



1

---

---

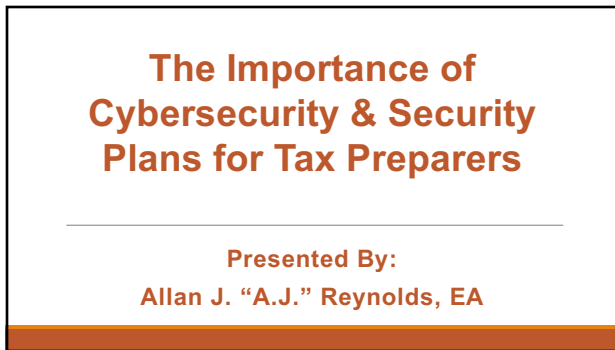
---

---

---

---

---



2

---

---

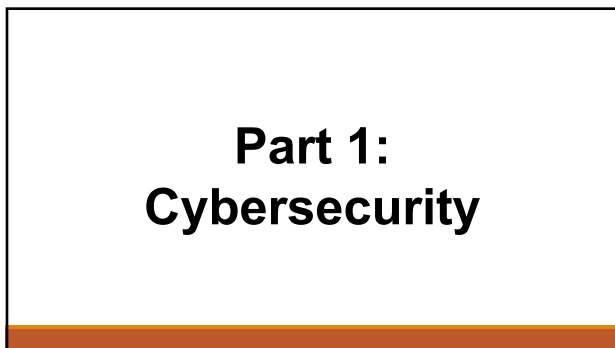
---

---

---

---

---



3

---

---

---

---

---

---

---

## Cybersecurity

**Objectives**

- The question is “not if, but when” you will be targeted. This session addresses scams, threats, prevention, data security requirements, and steps to take in the aftermath of a breach. The smaller your firm is, the more imperative due diligence regarding Cybersecurity is.

4

---

---

---

---

---

---

---

---

## Quote of the Session

*“Values are like fingerprints. Nobody’s are the same, but you leave them all over everything you do.”*

- Elvis Presley

5

---

---

---

---

---

---

---

---

## Cybersecurity

Confidentiality, integrity, and availability are duties of the tax professional community to protect our clients’ information from disclosure to third parties and threat from cyber-attacks.

6

---

---

---

---

---

---

---

---

### Cybersecurity

**Confidentiality**

- Protecting information from unauthorized access and disclosure. For example, what would happen to your company if client information such as client lists, client social security numbers, and other personal information was stolen?

7

---

---

---

---

---

---

---

### Cybersecurity

**Integrity**

- Protecting information from unauthorized use.

**Availability**

- Preventing disruption in how you access information.

8

---

---

---


---

---

---

---

### Cybersecurity



The diagram illustrates the components of Cyber Security. At the top, the words "CYBER SECURITY" are prominently displayed. Below this, a series of icons represent different security domains: Application, Information, Network, Operational, Encryption, Access control, End-user education, and Disaster recovery. Each icon is accompanied by its respective label.

Application Information Network Operational Encryption Access control End-user education Disaster recovery

9

---

---

---

---

---

---

---

### Cybersecurity

“Prevention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communications services, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation.”

10

---

---

---

---

---

---

---

### Cybersecurity

Cybersecurity works in conjunction with a variety of other security measures. As a whole, these information security components provide defense against a wide range of potential threats to your business's information.

11

---

---

---

---

---

---

---

### Cybersecurity

#### Advice From an Expert

- ✓ Separate personal from work.
- ✓ Only open known attachments or links.
- ✓ Slow Down and Validate
- ✓ Situational Awareness

12

---

---

---

---

---

---

---

### Cybersecurity

“Situational awareness is the use of the sensory system to scan the environment with the purpose of identifying threats in the present or projecting those threats into the future.” - Jason Mordecai

13

---

---

---

---

---

---

---

### Cybersecurity

**Federal Trade Commission**

✓ Cybersecurity for Small Business:

- <https://www.ftc.gov/business-guidance/small-businesses/cybersecurity>

14

---

---

---

---

---

---

---

### Cybersecurity

- ☐ Cybersecurity Basics
- ☐ Cyber Insurance
- ☐ Phishing
- ☐ Ransomware
- ☐ Tech Support Scams

15

---

---

---

---

---

---

---

### Cybersecurity

- ☐ Business Email Imposters
- ☐ Email Authentication
- ☐ Physical Security
- ☐ Secure Remote Access
- ☐ Vendor Security

16

---

---

---

---

---

---

---

### Cybersecurity Quiz

1. Which of the following should you do to restrict access to your files and devices?

- A. Update your software once a year.
- B. Share passwords only with colleagues you trust.
- C. Have your staff members access information via an open Wi-Fi network.
- D. Use multi-factor authentication.

17

---

---

---

---

---

---

---

### Cybersecurity Quiz

2. Backing up important files offline, on an external hard drive or in the cloud, will help protect your business in the event of a cyber attack. True or False?

- True
- False

18

---

---

---

---

---

---

---

### Cybersecurity Quiz

3. Which is the best answer for which people in a business should be responsible for cybersecurity?

A. Business owners. They run the business, so they need to know cybersecurity basics and put them in practice to reduce the risk of cyber attacks.

