Cyber Security and Technology in the Post Covid Office – What to expect

Presented by: Jim Kramer

at MCM 2021 NFP Summit

Post Covid – Trends for 2021

- Ransomware: Bigger, Meaner, Smarter
  - Average payout $1.1 Million – just the ransom
  - Secondary cost can exceed ransom
    - Consulting Fees
    - Recovery Fees
    - Lost Productivity
    - Damaged reputation
    - Lost clients and donors
- Phishing and Spearphishing
- CIO or CISO at Executive Level
  - Threats are growing, not going away. Expect more IT exposure at the highest level
- Security Strategies and Tech Stacks
  - 70% of companies will remain hybrid work force (remote) during 2021

Cybersecurity

Ransomware Increased 715% in 2020

- Crypto-ransomware (encrypting files)
- Ensnares PC users and expands to any network –connected device
- New target in smart phones, Mac and Linux systems
  - Most recent attack was an iPhone

Phishing Increased 400% in 2020

- More workers outside the protection of the network
  - Workers must be aware of their surrounding and communications

What does the hacker of today look like?

68% - State Sponsored or Organized Crime

26% - Insider Threats

6% - Individuals or Petty Thieves

Why do hackers want data?

Here are several examples of the price for your stolen data:

Spotify Account $2.75	Hulu Account $2.75	Netflix Account $1.00 - $3.00	PayPal Credentials $1.50	Social Security Number $1.00
Driver's License $20.00	Credit Card $8.00 - $22.00	Email Address & Password $0.70 - $2.30	Medical Record from Large Scale Attack $1.50 - $10.00	Complete Medical Record Up to $1000.00

Who will pay the most for your data?

YOU!

- Primary Reasons a "Bad Actor" will steal your data
  - To Damage or Destroy the owner
  - Sell
  - Ransom
  - Blackmail

Threat Landscape

- Remote exploits
  - Made more difficult by the advent of advanced defenses.
  - Resurgence of exploits with remote users
- Insider threats
  - An often overlooked threat to the organization.
- Social engineering
  - Has become the number one attack vector.

Remote Exploits

What is a remote exploit?

- A remote exploit is a weakness in software that allows a remote attacker to take control of a system or expose non-public information from the system.
- As defenses have evolved, remote exploits have become less of a concern than social engineering.
- With remote users & BYOD this is becoming more of an issue recently

Remote Exploits (Continued)

How can I prevent remote exploits?

- Technical measures
  - Firewall
  - Intrusion prevention/intrusion detection systems
  - Anti-virus/anti-malware
- Policies
  - Patch management
  - Regular vulnerability assessments

Insider Threats

What is an insider threat?

- Threats inside the organization, such as employees, former employees, contractors/vendors, and business associates.
- Examples
  - Fraudulent transactions
  - Data theft
  - Intellectual property theft
  - Sabotage

Insider Threats (Continued)

Policies

- Job rotation
- Mandatory vacation
- Separation of duties
- Dual-control
- After-hours logoff

Insider Threats (Continued)

Technical measures

- Least Privilege
- Secure, regularly tested backups
- Data encryption
- Anomaly-based intrusion prevention
- Data loss prevention systems

Social Engineering

What is Social Engineering?

- Exploiting the weaknesses in human interaction!
- This attack is often one of the most devastating to people and organizations
- Often difficult to detect in such a fast paced world

Social Engineering

Why is it so effective?

- Three common psychological traits help social engineers succeed:
  - Our desire to be helpful
  - We are naturally curious
  - We have a fear of getting into trouble
- Social engineers have the upper hand:
  - Have unlimited time
  - Know what they are after and the probable weakness of those who guard it
  - Have a vast toolkit of attacks and techniques

Most Common Techniques

Most common techniques

+Pretexting
+Baiting
+Physical access
+Familiar Attacker
+Ramsomware
+Phishing
+Spear Phishing
+Scareware
+Man-in-the-middle attacks

Note: attacks can take place in person, via phone and via the web/e-mail

Pretexting

- Involves the use of an invented scenario, or pretext, that will engage the mark and begin a series of events that leads them to hand over information or carry out the attackers wishes
- Common examples include business email compromise (BEC) and tech support programs

Baiting

- An attacker leaves a malware-laden device, like a USB drive in a place where it will be found
- The finder picks it up and plugs it into their computer, unintentionally loading malware onto their machine

Physical Access

- Unsecured access
  - An attacker will often just walk in the door and walk through open areas to secured environments
- Piggyback
  - An attacker may walk in with a group of users
- Repair technician
  - Just because someone has a badge (with or without a picture) does not equal access.

Familiar Attacker

- An attacker gains access to an email account and then spams everyone in the account's contact list
- Tactic relies on people trusting e-mails that appear to come from someone they know

Ransomware

What is it?

