Protecting What You Have

Record Retention - What do I Need to Keep And For How Long?

KEEP RECORDS AS LONG AS APPROPRIATE

Different records need to be saved for different periods of time. Divide your records into categories, such as short- term, medium-term, and long-term. There are no concrete rules about how long records must be saved, so you will often have to use your own judgment.

The following guidelines may help:

SHORT-TERM (1-3 YEARS)

- Household bills, except those that support tax deductions (items such as heat, water, and electricity are generally short-term unless you deduct them for home office use or a rental)
- Paycheck stubs
- Bank records - Go through your checks each year and keep those related to your taxes, business expenses, home improvements and mortgage payments.
- Expired insurance policies

MEDIUM-TERM (6-7 YEARS)

- Tax returns and supporting information
- Income and expense records (including lottery tickets and winnings)
- Bank and credit union statements
- Brokerage house statements
- Canceled checks and check registers (checks for major purchases may be kept longer)
- Paid-off loan documents
- Personal property sales receipts

LONG-TERM (INDEFINITELY)

- Tax dispute records
- Evidence of retirement plan contributions
- Investment records
- Medical history information
- Pension/retirement plan documents
- Social Security information

The IRS typically has three years after a return is led to audit a return, or two years after you've paid the tax, whichever is later. However, if income was underreported by at least 25 percent, the IRS can look back six years after the return is led, and there is no time limit for fraudulent tax returns. An audit requires that you provide documentation to substantiate the return being audited.

CYBER PROTECTION CHECKLIST

MANAGING PERSONAL DEVICES

- Install the most up-to-date antivirus and antispyware programs on all devices (PCs, laptops, tablets, smartphones) and update these software programs as they become available. These programs are most effective when users set them to run regularly rather than just running periodic scans, which may not provide maximum protection to your device.
- Access sensitive data only through a secure location or device; never access confidential personal data via a public computer, such as in a hotel or cybercafé.

PROTECTING PASSWORDS

- Use a personalized custom identifier for financial accounts you access online. Never use your Social Security number in any part of your login activity.
- Regularly reset your passwords, including those for your email accounts. Avoid using common passwords across a range of financial relationships.

SURFING THE WEB SAFELY

Do not connect to the Internet via unsecured or unknown wireless networks, such as those in public locations like hotels or cybercafés. These networks may lack virus protection, are highly susceptible to attacks, and should never be used to access confidential personal data.

PROTECTING SOCIAL NETWORKS

Limit the amount of personal information you post on social networking sites. Never post your Social Security number (even the last four digits). Consider keeping your birthdate, home address, and home phone number confidential. We also discourage clients from posting announcements about births, children's birthdays, or loss of loved ones.

PROTECTING YOUR EMAIL

- Review unsolicited emails carefully. Never click links in unsolicited emails or in pop-up ads, especially those that warn that your computer is infected with a virus and request that you take immediate action.

SAFEGUARD YOUR FINANCIAL ACCOUNTS

- Review all your credit card and financial statements as soon as they arrive or become available online. If any transaction looks suspicious, immediately contact the financial institution where the account is held.
- Never send account information or personally identifiable information over email, chat, or any other unsecure channel.

IRS-IMPERSONATION TELEPHONE SCAM

An aggressive and sophisticated phone scam targeting taxpayers, including recent immigrants, has been making the rounds throughout the country. Callers claim to be employees of the IRS, but are not. These con artists can sound convincing when they call. They use fake names and bogus IRS identification badge numbers. They may know a lot about their targets, and they usually alter the caller ID to make it look like the IRS is calling.

Note that the IRS will never:

1. Call to demand immediate payment, nor will the agency call about taxes owed without first having mailed you a bill.
2. Demand that you pay taxes without giving you the opportunity to question or appeal the amount they say you owe.
3. Require you to use a specific payment method for your taxes, such as a prepaid debit card;
4. Ask for credit or debit card numbers over the phone.
5. Threaten to bring in local police or other law-enforcement groups to have you arrested for not paying.

Also, don't fall victim to tax scams.

REMEMBER If it sounds too good to be true, *it probably is*.