B. IT specialists, because they are in the best position to know about and promote cybersecurity within a business.

C. Managers, because they are responsible for making sure that staff members are following the right practices.

D. All staff members should know some cybersecurity basics to reduce the risk of cyber attacks.

19

---

---

---

---

---

---

---

### Cybersecurity Quiz

4. Cyber criminals only target large companies. True or False?

True

False

20

---

---

---

---

---

---

---

### Cybersecurity Quiz

5. Which of the following is the best answer for how to secure your router?

A. Change the default name and password of the router.

B. Turn off the router's remote management.

C. Log out as the administrator once the router is set up.

D. All of the above.

21

---

---

---

---

---

---

---

Cybersecurity Checklist
<ul style="list-style-type: none"><li>✓ Automatic Screen locks</li><li>✓ Password Manager and Policies</li><li>✓ Ensure computers, software, and operating systems are always up-to-date.</li><li>✓ Document Equipment/Computers of Office</li><li>✓ Physical Security</li><li>✓ Personnel Security</li></ul>

---

---

---

---

---

---

---

22

Cybersecurity Checklist
<ul style="list-style-type: none"><li>✓ Client Policies</li><li>✓ VPNs</li><li>✓ Multi-Factor Authentication</li><li>✓ Organize Access with Personnel</li><li>✓ Security Software Installed on All Computers</li><li>✓ Back-Up Files</li><li>✓ Secure Portals</li></ul>

---

---

---

---

---

---

---

23

Cybersecurity Checklist
<ul style="list-style-type: none"><li>✓ Training of Employees and Yourself</li><li>✓ Scam Awareness with Weekly Meetings</li><li>✓ Retain cybersecurity expert for monthly/quarterly check-up.</li><li>✓ Destroying or Deleting Data</li><li>✓ Remote Access Policy</li></ul>

---

---

---

---

---

---

---

24



Cybersecurity Checklist

- ✓Breach Response Plan
- ✓Review Policies Annually
- ✓CPE on cybersecurity annually for all employees including yourself.
- ✓Evaluate Insurance Coverage

25

---

---

---

---

---

---

---

Information Security for Tax Professionals

Cybersecurity

- Defined on Previous Slide...

Personnel Security

- Ex: Using Background Checks

Operational Security

- Protecting Business Plans and Processes

26

---

---

---

---

---

---

---

Information Security for Tax Professionals

Privacy

- Protecting Personal Information

Physical Security

- Protection of Property

Contingency Planning + Disaster Recovery

- How to resume normal operations after an incident, also known as Business Continuity Planning.

27

---

---

---

---

---

---

---

Physical Security Quiz

1. Promoting physical security includes protecting:

A. Only paper files.

B. Only paper files and any computer on which you store electronic copies of those files.

C. Only paper files, flash drives, and point-of-sale devices.

D. All the above plus any other device with sensitive information on it.

28

---

---

---

---

---

---

---

Physical Security Quiz

2. Paper files that have sensitive information should be disposed of in a locked trash bin. True or False?

True

False

29

---

---

---

---

---

---

---

Physical Security Quiz

3. When you hit the "delete" key, that means a file is automatically removed from your computer. True or False?

True

False

30

---

---

---

---

---

---

---

Physical Security Quiz

4. Which one of these statements is true?

A. It's best to use multi-factor authentication to access areas of the business network with sensitive information.

B. You should use the same password for key business devices to guarantee that high-level employees can access them in an emergency.

C. The best way to protect business data is to make sure no one loses any device.

D. You shouldn't limit login attempts on key business devices, because getting locked out for having too many incorrect attempts would leave you unable to access your accounts.

31

---

---

---

---

---

---

---

---

Physical Security Quiz

5. Only people with access to sensitive data need to be trained on the importance of the physical security of files and equipment. True or False?

True

False

32

---

---

---

---

---

---

---

---

Information Security for Tax Professionals

- Lacking any one of these components diminishes the effectiveness of the others.
- It is not possible for any business to be completely secure.
- Nevertheless, it is possible - and reasonable - to implement a program that balances security with the needs and capabilities of your business.

33

---

---

---

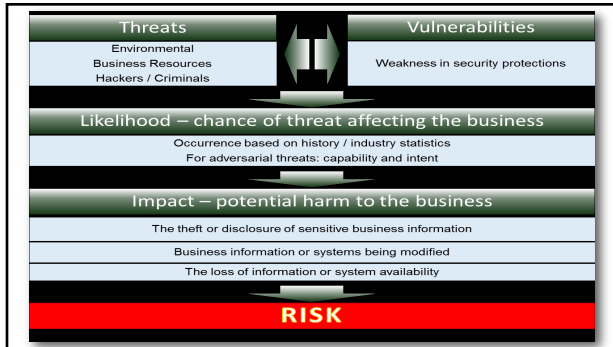
---

---

---

---

---



34

---

---

---

---

---

---

---

---

### Managing Risks

- Identify what information your business stores and uses.
- Determine the value of your information.
- Develop an Inventory
- Understand your threats and vulnerabilities.