Malware that locks up your data and won't unlock it unless you pay a ransom

+Very popular

+Single reason that Bitcoin maintains high value

+Proper security awareness and techniques can help protect you

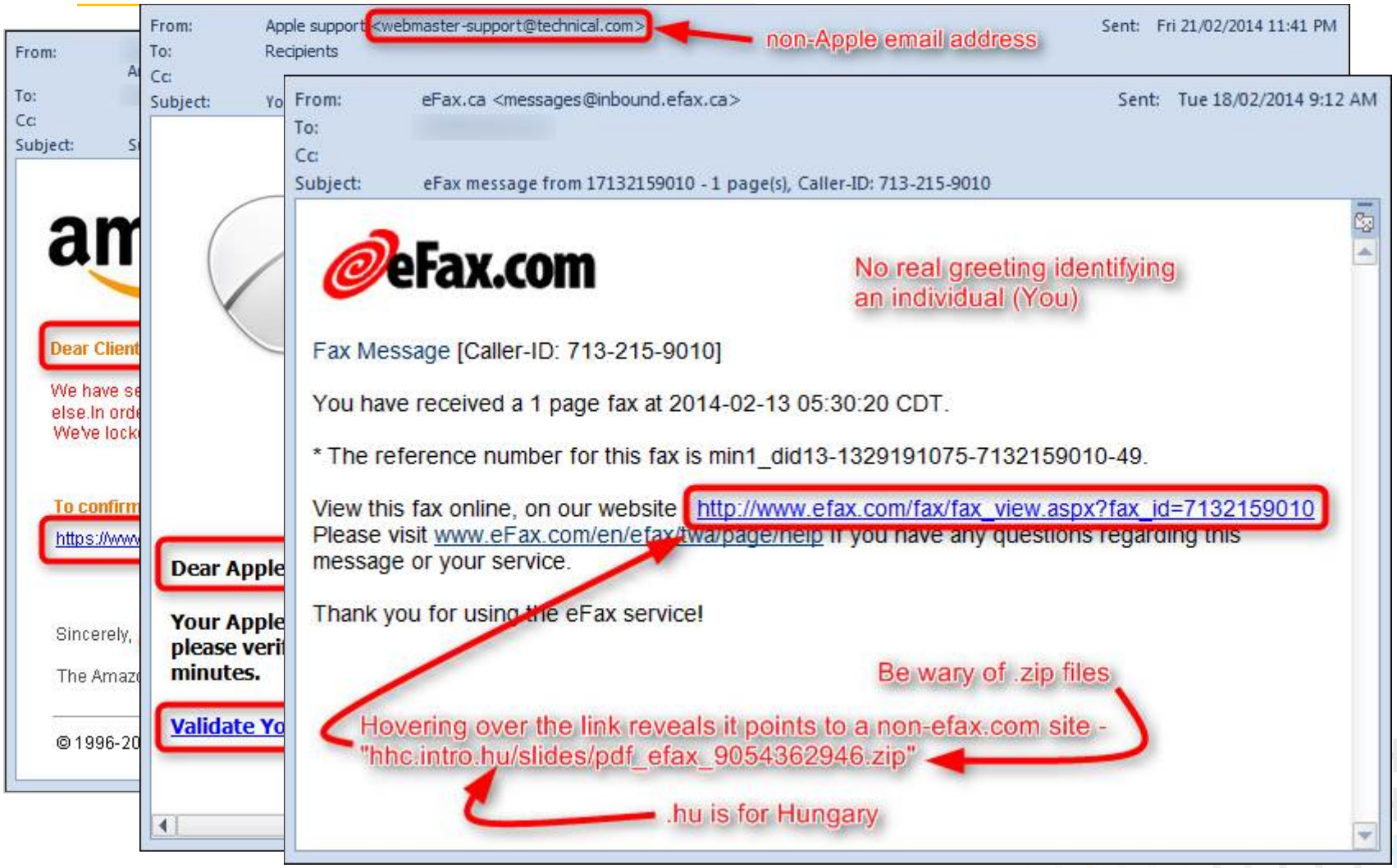
+Many companies pay the ransom to get their data back

Phishing

Simply, gathering information via fraud

- Most common data they're after? User credentials (work, bank, home), banking information, etc.
- They do this by posing (masquerading) as someone or something else.
- Phishing and Social Engineering are often the first lines of attack when trying to breach an organization
- Rebuffing their attack here, can show a solid security presence and hopefully thwart an attack or at least alert IT to its presence.
- A malicious party sends a fraudulent e-mail disguised as a legitimate e-mail, often purporting to be from a trusted source
- The message is intended to trick the recipient into sharing personal or financial information or clicking on a link that installs malware

