Security Tips for Tax Professionals

Tax professionals, such as certified public accountants, attorneys, enrolled agents, tax preparers, etc., are a lucrative target for hackers for several reasons:

- Tax professionals work with a large amount of sensitive data.
- The filing of fraudulent tax returns has a very high return on investment.
- Small firms are an even more attractive target as these firms often have small networks with fewer security controls, making it easier to execute an attack.

Small businesses will continue to be targeted. There are measures you can take to mitigate risk of a network breach; and furthermore, you may protect data from theft even if your network has been breached.

If you believe a network breach has occurred, log in from a different network and change your passwords.

More Help

For more information about how to safeguard taxpayer information, go to **irs.gov** and search for **4557** to find IRS Publication 4557, *Safeguarding Taxpayer Data, A Guide for Your Business.* This publication provides a checklist to help safeguard taxpayer information and enhance office security.

To safeguard taxpayer information, you must determine the appropriate security controls for your environment based on the size, complexity, nature, and scope of your business. Security controls are the management, operational, and technical safeguards you may use to protect the confidentiality, integrity, and availability of your clients' information. Examples of security controls:

- Lock office doors to restrict access to paper or electronic files.
- Require passwords to restrict access to computer files.
- Encrypt electronically stored taxpayer information.
- Keep a backup of electronic data for recovery purposes.
- Shred paper containing taxpayer information before disposing of it.
- Use encryption when you send emails with sensitive or personal information.

Useful Online Resources

ftb.ca.gov
irs.gov
consumer.ftc.gov
identitytheft.gov

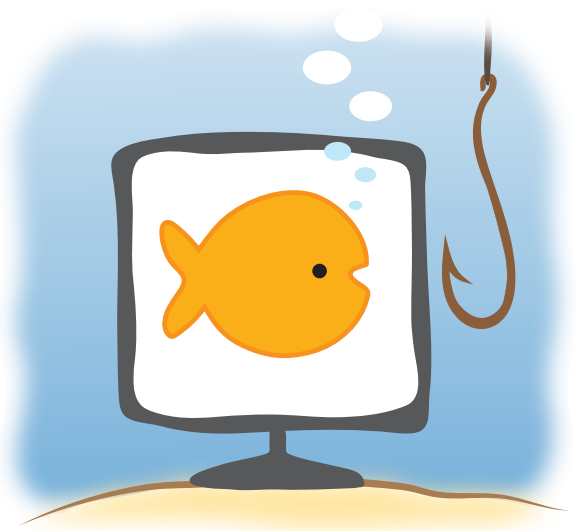
Tax Practitioner Assistance

Phone: 916.845.7057
Fax: 916.845.9300

FTB 5616 (REV 02-2018)

Security Tips for Tax Professionals

STATE OF CALIFORNIA
Franchise Tax Board



The #1 Attack Method is…

Phishing Scams

Enticing users to open an attachment in an email, which contains malicious code, is the most popular way to launch an attack. Be alert for phishing scams: **do not** open links or attachments from unknown senders. These items can be very difficult to recognize if attackers use the "spear phishing" tactic, which specifically targets selected users by sending emails with targeted knowledge.

Tax professionals should educate all staff about the dangers of phishing scams in the form of e-mails, text messages, and phone calls.

Other Ways to Protect your Network and Data

- Ensure that **antivirus** software is installed and configured to automatically scan and update signatures for viruses and malware on all computers on your business network.
- **Strengthen passwords** for both computer access and software access. A strong password has a minimum of eight digits (more is better) with at least one of each of the following: upper and lower case letters, numbers, and special characters.
- **Maintain backups offline.** For example, back up all critical data to an encrypted flash drive or external hard drive and store these drives in a safe. If cloud storage is used, employ a strong and complex password with at least 15 characters.
- Ensure that you **do not** share your MyFTB password with staff.
- Use a **dedicated system** for processing sensitive data. While you might incur some extra expenses such as purchasing dedicated systems for specific business functions, using one or more systems exclusively for online filing services ensures that tax data is not commingled with other information on your network.
- **Power down** your systems when not in use. Hackers love to strike when you are least expecting it, such as after business hours or over the weekend.

Unless properly configured, the typical home or small business network uses equipment that has limited security functionality out of the box. If you do not have the knowledge or resources to manage your own small business network, consider outsourcing to an IT consulting firm or cloud service. These businesses have the benefit of having security as part of the service, and the added value of maintaining a team of professionals on call to manage your network and make sure it's available when you need it.

It is critical that we work in partnership to combat identity theft. Major software providers are required to report data thefts to the IRS. We urge individual tax preparers to notify their local IRS Stakeholder Liaison of any data theft to lessen the impact on clients and the tax system.