35

---

---

---

---

---

---

---

---

### Safeguarding Information

- Identify
- Protect
- Detect
- Respond
- Recover

36

---

---

---

---

---

---

---

---

### Safeguarding Information

- ☐ Security Affects Availability
- ☐ Security = Weakest Link
- ☐ Windows Key + L = Locks Computer

---

---

---

---

---

---

---

37

### Working Safely and Securely

- ✓ Email Attachment and Web Links
- ✓ Use separate personal and business computers, mobile devices, etc.
- ✓ Connecting personal or untrusted storage devices or hardware to your business computer.
- ✓ Downloading Software

---

---

---

---

---

---

---

38

### Working Safely and Securely

- ✓ **Do not share personal or business information!**
- ✓ Harmful Pop-Ups
- ✓ Strong Passwords
- ✓ Use secure browsers when conducting online business.

---

---

---

---

---

---

---

39

## Working Safely and Securely

### Dangers Beyond Email:

- Vishing
- Smishing
- QRishing



40

---

---

---

---

---

---

---

## Working Safely and Securely

### Dangers Beyond Email:

- Vishing  
*Ex: Caller pretending to be from a government office.*

41

---

---

---

---

---

---

---

## Working Safely and Securely

### Dangers Beyond Email:

- Smishing - Malicious Text Messages

42

---

---

---

---

---

---

---

## Working Safely and Securely

### Dangers Beyond Email:

- QRishing - Malicious QR Codes

---

---

---

---

---

---

---

43

## Cybersecurity “So What?”

### Cybersecurity Common Sense

- Being safe online is not so different from being safe in the physical world.
- Keep calm and trust your gut!

### Commonly Used Terms

- Bad Actor
- Hacker
- Cyber Attack



### Antivirus Software is Available for Mobile Devices

- Mobile services are easy and common for hackers to target.

---

---

---

---

---

---

---

44

## Cybersecurity “So What?”

### Do Your Part!

- #BeCyberSmart
- Cybersecurity starts with YOU and is everyone's responsibility.

**Fun Fact:** There are currently an estimated 5.2 billion internet users or 60% of world's population.

---

---

---

---

---

---

---

45

## Malware

Any software intended to...

- Damage
- Disable
- Give someone unauthorized access to your computer or other internet-connected device.

---

---

---

---

---

---

---

46

## Malware



### Examples:

- Ransomware
- Adware
- Botnet
- Rootkits
- Spyware
- Viruses
- Worms

---

---

---

---

---

---

---

47

## Ransomware

Malware designed to make data or hardware inaccessible to the victim until a ransom is paid.

### Why should you care?

- Often downloaded as malicious email links.
- Damage to both financial stability and reputation.
- No guarantee that you will get your data back, even if you pay.
- Often used as a decoy for other malicious activity.

---

---

---

---

---

---

---

48



### Ransomware Quiz

1. What is ransomware?

A. Software that infects computer networks and mobile devices to hold your data hostage until you send the attackers money.

B. Computer equipment that criminals steal from you and won't return until you pay them.

C. Software used to protect your computer or mobile device from harmful viruses.

D. A form of cryptocurrency.

49

---

---

---

---

---

---

---

### Ransomware Quiz

2. Local backup files – saved on your computer – will protect your data from being lost in a ransomware attack. True or False?

True

False

50

---

---

---

---

---

---

---

### Ransomware Quiz

3. Which of these best describes how criminals start ransomware attacks?

A. Sending a scam email with links or attachments that put your data and network at risk.

B. Getting into your server through vulnerabilities and installing malware.

C. Using infected websites that automatically download malicious software to your computer or mobile device.

D. All of the above.

51

---

---

---

---

---

---

---

### Ransomware Quiz

4. If you encounter a ransomware attack, the first thing you should do is pay the ransom. True or False?

True

False

---

---

---

---

---

---

---

52

### Ransomware Quiz

5. Setting your software to auto-update is one way you can help protect your business from ransomware. True or False?

True

False

---

---

---

---

---

---

---

53

### Bots

Bots are a type of program used for automating tasks on the internet.

**Why should you care?**

- Gather Passwords
- Log Keystrokes
- Obtain Financial Information
- Use Email to Send Spam

---

---

---

---

---

---

---

54

## Physical Cyber Attacks

Physical cyber attacks use hardware, external storage devices, or other physical attack vectors to infect, damage, or otherwise compromise digital systems.

### Think...

- USB Storage Devices
- Mainframe
- Network
- Stand-On Alone

---

---

---

---

---

---

---

55

## Physical Cyber Attacks

### Why should you care?

- Easy to Overlook
- Difficult to Identify and Detect
- Extremely Difficult to Remove
- Do anything from installing ransomware, to sending copies of/ or modifying information systems, to dismantling networks.

***Anything connected to internet is potentially vulnerable!***

---

---

---

---

---

---

---

56

## Social Engineering

Cybercriminals can take advantage of you by using information commonly available through...

- Social Media Platforms
- Location Sharing
- In-Person Conversations

---

---

---

---

---

---

---

57

## Social Engineering

### Why should you care?

- Your privacy isn't just a luxury – it's a security measure.
- Attacks can be successful with little to no programming knowledge or ability.
- Technological security measures can only protect you so much – you are your best defense.