Phishing Examples



Phishing vs. Spear Phishing

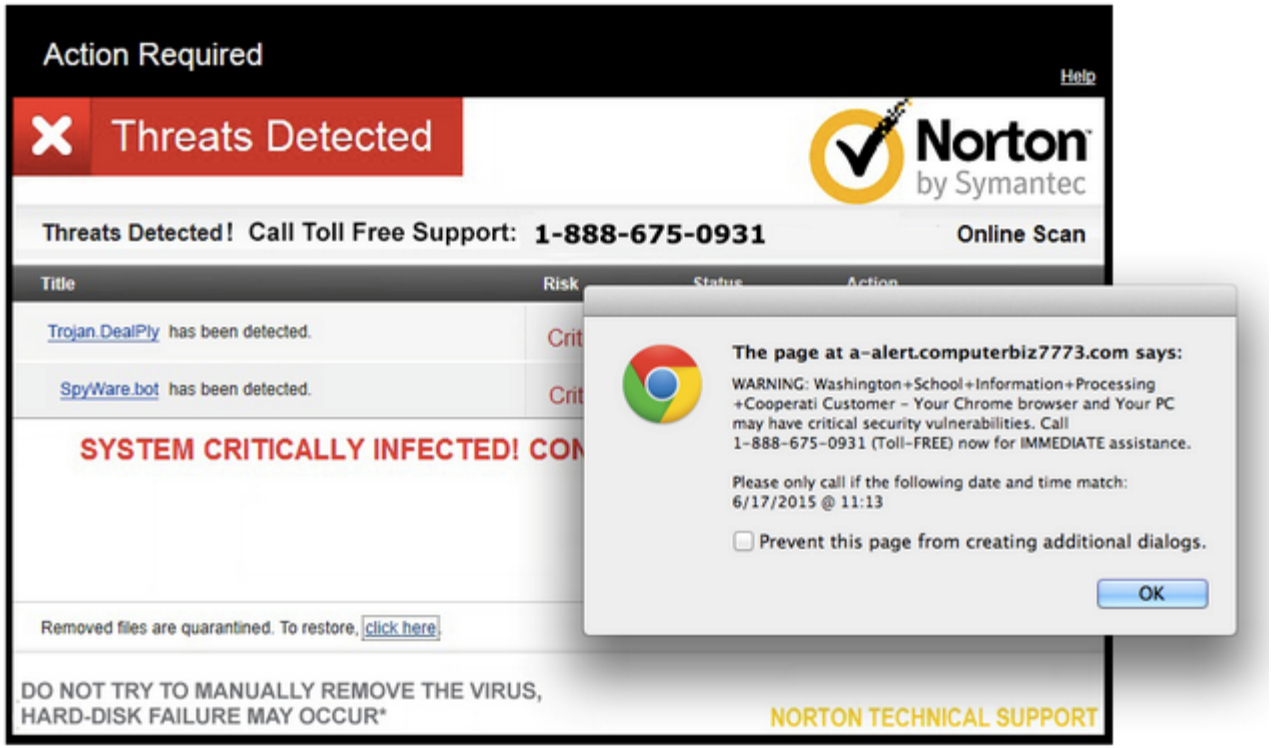
+ Similar techniques…

Phishing	Spear Phishing
Generally an exploratory attack targeting a broader audience	A more targeted version
Typically more straightforward in nature – once information is stolen, attackers have what they intended to get	Theft of credentials or personal information is usually the beginning of the attack, used to gain access to the target network

Scareware

- Involves tricking a victim into think his or her computer is infected with malware or has inadvertently downloaded illegal content
- Attacker then offers the victim a solution that will fix the bogus problem
- What really happens is the victim is tricked into downloading the “fix”, which is the attacker’s malware

Scareware Example



- Appears to be from a valid source
- Sense of urgency created by pop-up box
- False sense of security with confirmation of date and time

Man-In-The-Middle Attacks

- Involves an attack where the attacker will setup a wireless AP using the same SSID as a Free / Open Wireless network
- When users connect to the AP, the attacker will pass your data to the real network and collect the data stream

First Step in Protection

- **Establish Your Baseline**

- Evaluate existing policies and procedures governing security
- Conduct system vulnerability and penetration testing
- Perform a security controls assessment
  - SOC 2 Verification

Social Engineering Prevention

How can I prevent successful social engineering attacks?

- Security awareness training
- Policies
  - Requests for confidential employee information must be made in-person.
  - Wire transfer information must not be sent or accepted via email (use ACH when possible).
  - Visitors must wear a visitor badge and be escorted when in the building.

Social Engineering (Continued)

