victim to a scam, act quickly and report it to the appropriate authorities.

- **Report to the IRS** – Forward IRS-related phishing emails to Phishing@IRS.gov. Do not open any attachments or click on any links. For more information, visit https://www.irs.gov/privacy-disclosure/report-phishing.
- **Report to Your Tax Return Preparer** – If you receive a suspicious email claiming to be from your tax preparer, contact them directly to report the issue.
- **Monitor Your Accounts** – Check your bank accounts and credit reports regularly for unauthorized activity.
- **File a Report** – If you believe you've provided sensitive information to a fraudulent source, report it to the Federal Trade Commission (FTC) at IdentityTheft.gov, and consider placing a fraud alert on your credit reports.
- **Change Your Passwords** – Immediately change any passwords that may have been compromised, especially for your financial accounts.