Data theft safety tips

Steps to take to reduce the risk of having your client data stolen when using remote access software.

1) Use strong passwords. A strong password has a minimum of 12 alpha, numeric and special characters. Remember strong passwords have to be used by everyone who has access to your client data.
2) Use layers of passwords. For example a strong password for your remote access software and a separate strong password for your tax software. In addition you should use strong passwords for other files containing client information stored on your hard drive.
3) Use password lock out software; that is software that temporarily locks access to your computer when a password is repeatedly entered incorrectly.
4) Use geographical IP or internet protocol filtering software to prevent hacking from outside the United States.
5) Limit the number of hours your remote access software is available during the day. For example from 7:00 a.m. to 11:00 p.m.

(As an alternative consider using a VPN or virtual private network instead of remote access software to access your computer from a remote location.)

Steps to take to reduce the risk of losing client data to ransomware.

1) Be extremely careful when clicking on email links, attachments and images. Phishing emails sometimes contain links and attachments that can install malware. Be aware that phishing emails can even come from trusted sources, if the source's computer system has been compromised.
2) Back up your computer system regularly and periodically test your backup system.

NOTE: IRS Publication 4557 "Securing Taxpayer Data" is an excellent reference guide that discusses a wide variety of security issues including facilities, personnel, computer and information systems security. Publication 4557 includes checklists to help identify specific tasks to be completed and to track the progress of completing those tasks.