Technical measures

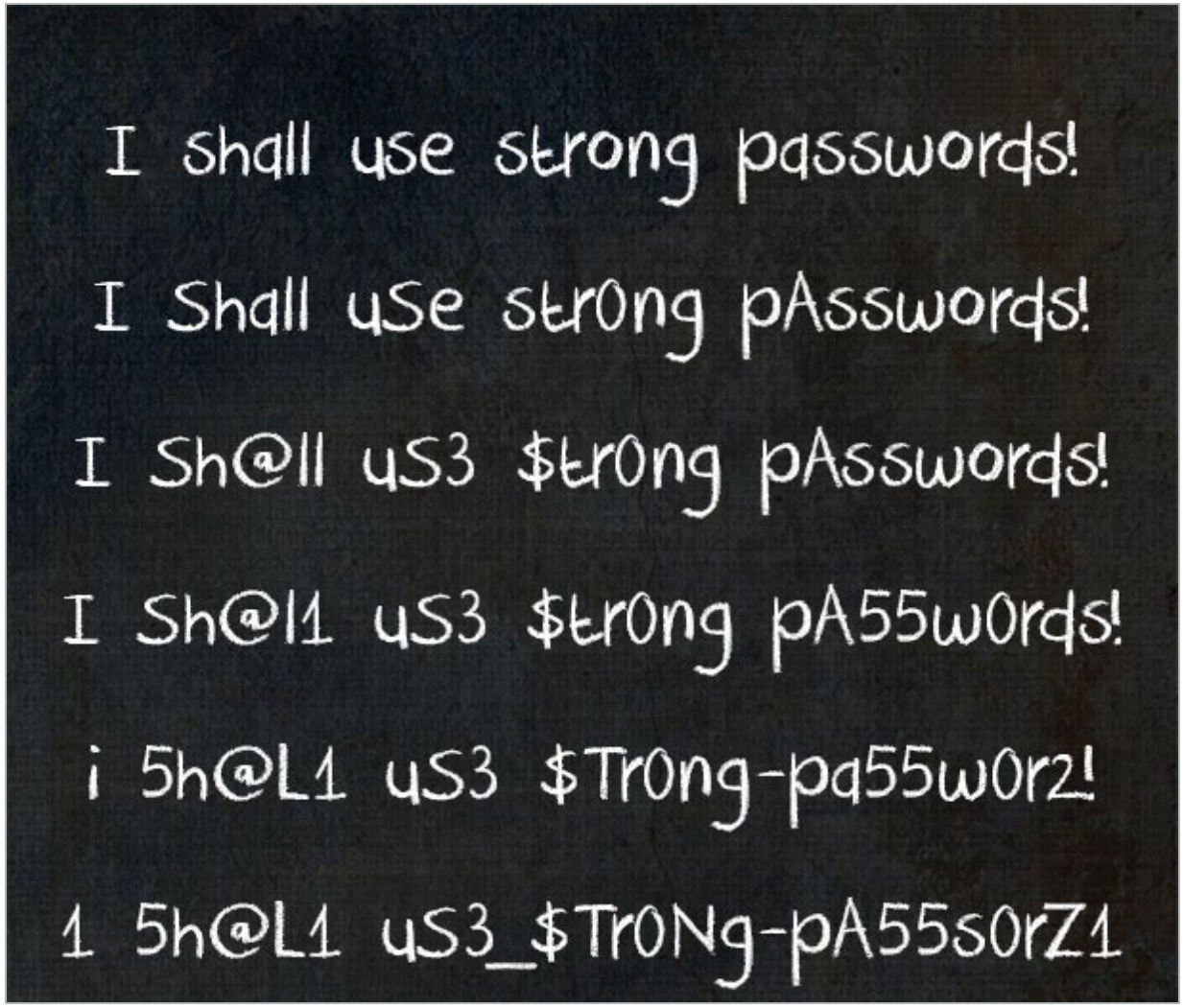
+ Visual cues
+ Least-privilege
+ Email spam/malware filtering
+ Web content filtering
+ DNS Filters
+ Anti-malware/anti-virus

Password Security

If your password looks anything like the ones below, change it!

1. 123456
2. 123456789
3. Qwerty
4. password
5. 1234567
6. 12345678
7. 12345
8. Iloveyou
9. 111111
10. 123123
11. abc123
12. Qwerty123
13. 1q2w3e4r
14. Admin
15. qwertyuiop
16. 654321
17. 555555
18. dragon
19. princess
20. welcome

Password Security



Password Security

Tips For Home

- WiFi Router Password
- WiFi Security
  - WEP
  - WPA
- Change your PWs for home often!
- Different accounts for family members/guests
  - NexFlix
  - Disney+
  - Home Security System

Tips for Work

- Simple rule: If you ever find yourself speaking your PW…STOP!
- Complex helps but length is better
- Use Pass Phrase – not Password
- Come up with your own unique algorithm
- Don't reuse key passwords
- Under no circumstances do you give it away!

Password Security

Tips for Work

- If you think you've made a mistake, change your password!
- In general, it's best not write passwords down anywhere.
- Passphrases are better than passwords
- Don't use the same passwords across multiple platforms
  - ***MOST ESPECIALLY – Don't use password on personal sites/services that you use for work***
- Breathe easy, Passwords won't be around forever!
  - Biometrics on the rise
- USE MFA whenever possible

Risk Minimization

- Security Posture
  - Layered Protection
  - Documented Security Policy and Manual
  - SOC Compliance or other verification
- Management Support
  - Solutions come from the top down
  - Leadership awareness and promotion
- Equipment Documentation
  - Compliant HW and SW
  - Training
  - Outside Verification