58

---

---

---

---

---

---

---

## Social Engineering

### Examples:

- Phishing
- Pretexting
- Baiting
- Quid Pro Quo
- Tailgating
- Inside Job
- Swatting

59

---

---

---

---

---

---

---

## Phishing



60

---

---

---

---

---

---

---

## Phishing

- Phishing can often lead to vulnerabilities that can result in ransomware or other types of malware.
- Importance of being wary of emails, text messages or chat boxes that come from a stranger or someone you were not expecting.
- Think before you click on any suspicious emails, links, or attachments.

---

---

---

---

---

---

---

61

## Phishing

- Phishing has become more prevalent with sophisticated attempts such as connecting your Social Media presence with known associates to gather information about you. Information gathered is then used to trick you into sending money or buying gift cards.
- Protect your privacy online and **Fight the Phish!**



---

---

---

---

---

---

---

62

## Phishing

*Protect your privacy online and **Fight the Phish!***



---

---

---

---

---

---

---

63

## Phishing

- Know the Red Flags
- Verify the Source
- Be Aware!



64

---

---

---

---

---

---

---

## Phishing

Fake messages from a seemingly trusted or reputable source designed to convince you to...

- Reveal Information
- Give Unauthorized Access to a System
- Click On a Link
- Commit to a Financial Transaction

65

---

---

---

---

---

---

---

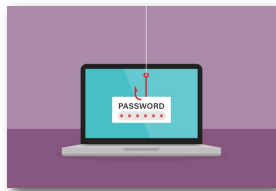
## Phishing

### Why should you care?

- Extremely Common
- Can have severe consequences.

### Examples:

- Emails
- Text Messages
- Phone Calls
- Suspicious Hyperlinks



66

---

---

---

---

---

---

---

### Phishing Email

**From:** Legitimate-Looking-Source@notquiteyourworkemail.com  
**Subject:** Urgent IT Update: Software Vulnerability

Software Update

Good afternoon Tom:

A vulnerability has been identified in "Big Name Software" that allows an attacker to record calls and videos from your computer without your knowledge. Please install the attached update by the end of the day or your workstation will be locked.

We have also created app for all employees to determine if they been affected by this vulnerability. Click hereto run the app.

Sincerely,  
Skippy  
Your Company IT Department

[www.fakewebsite.com/gotcha.exe](http://www.fakewebsite.com/gotcha.exe)  
Click or tap to follow link

67

---

---

---

---

---

---

---

### Phishing Quiz

1. Which one of these statements is correct?

A. If you get an email that looks like it's from someone you know, you can click on any links as long as you have a spam blocker and anti-virus protection.

B. You can trust an email really comes from a client if it uses the client's logo and contains at least one fact about the client that you know to be true.

C. If you get a message from a colleague who needs your network password, you should never give it out unless the colleague says it's an emergency.

D. If you get an email from Human Resources asking you to provide personal information right away, you should check it out first to make sure they are who they say are.

68

---

---

---

---

---

---

---

### Phishing Quiz

2. An email from your boss asks for the name, addresses, and credit card information of the company's top clients. The email says it's urgent and to please reply right away. You should reply right away. True or False?

True

False

69

---

---

---

---

---

---

---

### Phishing Quiz

3. You get a text message from a vendor who asks you to click on a link to renew your password so that you can log in to its website. You should:

A. Reply to the text to confirm that you really need to renew your password.

B. Pick up the phone and call the vendor, using a phone number you know to be correct, to confirm that the request is real.

C. Click on the link. If it takes you to the vendor's website, then you'll know it's not a scam.

70

---

---

---

---

---

---

---

### Phishing Quiz

4. Email authentication can help protect against phishing attacks. True or False?

True

False

71

---

---

---

---

---

---

---

### Phishing Quiz

5. If you fall for a phishing scam, what should you do to limit the damage?

A. Delete the phishing email.

B. Unplug the computer. This will get rid of any malware.

C. Change any compromised passwords.

72

---

---

---

---

---

---

---



### How Can You Better Protect Yourself Online?

#### Secure Your Networks

- Wireless routers are a way for cybercriminals to access online devices.

#### If You Connect It, Protect It

- One proven defense against intrusion is updating to the latest virus protection software.

73

---

---

---

---

---

---

---

### How Can You Better Protect Yourself Online?

#### Stay Up to Date

- Keep software updated to the latest versions and set security software to run regular scans.

#### Double Your Login Protection

- Enable multi-factor authentication (MFA) to ensure that the only person who has access to your account is you.

74

---

---

---

---

---

---

---

### Password Tips

- Use different passwords on different systems and accounts.
- Use the longest password allowed.
- Use a mix of uppercase and lowercase letter, numbers, and symbols.
- Reset your password every few months.
- Use a password manager.

75

---

---

---

---

---

---

---

## Password Tips

### Did You Know?

Password or credential stuffing is a cyber-attack that tries “stuffing” already comprised username and passwords from one site into another site in hopes that the user uses the same login information across platforms.

