Drake Software

INTERNAL OPERATIONS

EDUCATION | COMPLIANCE | PREVENTION | DETECTION

Be Vigilant When Using Email

- Use separate personal and business emails.
- Be cautious of scams and emails from people you do not know
    - Verify the sender's display name is consistent with the email address
- Never click on links in messages from unknown or suspicious senders. To visit the link, type the link or address into your browser's address bar.
- Never open or download attachments from unknown senders.
- Do not send personal information in an email.
- Do not send taxpayer data in emails. If you must, put this information in a document file (such as a PDF) and password protect it.
    - Use a secure document exchange system, such as Drake Software's SecureFilePro

Create and Maintain Strong Passwords

- Use strong, unique passwords of 8 or more mixed characters.
- Password protect all wireless devices.
- Use a phrase or words that are easily remembered and change passwords periodically. The longer your password is, the more secure it is.
- Change default/temporary passwords that come with an account or device.
- Do not reuse passwords – each account, device, and website should have a unique password.
- Keep passwords secure
    - Use a password manager
    - Never share your passwords with anyone
    - Use an on-screen keyboard to type passwords in
    - Never write down passwords
- Use Multi-Factor Authentication when possible.

Watch for Signs of Data Theft

- Your clients e-filed returns begin to reject because returns with their Social Security numbers were already filed.
- Your clients who haven't filed tax returns begin to receive authentication letters (5071C, 4883C, 5747C) from the IRS.
- Your clients who haven't filed tax returns receive refunds.
- Your clients receive tax transcripts that they did not request.

- Your clients who created an IRS online services.gov account receive an IRS notice that their account was accessed (and they did not), or the IRS emails them stating their account has been disabled; or, the taxpayer receives an IRS notice that an IRS online account was created in their name (they did not create the account.).
- The number of returns filed using your Electronic Filing Identification Number (EFIN) exceeds the number of clients in your practice.
- Tax professionals or clients are responding to emails that you did not send.
- Network computers are running slower than normal.
- Computer cursors moving or changing numbers without touching the keyboard.

Implement Internal Controls

- Install security software on all devices (laptops, desktops, routers, printers, tablets, and phones) and keep software set to automatically update.
    - Antivirus – prevents viruses from infiltrating your systems
    - Antispyware – prevents unauthorized software from stealing information that is on your system
    - Firewall – blocks unwanted and unauthorized connections to your system
    - Drive Encryption – protects information from being read on your systems if they are lost, stolen, or improperly destroyed after their useful life has expired
- Encrypt all sensitive files/emails and use strong password protections.
    - To encrypt a Drake Tax data file, under the **Tools** menu, select **File Maintenance > Password Protect Files**
    - To encrypt a tax return printed to PDF in Drake Tax, set the password in the lower left corner of the printer dialogue
- Back up sensitive data to a safe and secure external source not connected full-time to a network.
- Wipe clean or destroy old computer hard drives and printers that contain sensitive data.
- Limit access to taxpayer data to individuals who need to know.

Create a Data Security and Response Plan

- Become familiar with IRS Publication 4557 - Safeguarding Taxpayer Data
- Report any data theft or loss to your IRS Stakeholder Liaison, FBI, and local police

Properly Dispose of Old Devices and Information

- Delete all information from devices, hard drives, tapes, USB, tablets, or phones.
- Once data is deleted, ***physically*** destroy devices, hard drives, tapes, USBs, CDs, tablets, or phones.