Cybersecurity

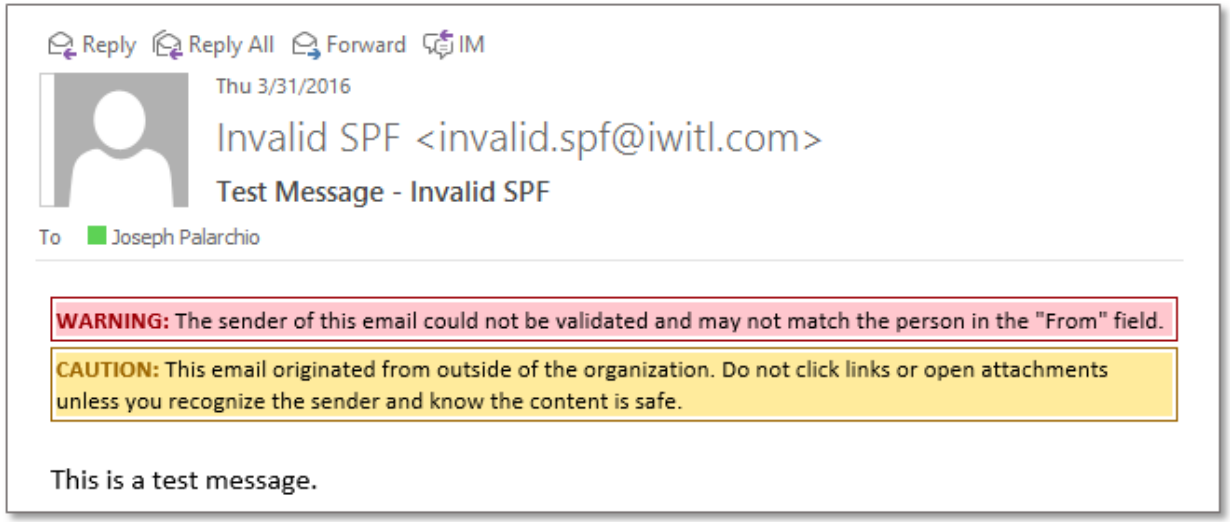
TECHNOLOGY SOLUTIONS

Ways to Reduce Risk

+ Patching vulnerabilities
+ Maintaining good software
+ Deploying effective email filters
+ Using intrusion prevention and detection software
+ Restricting third-party access to company data
+ Employing encryption where appropriate to security confidential data
+ Implementing data loss prevention technology
+ Employee and customer awareness programs

Use tools to assist with identification

How can I prevent successful social engineering attacks?



Methods to Minimize the Risk

- Develop a security policy and manual
  - Make this available to all employees
  - Update on a routine basis as threats are continually evolving
- Prioritize and address any gaps or observations resulting from vulnerability and penetration testing (must perform them first)
- Where possible, use technology to take decision making away from the employee
- Train your staff! Make them your #1 security source
- Implement Multi-Factor Authentication

Ask
Answer
Who
Where
How
Question
Apply
Why
Understand
What
When
Answers
Query
Questions

Contact Information

+ Jim Kramer

+ Jim.Kramer@mcmcpa.com
+ 502.882.4348
+ www.mcmcpa.com

2021 Summer Not-for-Profit Summit

TAX UPDATE

Eleanor Livingston, CPA, MST
Tax Senior Manager

Agenda

- 990 reporting
  - Compensation
  - Public support
- UBTI update and maintaining tax exemption in challenging times
- State registration
- IRS workplan
- Bits and pieces

Compensation

- Has to be "reasonable"
- Rebuttable presumption
  - Approved in advance by governing body
  - Use of comparability data
  - Documentation of process and discussion

15	Did the process for determining compensation of the following persons include a review and approval by independent persons, comparability data, and contemporaneous substantiation of the deliberation and decision?			
a	The organization's CEO, Executive Director, or top management official	15a		
b	Other officers or key employees of the organization	15b		
	If "Yes" to line 15a or 15b, describe the process in Schedule O (see instructions).			

Compensation Reporting

- Who has to be included on Part VII?
  - Officers
  - Key Employees
  - Highest compensated employees

- Officer
  - What do the by-laws say
  - Top management and top financial officials

Compensation Reporting (cont'd)

- Key employees
  - $150K of reportable compensation
  - Responsibility test
    - Manages whole organization OR
    - Manages discrete segment that comprises 10% or more of the organization as determined by activities, assets, revenue or expense OR
    - Has or shares authority to control or determine 10% or more of organization's capital expenditures, operating budget or compensation of employees
  - Top 20 test

Compensation Reporting (cont'd)

- Highest compensated employees
  - Reportable compensation of $100K or more
  - Not already listed as officer or key employee

Employee Retention Credit

- Just a reminder that this has been extended
- Any amounts used for credit purposes cannot also be used for loan forgiveness purposes
- Eligibility
- 2021 credit is 70% of $10,000 per quarter per employee (2020 was 50% of $10,000 per year per employee)

Public Support Test

+ Schedule A of your 990

SCHEDULE A
(Form 990 or 990-EZ)

Department of the Treasury
Internal Revenue Service

Public Charity Status and Public Support

Complete if the organization is a section 501(c)(3) organization or a section 4947(a)(1) nonexempt charitable trust.

► Attach to Form 990 or Form 990-EZ.

► Go to *www.irs.gov/Form990* for instructions and the latest information.

OMB No. 1545-0047

2019

Open to Public Inspection

Name of the organization | **Employer identification number**

Part I **Reason for Public Charity Status** (All organizations must complete this part.) See instructions.

The organization is not a private foundation because it is: (For lines 1 through 12, check only one box.)

1 ☐ A church, convention of churches, or association of churches described in **section 170(b)(1)(A)(i).**

2 ☐ A school described in **section 170(b)(1)(A)(ii).** (Attach Schedule E (Form 990 or 990-EZ).)

3 ☐ A hospital or a cooperative hospital service organization described in **section 170(b)(1)(A)(iii).**

4 ☐ A medical research organization operated in conjunction with a hospital described in **section 170(b)(1)(A)(iii).** Enter the hospital's name, city, and state:

5 ☐ An organization operated for the benefit of a college or university owned or operated by a governmental unit described in **section 170(b)(1)(A)(iv).** (Complete Part II.)

6 ☐ A federal, state, or local government or governmental unit described in **section 170(b)(1)(A)(v).**

7 ☐ An organization that normally receives a substantial part of its support from a governmental unit or from the general public described in **section 170(b)(1)(A)(vi).** (Complete Part II.)