76

---

---

---

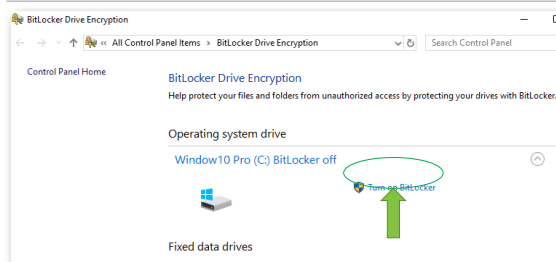
---

---

---

---

## Drive Encryption



77

---

---

---

---

---

---

---

## Office Practices and Security

Monitor your EFIN for suspicious activity:

<https://www.irs.gov/tax-professionals/how-to-maintain-monitor-and-protect-your-efin>

78

---

---

---

---


---

---

---

### Data Breach

Data thieves are attempting to compromise our systems and steal our client data year-round. Unfortunately, the best laid plans sometimes can't prevent a data breach. Cybercriminals use sophisticated and ever-evolving techniques to gain access to our systems.



---

---

---

---

---

---

---

---

79

### Data Breach

- What do you do now?
- What are your next steps?
- Time is of the essence after a security incident. Immediately after you've identified a data breach, you want to begin the process of mitigating its impact.
- If you experience a data breach, here's how to report your data loss...

---

---

---

---

---

---

---

---

80

### Data Breach

**Next Steps:**

- Contact the IRS and Law Enforcement
- Contact the states in which you prepare returns.
- Contact Experts
- Contact your clients and other services, partners, etc.

---

---

---

---

---

---

---

---

81

## Data Breach

Remain vigilant against cybercriminals by making data security a daily priority and hopefully you won't find yourself in the situation of needing to make these contacts.

But if you do... the faster you notify the necessary agencies, the better!

---

---

---

---

---

---

---

82

## Data Breach Response – A Guide for Business

<https://www.ftc.gov/business-guidance/resources/data-breach-response-guide-business>

---

---

---

---

---

---

---

83



---

---

---

---

---

---

---

84

Other Issues

Have your client obtain an Identity Protection PIN (IP PIN):  
<https://www.irs.gov/identity-theft-fraud-scams/get-an-identity-protection-pin>

85

---

---

---

---

---

---

---

Other Issues

**Fraud Alert:**  
  
Taxpayer is notified if someone tries to open an account in their name. No notification if someone uses an existing account for fraudulent purposes.

86

---

---

---

---

---

---

---

Other Issues

- Recommend that your clients put a fraud alert on their financial information.
- Can place a Fraud Alert on-line with one of the credit bureaus. That credit bureau notifies the others **automatically**.
- **No Charge!**

87

---

---

---

---

---

---

---

**Other Issues**

Credit Freeze:

No one can open a **new** financial account. Must remove freeze for taxpayer to apply for credit.

88

**Cybersecurity Summary**

☐ Treat business information as personal information.

☐ Do not make passwords easy to guess.

☐ Stay up to date on all things cyber/data security.

☐ Social media is part of the fraud tool set.

☐ It only takes one time!

☐ Install and update antivirus software.

89

**Cybersecurity Summary**

☐ If you connect it. Protect it.

☐ Back Up Your Information

☐ Connect only with people you trust.

☐ Keep Up to Date

☐ Double Your Login Protection (MFA)

90

## Cybersecurity Summary

### Password Tips:

- ✓ Use a long passphrase.
- ✓ Avoid using common words.
- ✓ Be Creative
- ✓ Keep your passwords on the "down-low."
- ✓ Unique account, unique password.

---

---

---

---

---

---

---

91

## Cybersecurity Summary

### Working From Home:

- ✓ Only use approved tools!
- ✓ Secure Your Meetings
- ✓ Secure Your Information
- ✓ Secure Yourself

---

---

---

---

---

---

---

92

## Cybersecurity Summary

### While Traveling:

- ✓ Stop Auto Connecting
- ✓ Stay protected while you are connected.
- ✓ Play hard to get with strangers.
- ✓ Never click and tell!
- ✓ Guard your mobile device(s).

