SAMPLE DATA THEFT CHECKLIST

Phishing Attacks

Spear phishing is a type of phishing scam. The objective of a spear phishing email is to pose as a trusted source and “bait” the recipient into opening an embedded link or an attachment. The email may make an urgent plea to the tax pro to update an account immediately. A link may seem to go to another trusted website, but it’s actually a website controlled by the thief.

Key Logging

An attachment may contain malicious software called keylogging. This software secretly infects a computer and provides the thief with the ability to see every keystroke. Thieves can then steal passwords to various accounts.

Client Impersonation

A common spear phishing scam is when the thief poses as a prospective client and sends an unsolicited email to a tax professional. After an exchange of emails, the thief sends a follow-up email with an attachment. The thief claims it contains the tax information needed to prepare a return. Instead, it contains spyware that allows thieves to track each keystroke.

Sending Links

Thieves pose as tax software providers or data storage providers with emails containing links. These links go to web pages that mirror real sites. The thieves’ goal is to trick tax professionals into entering their usernames and passwords into these fake sites, which the crooks then steal.

Ransomware

Another trick used by thieves is ransomware. In this scam, the thief doesn’t steal the data, they encrypt it. Once they encrypt the data, thieves demand a ransom in return for the code to unencrypt the data. The FBI warns users not to pay the ransom because thieves often don’t provide the code.

Steps to Protect Data

Here are some simple steps that tax pros and their employees can take to protect their clients’ data. They should:

- Use separate personal and business email accounts.
- Protect email accounts with strong passwords and two-factor authentication if available.
- Install an anti-phishing tool bar to help identify known phishing sites.
- Use anti-phishing tools that are included in security software products.
- Use security software to help protect systems from malware and scan emails for viruses.
- Never open or download attachments from unknown senders, including potential clients. They should instead make contact first by phone.
- Send only password-protected and encrypted documents when files must be shared with clients over email.
- Not respond to suspicious or unknown emails