8 ☐ A community trust described in **section 170(b)(1)(A)(vi).** (Complete Part II.)

9 ☐ An agricultural research organization described in **section 170(b)(1)(A)(ix)** operated in conjunction with a land-grant college or university or a non-land-grant college of agriculture (see instructions). Enter the name, city, and state of the college or university:

10 ☐ An organization that normally receives: (1) more than 33 1/3% of its support from contributions, membership fees, and gross receipts from activities related to its exempt functions—subject to certain exceptions, and (2) no more than 33 1/3% of its support from gross investment income and unrelated business taxable income (less section 511 tax) from businesses acquired by the organization after June 30, 1975. See **section 509(a)(2).** (Complete Part III.)

Schedule A Public Support

Part II

Part III. If the organization fails to

Section A. Public Support

	Calendar year (or fiscal year beginning in) ►
1	Gifts, grants, contributions, and membership fees received. (Do not include any "unusual grants.") . . .
2	Tax revenues levied for the organization's benefit and either paid to or expended on its behalf . . .
3	The value of services or facilities furnished by a governmental unit to the organization without charge . . . .
4	**Total.** Add lines 1 through 3 . . . .
5	The portion of total contributions by each person (other than a governmental unit or publicly supported organization) included on line 1 that exceeds 2% of the amount shown on line 11, column (f) . . . .
6	**Public support.** Subtract line 5 from line 4

Part III

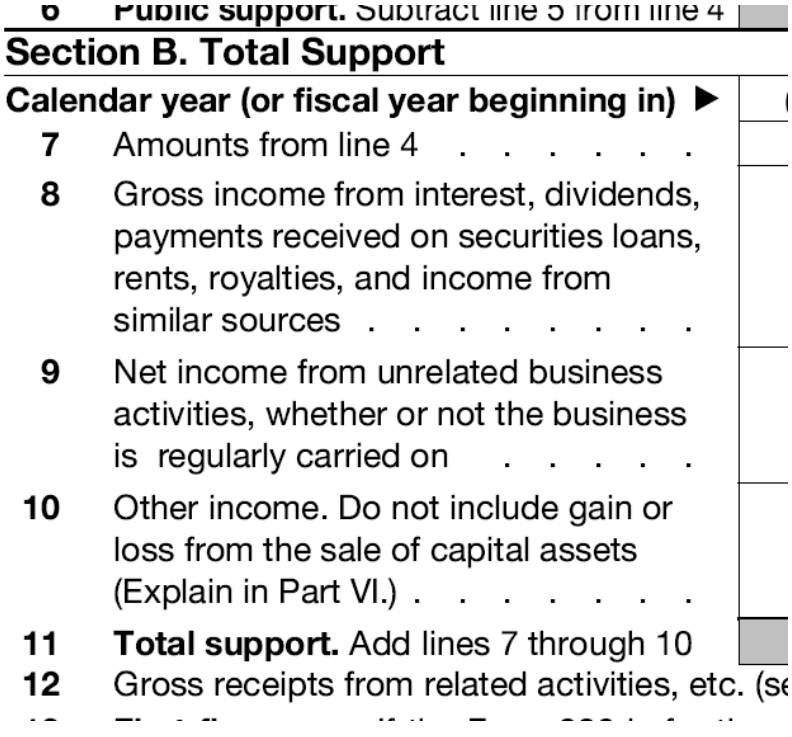
Part III **Support Schedule for Organizations**
(Complete only if you checked the bo
If the organization fails to qualify unde

Section A. Public Support

	Calendar year (or fiscal year beginning in) ►	**(a)**
1	Gifts, grants, contributions, and membership fees received. (Do not include any "unusual grants.")	
2	Gross receipts from admissions, merchandise sold or services performed, or facilities furnished in any activity that is related to the organization's tax-exempt purpose . . .	
3	Gross receipts from activities that are not an unrelated trade or business under section 513	
4	Tax revenues levied for the organization's benefit and either paid to or expended on its behalf	
5	The value of services or facilities furnished by a governmental unit to the organization without charge	
6	**Total.** Add lines 1 through 5	
7a	Amounts included on lines 1, 2, and 3 received from disqualified persons .	
b	Amounts included on lines 2 and 3 received from other than disqualified persons that exceed the greater of $5,000 or 1% of the amount on line 13 for the year	
c	Add lines 7a and 7b	
8	**Public support.** (Subtract line 7c from line 6.)	

