Information Security Express Lane – 12 Items or Less

In today's fast-paced world, we want to get things done as quickly and effectively as possible. This tendency often forces us to make difficult choices. For example, to get out of the grocery store quickly, some might put back the 13th item in order to get into the express lane. You leave the store with only those 12 things that you must have to survive.

Here are the 12 information security items that, at a minimum, you need to survive. If you do not have or have not completed one or more of these items, you need to stop by the store and pick up a few things.

1. **Hire an IT Professional.** Having a talented and qualified expert to assist you in assessing and protecting your office and your information is a must. When you have a cyber fraud incident, whether it is a cyber breach, cyber theft, or wire fraud incident, you want to have this professional on speed dial.

2. **Assess the Current State of Your Office and Network.** Work with your IT Professional to take a comprehensive review of yourself, your staff, your office, and your network to assess vulnerabilities and where the most damage can be inflicted. Think in terms of clients' information, critical business information, and surviving a cyber fraud incident. You need to understand where and how this information is stored, how it is protected, and where you are vulnerable.

3. **Change Your Passwords.** If you have not changed ALL of your passwords in the past three months, do so now. Employ a strong password policy, requiring (1) a minimum of 8 characters; (2) an upper case and lower case letter; (3) a number; and (4) a special character. Longer, more complex passwords are even better. Do not use the same passwords for different accounts or systems. Everyone should have their own password – no sharing.

4. **Get Encrypted Email.** Email is like a post card, which can be viewed by anyone in its path. Encryption is like the envelope that ensures a secure delivery of its contents. If you have not secured your communication yet, we offer solutions through selected vendors at *invtitle.com/vip*. It is not as expensive as you may think.

5. **Check Your Back-Up.** You should have a routine back-up plan in place, which should include: (1) back-ups on a routine schedule; (2) confirmation of their completion; and (3) periodic off-site storage. You could also run a digital back-up stored in the cloud, but you must check their security also. This step is essential to your disaster recovery plan.

6. **Check for any Outstanding Updates on Operating Systems, Digital Devices, and Programs.** Nearly all software programs provide periodic updates to address vulnerabilities as they are discovered and exploited. In most cases, you have already paid for these updates. Please take advantage of them. Check every program on every computer to make sure it is running the latest and most secure version.

7. **Check Your Virus Protection, Malware Protection, and Firewall.** Cyber threats are evolving every minute, and your security software must evolve too. Confirm that the programs are routinely running and automatically updating. This maintenance measure is not a one-time thing – it is an everyday thing.

8. **Written Information Security Policies.** Once you assess your systems, information, and environments, decide your best protections and policies. Document them to guide your office and staff in your daily activities. Work with your IT Professional, consider your assessment, review ALTA's Best Practice #3, and consult ***C.Y.B.E.R. – Can You Be Entirely Ready.**** C.Y.B.E.R. includes steps, policies, and procedures to consider in formulating your **Information Security and Trust Account Security Plans**.

9. **Written Wire Fraud Prevention Policies.** Document and train on policies and procedures for wiring funds. Before you send another wire, consult ***W.I.R.E. – What I Require Every time.**** Your policy should include ***(1) proper identification*** of the authorized party; ***(2) verbal confirmation*** of wiring instructions; and ***(3) delivery verification*** of the funds receipt.

10. **Written Cyber Fraud Response Plan.** If you do not have one, consult ***F.A.S.T. – Fast Action Stops Theft;**** which includes steps, policies, and procedures to consider in formulating your **Cyber Fraud Response Team** and your **Cyber Fraud Response Plan**. Have a plan for surviving a cyber fraud incident.

11. **Train Your Staff and Educate Others.** The biggest vulnerability is not the computer or phone, it is the person using those devices. All of the policies in the world will not protect those who do not follow them. You should also share information about information security with your clients. We have prepared materials to assist you with this process. Visit *invtitle.com/fraud*.

12. **Get Cyber Fraud Insurance.** In addition to software and digital data back-ups, you need a financial back-up. You can find this in the form of cyber fraud insurance. There are three types of coverage that you will want to have in place ***(1) Cyber Breach Coverage*** for data breaches; ***(2) Cyber Crime Coverage*** for theft of funds; and ***(3) Social Engineering Coverage*** for being tricked into the loss of funds.

*Visit *invtitle.com/wire*.

If you have already completed some of these items, then congratulations are in order. Your list at the store is a little lighter. If you are missing any of these items, however, you need to go straight to the **information technology express lane** and protect yourself in this fast-changing world of cyber threats.

Investors Title
Investors Title Insurance Company
800.326.4842 | invtitle.com