---

---

---

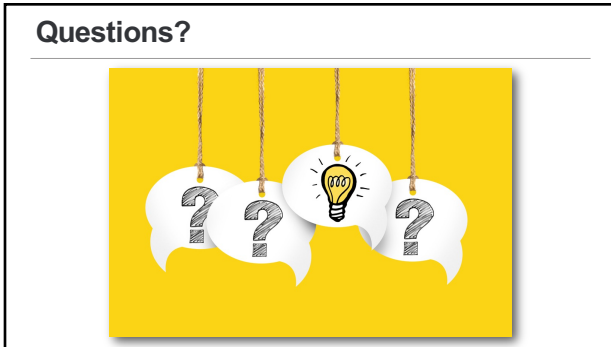
---

---

---

---

93



94

---

---

---

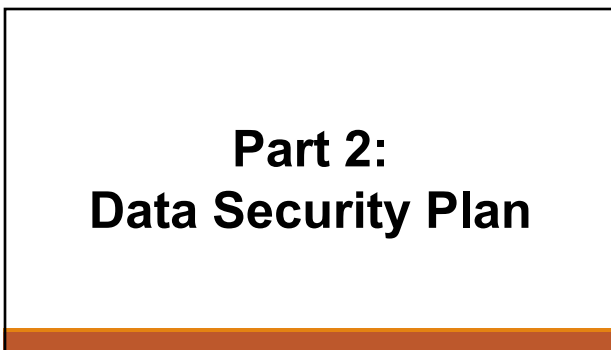
---

---

---

---

---



95

---

---

---

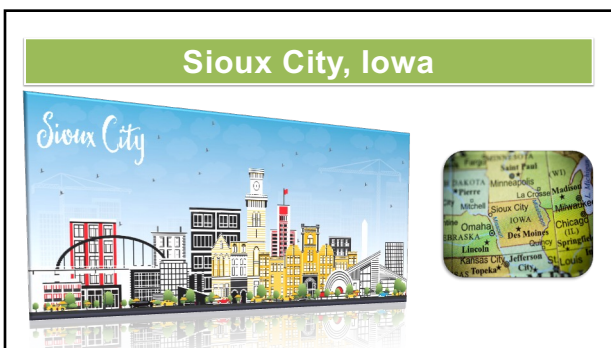
---

---

---

---

---



96

---

---

---

---

---

---

---

---



## Objectives

- IRS Security Six
- Requirements for PTIN Renewal
- Data Security Plan {WISP}

---

---

---

---

---

---

---

97

## Data Security Plan



---

---

---

---

---

---

---

98

## Quote of the Session

“A tax professional without a Data Security Plan is a wild beast set free upon this world.”

- Albert Camus (Modified)

---

---

---

---

---

---

---

99

**Data Security Plan**

***One Size Does Not Fit All!***

100

---

---

---

---

---

---

---

**Data Security Plan**

Protecting Taxpayer/Consumer Data is your obligation under the law.

101

---

---

---

---

---

---

---

**Data Security Plan - Updated**

**FTC Safeguards - Finalized June 09, 2023**

- Must designate qualified individual to oversee.
- Written risk assessment develop required.
- Monitor and limit those who can access sensitive customer information.
- Encrypt customer information on your system, even when it's in transit.

102

---

---

---

---

---

---

---

Data Security Plan - Updated

**FTC Safeguards - Finalized June 09, 2023:**

- Train Security Personnel
- Periodically Assess Practices
- MFA
- Make sure you know what you have and where you have it!
- Entered "Penalty" Phase

103

---

---

---

---

---

---

---

Data Security Plan - Updated

**Do the FTC Safeguards that were finalized on June 09, 2023, apply to your firm?**

- If You Prepare Tax Returns: Yes
- Tax and accounting professionals are considered "financial institutions" **regardless** of size of firm.

104

---

---

---

---

---

---

---

Data Security Plan - Updated

**FTC Safeguards - Finalized June 09, 2023:**

- For firms holding over 5,000 "consumer records," compliance is **mandatory**.
- Firms with less than 5,000 "consumer records," are exempt from **certain** requirements.

105

---

---

---

---

---

---

---

**Data Security Plan - Updated**

**How many “consumer records” does your firm hold? To calculate...**

The number of clients (past + present) in your software and storage drives.

+

Total Number of Employees

+

Total Number of Customers

=

Consumer Records

106

---

---

---

---

---

---

---

**Data Security Plan - Updated**

**How many “consumer records” does your firm hold:**

**Major Takeaway:**  
The FTC Safeguard is 5,000 or more consumer records **total**. Not annually. Not monthly.

107

---

---

---

---

---

---

---

**Data Security Plan**

**Two great reasons for taking action, even if your firm is under the FTC consumer records total:**

1. Clients will be confident working with you.
2. Shows you hold your firm to a higher security standard. By taking action now, should the rules be redefined, your firm will be ahead of game.

108

---

---

---

---

---

---

---

**Data Security Plan**

- Exemption is NOT a free pass on safeguard measures.**
- Your firm will still need to adhere to parts of FTC requirements.**

109

---

---

---

---

---

---

---

**Data Security Plan**

**Mandatory Rules:**

- ✓ ID qualified person to head up cybersecurity program.
- ✓ Run Risk Assessment
- ✓ Deploy Safeguards + Mitigate Risks
- ✓ Examine your infrastructure on regular basis.
- ✓ Security Awareness - Training Staff

110

---

---

---

---

---

---

---

**Data Security Plan**

**Mandatory Rules:**

- ✓ Monitor Progress
- ✓ Updates
- ✓ Incident Response Plan
- ✓ Regular Reports + Monitor Progress
- ✓ Multi-Factor Authentication {MFA}

111

---

---

---

---

---

---

---

### Data Security Plan

**Mandatory rules for firms under 5,000 “customer records”:**

- ✓ ID qualified person to head up cybersecurity program.
- ✓ Deploy Safeguards + Mitigate Risks
- ✓ Examine infrastructure on regular basis.
- ✓ Security Awareness - Training Staff
- ✓ Make Updates

112

---

---

---

---

---

---

---

### Data Security Plan

**Mandatory rules for firms under 5,000 “customer records”:**

- ✓ Standards for protecting the confidentiality, integrity, and security of customer data.
- ✓ Continual Improvement of Program
- ✓ Policy and Procedures

113

---

---

---

---

---

---

---

### Resources

- Creating a Written Information Security Plan for your Tax and Accounting Practice, IRS Publication 5708.
- Safeguarding Taxpayer Data, IRS Publication 4557.
- Protect Your Clients; Protect Yourself, IRS Publication 5293.