Schedule A Public Support

Part II



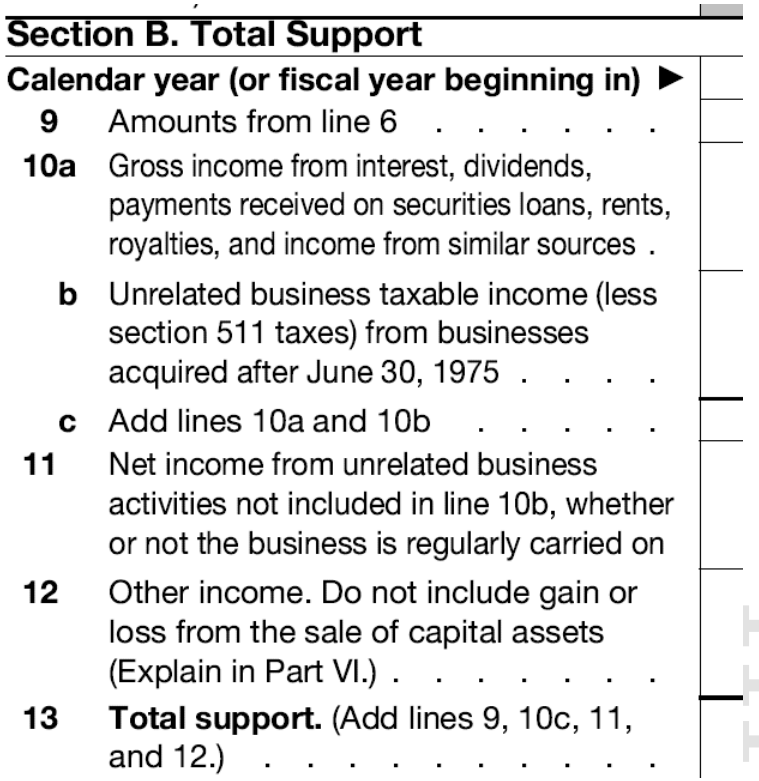
6 **Public support.** Subtract line 5 from line 4

Section B. Total Support

Calendar year (or fiscal year beginning in) ▶

7	Amounts from line 4 . . . . .
8	Gross income from interest, dividends, payments received on securities loans, rents, royalties, and income from similar sources . . . . .
9	Net income from unrelated business activities, whether or not the business is regularly carried on . . . . .
10	Other income. Do not include gain or loss from the sale of capital assets (Explain in Part VI.) . . . . .
11	**Total support.** Add lines 7 through 10
12	Gross receipts from related activities, etc. (se

Part III



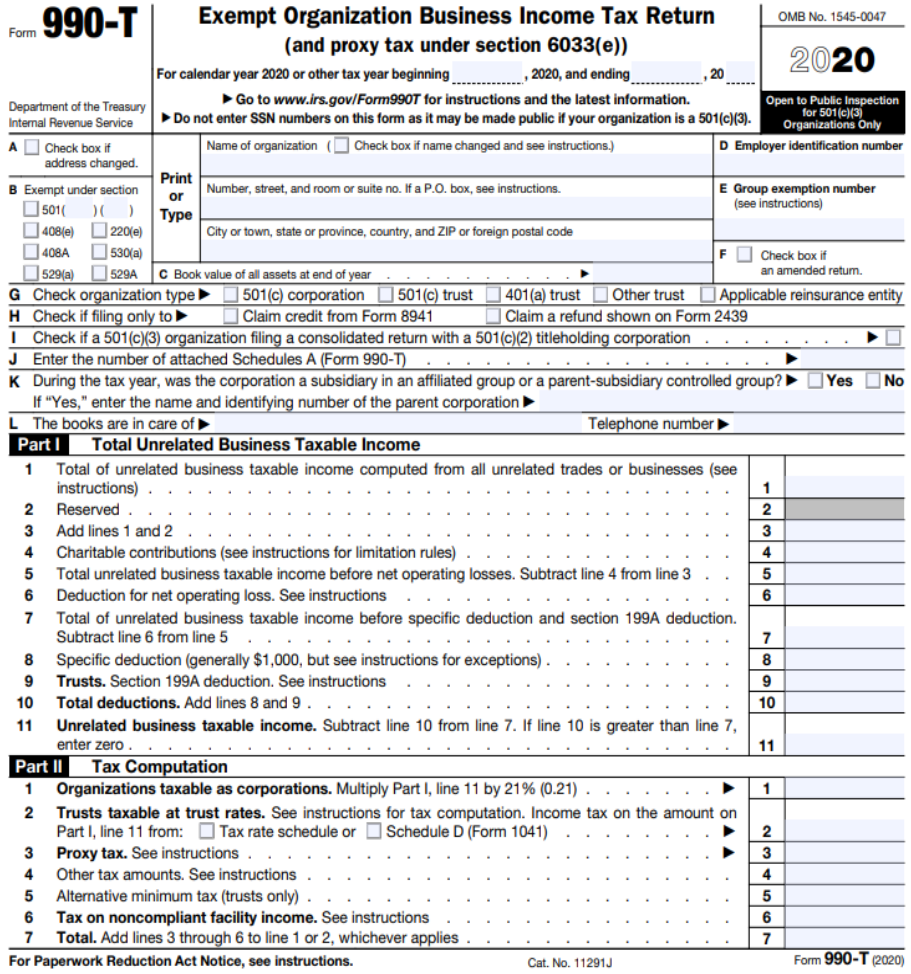
Section B. Total Support

Calendar year (or fiscal year beginning in) ▶

9	Amounts from line 6 . . . . .
10a	Gross income from interest, dividends, payments received on securities loans, rents, royalties, and income from similar sources .
b	Unrelated business taxable income (less section 511 taxes) from businesses acquired after June 30, 1975 . . . .
c	Add lines 10a and 10b . . . . .
11	Net income from unrelated business activities not included in line 10b, whether or not the business is regularly carried on
12	Other income. Do not include gain or loss from the sale of capital assets (Explain in Part VI.) . . . . .
13	**Total support.** (Add lines 9, 10c, 11, and 12.) . . . . .