114

---

---

---

---

---

---

---

### Resources

**Small Business Information Security: The Fundamentals By the National Institute of Standards and Technology.**  
<https://www.ftc.gov/business-guidance/privacy-security/gramm-leach-bliley-act>  
<https://www.irs.gov/>

115

---

---

---


---

---

---

---

### Information Security for Tax Professionals



- Cybersecurity
- Personnel Security
- Operational Security
- Privacy
- Physical Security
- Contingency Planning

116

---

---

---

---

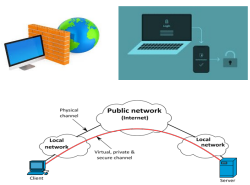
---

---

---

### IRS Security Six

- Anti-Virus Software
- Firewalls
- Two-Factor Authentication
- Backup Software or Services
- Drive Encryption {Bitlocker}
- Virtual Private Network (VPN)



117

---

---

---

---

---

---

---

Office Practices and Security

- Best practices to interchange data with your clients.
- Options to protect data work **BOTH** ways: Secure Portal!

118

---

---

---

---

---

---

---

Office Practices and Security

Send correspondence to all your clients and inform them you will **no** longer accept documents and sensitive information via email, and that they should/must use the tax firms Secure Portal.

LOG IN TO THE  
**SecurePortal**

119

---

---

---

---

---

---

---

Office Practices and Security

**Monitor Your PTIN Activity:**

- Log into your account on IRS Tax Professional PTIN System.
- A count of individual income tax returns filed and processed in the current year will be displayed.
  - *The information is updated weekly.*

120

---

---

---

---

---

---

---



### Requirement for PTIN Renewal

**Understand Your Data Security Responsibilities:**  
Paid tax return preparers **must** have a data security plan and system security protections for all taxpayer information.

Select the box below to confirm you are aware of this responsibility.

☐ Yes, I am aware of this responsibility.

121

---

---

---

---

---

---

---

### Data Security Plan



122

---

---

---

---

---

---

---

### Data Security Plan

The Gramm-Leach-Bliley Act of 1999 requires financial institutions – companies that offer consumers financial products or services like loans, financial, investment advice, or insurance – to explain their information-sharing practices to their customers and to **safeguard sensitive data.**

123

---

---

---

---

---

---

---

**Data Security Plan**

- Under the FTC Safeguards Rule, financial institutions must protect the consumer information they collect.
- The Gramm-Leach-Bliley (GLB) Act requires companies defined under the law as "financial institutions" to ensure the security and confidentiality of this type of information.
- The "financial institutions" definition includes tax professionals.

---

---

---

---

---

---

---

---

124

**Data Security Plan**

Tax professionals should make sure to do these things when writing and following their data security plans...

- Include the name of all information security program managers.
- Identify all risks to customer information.
- Evaluate risks and current safety measures.
- Design a program to protect data.
- Put the data protection program in place.
- Regularly monitor and test the program.

---

---

---

---

---

---

---

---

125

**Privacy Policy Requirements**

Tax Professionals **MUST** provide a Privacy Policy statement to all clients annually.

See handouts for sample!

---

---

---

---

---

---

---

---

126

### Privacy Policy

Enrolled Agents (EAs) like all providers of personal financial services, are now required by law to inform their clients of their policies regarding privacy of client information.

Your privacy is important to us, and we are required by law to comply with specific data-sharing regulations. Please read the following privacy policy before moving forward.

We collect nonpublic personal information (NPI) about you and your household or business from various sources, including:

- Interviews regarding your tax situation
- Organizers, or other documents that supply such information as your name, address, telephone number, Social Security Number, number of dependents, income, and other tax-related data
- Tax-related documents you provide that are required for processing tax returns, such as Forms W-2, 1099R, 1099-INT and 1099-DIV, and stock transactions
- Electronic tools and applications used to collect, store, reconcile and compile such information
- Any other documents you provide to us to assist in the preparation of your tax return.

We do not disclose any nonpublic personal information about our clients, prospective clients or former clients to anyone, except as requested by our clients in writing or as required by law.

We restrict access to personal information concerning you, except to our employees who need such information in order to provide products or services to you. We maintain physical, electronic, and procedural safeguards that comply with federal regulations to guard your personal information.

\*\*\*\*\*

Please contact us with any questions, because your privacy, our professional ethics, and the ability to provide you with quality professional services are very important to us.

---

---

---

---

---

---

---

---

127

### Information Retained

- Personally Identifiable Information {PII}
- Nonpublic Personal Information {NPI}
- Payment Card Industry {PCI}

---

---

---

---

---

---

---

---

128

### Record Retention Guide

How long should tax professionals keep records?  
See provided handout.

---

---

---

---

---

---

---

---

129

### Exchange Records

**Exchange Records with Clients:**

- ✓ Drop-off
- ✓ Pick-up
- ✓ Mail
- ✓ Email
- ✓ Secure Online Portal

130

---

---

---

---

---

---

---

### Communication

**Communicate with Clients:**

- ✓ Telephone
- ✓ Text
- ✓ Go to Meeting or Similar Virtual Meeting
- ✓ Email
- ✓ Secure Online Portal

131

---

---

---

---

---

---

---

### What is Security?

**FTC Safeguards Rules**

**Physical:**

- ☐ Keep data safe from physical threats.
- ☐ Limit Access to Computers
- ☐ Back-Up
  - Cloud Based
  - Secure Location Offsite (Portable Drive)

132

---

---

---

---

---

---

---

**What is Security?**

**FTC Safeguards Rules**

**Technical:**

- ☐ Updated Anti-Malware
- ☐ Updated Antivirus

---

---

---

---

---

---

---

133

**What is Security?**

**FTC Safeguards Rules**

**Administrative:**

- ☐ Manage and Train Staff
- ☐ Leading Cause of Data Breaches

---

---

---

---

---

---

---

134

**IRC § 7216**

- Penalty is \$1,000!
- Disclosure of tax return information is the act of making tax return information known to any person in any manner whatsoever.
- The regulations authorize two types of disclosures:
  - Certain permissible disclosures without taxpayer consent.
  - Disclosures requiring taxpayer consent.

---

---

---

---

---

---

---

135

### Data Security Plan

- Define the Written Information Security Plan (WISP) objectives, purpose, and scope.



136

---

---

---

---

---

---

---

### Data Security Plan

- The Safeguards Rule dictates that tax professionals must create and enact **Written Information Security Plans (WISPs)** to protect client data.
- The Safeguards Rule requirements are flexible so that companies can implement safeguards appropriate to their own circumstances, size, and needs of their firm.

137

---

---

---

---

---

---

---

### WISP Objective Statement

Defines the reason for the plan, stating any legal obligations such as compliance with the provisions of GLBA and sets the tone and defines the reasoning behind the plan.

138

---

---

---

---

---

---

---

WISP Objective Statement
<p>The Objective Statement should explain why the Firm developed the plan. It also serves to set the boundaries for what the document should address and why.</p>

139

---

---

---

---

---

---

---

WISP Purpose Statement
<p>Explains what and how taxpayer information is being protected with the security process and procedures.</p>

140

---

---

---

---

---

---

---

WISP Scope Statement
<p>Sets the limits on the intent and purpose of the WISP. Since you should not be legally held to a standard that was unforeseen at the writing or periodic updating of your WISP, you should set reasonable limits that the scope is intended to define.</p>

141

---

---

---

---

---

---

---

### WISP

Ensure that your security policies are appropriate to your company's:

- ✓Size – Not One Size Fits All
- ✓Complexity
- ✓Scope of Activities
- ✓Sensitivity of Customer Data

142

---

---

---

---


---

---

---

### WISP

**Do not adopt policies arbitrarily just to check a box!**



143

---

---

---

---

---

---

---

### WISP

**Security Plans are unique to each firm.**



144

---

---

---

---

---

---

---



**WISP**

**Focus on what is essential and critical to your firm - i.e.:**

- ✓ Information Systems
- ✓ Employee / Staff Training
- ✓ Detecting Issues
- ✓ Managing Issues

---

---

---

---

---

---

---

145

**WISP**

**Starting point for any WISP (previously discussed):**

- ✓ Objectives
- ✓ Purpose
- ✓ Scope

---

---

---

---

---

---

---

146

**Data Security Plan**

**Checklist (Not All Inclusive):**

- ✓ Anti-Virus Software
- ✓ Firewall
- ✓ Two-Factor Authentication (MFA)
- ✓ Backups
- ✓ Drive Encryption
- ✓ Virtual Private Networks (VPN)
- ✓ Passwords

---

---

---

---

---

---

---

147

**Data Security Plan**

**Checklist (Not All Inclusive):**

- ✓ Wireless and/or Hardwired Networks
- ✓ Protecting Stored Client Data
  - Computer
  - Cloud
  - Hard Copies
- ✓ Known Vulnerabilities and Potential Threat
- ✓ Hardware Inventory

---

---

---

---

---

---

---

148

**Data Security Plan**

**Checklist (Not All Inclusive):**

- ✓ Main Contacts / Responsible Individuals
- ✓ Security Contacts
- ✓ Users List
- ✓ Plan Readily Available
- ✓ Data Breach Procedures – See Handout...
- ✓ Spotting Data Theft
- ✓ Training Procedure
- ✓ Remote Work Policy

---

---

---

---

---

---

---

149

**Data Security Plan**

**See Handout: Creating Written Information Security Plan, IRS Publication 5708.**

---

---

---

---

---

---

---

150

### WISP

**Be On the Defensive.**

- ✓Spot Data Theft
- ✓Monitor EFIN
- ✓Internet Usage and Availability
- ✓Phishing

151

---

---

---


---

---

---

---

### Questions?



152

---

---

---

---

---

---

---



153

---

---

---

---

---

---

---

**Disclaimers:**

Opinions expressed by A.J. Reynolds are solely A.J. Reynolds' own and do not necessarily express the views or opinions of TaxAct Professional.

TaxAct is not responsible for, and expressly disclaims all liability and damages, of any kind arising out of use, reference to, or reliance on any third-party information contained on this site.



154

---

---

---

---

---

---

---



155

---

---

---

---

---

---

---