UBTI Update

2020 990-T reformatted



Form **990-T** — **Exempt Organization Business Income Tax Return (and proxy tax under section 6033(e))**

OMB No. 1545-0047

2020

For calendar year 2020 or other tax year beginning , 2020, and ending , 20

▶ Go to *www.irs.gov/Form990T* for instructions and the latest information.

▶ Do not enter SSN numbers on this form as it may be made public if your organization is a 501(c)(3).

Open to Public Inspection for 501(c)(3) Organizations Only

Department of the Treasury
Internal Revenue Service

A ☐ Check box if address changed.

B Exempt under section
☐ 501( )( ) ☐ 408(e) ☐ 220(e) ☐ 408A ☐ 530(a) ☐ 529(a) ☐ 529A

Print or Type

Name of organization (☐ Check box if name changed and see instructions.)

Number, street, and room or suite no. If a P.O. box, see instructions.

City or town, state or province, country, and ZIP or foreign postal code

C Book value of all assets at end of year ▶

D Employer identification number

E Group exemption number (see instructions)

F ☐ Check box if an amended return.

G Check organization type ▶ ☐ 501(c) corporation ☐ 501(c) trust ☐ 401(a) trust ☐ Other trust ☐ Applicable reinsurance entity

H Check if filing only to ▶ ☐ Claim credit from Form 8941 ☐ Claim a refund shown on Form 2439

I Check if a 501(c)(3) organization filing a consolidated return with a 501(c)(2) titleholding corporation ▶ ☐

J Enter the number of attached Schedules A (Form 990-T) ▶

K During the tax year, was the corporation a subsidiary in an affiliated group or a parent-subsidiary controlled group? ▶ ☐ Yes ☐ No
If "Yes," enter the name and identifying number of the parent corporation ▶

L The books are in care of ▶ Telephone number ▶

Part I Total Unrelated Business Taxable Income

1	Total of unrelated business taxable income computed from all unrelated trades or businesses (see instructions)	1	
2	Reserved	2	
3	Add lines 1 and 2	3	
4	Charitable contributions (see instructions for limitation rules)	4	
5	Total unrelated business taxable income before net operating losses. Subtract line 4 from line 3	5	
6	Deduction for net operating loss. See instructions	6	
7	Total of unrelated business taxable income before specific deduction and section 199A deduction. Subtract line 6 from line 5	7	
8	Specific deduction (generally $1,000, but see instructions for exceptions)	8	
9	**Trusts.** Section 199A deduction. See instructions	9	
10	**Total deductions.** Add lines 8 and 9	10	
11	**Unrelated business taxable income.** Subtract line 10 from line 7. If line 10 is greater than line 7, enter zero	11	

Part II Tax Computation

1	**Organizations taxable as corporations.** Multiply Part I, line 11 by 21% (0.21) ▶	1	
2	**Trusts taxable at trust rates.** See instructions for tax computation. Income tax on the amount on Part I, line 11 from: ☐ Tax rate schedule or ☐ Schedule D (Form 1041) ▶	2	
3	**Proxy tax.** See instructions ▶	3	
4	Other tax amounts. See instructions	4	
5	Alternative minimum tax (trusts only)	5	
6	**Tax on noncompliant facility income.** See instructions	6	
7	**Total.** Add lines 3 through 6 to line 1 or 2, whichever applies	7	

For Paperwork Reduction Act Notice, see instructions. Cat. No. 11291J Form **990-T** (2020)

UBTI Update

- Siloing regs
  - Good news – 2 digit NAICS code
  - Expense allocation

- Sponsorship payments
  - "Substantial" benefit can give rise to UBTI

- Efiling

UBTI & Maintaining Exempt Status

- How does what you're wanting to do align with your exempt purpose?
- How much of your revenue is from unrelated businesses?
- Affinity fundraising
  - Qualified sponsorship payment, advertising or licensing revenue?
- Advertising
- Licensing Agreements

State Registration

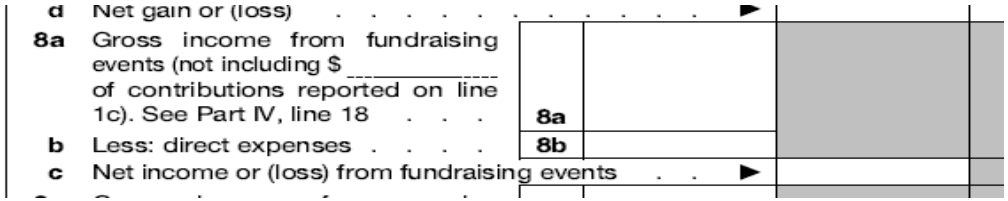
- Keep in mind that soliciting donations online typically requires you to register in every state you receive donations from
- 25 states require that written solicitations include disclosures *
  - Provide details of charitable registration status
  - Directions on where to find more information on entity's mission and financials
- Deciding where to register

IRS TE/GE Workplan FY 2021

- Strengthen compliance activities
- Improve operational efficiencies
- Maintain a taxpayer-focused organization
- Ensure awareness and collective understanding
- Leverage technology and data analytics
- Develop the TE/GE workforce

Bits and Pieces

- Program Service Accomplishments
- Donor Advised Funds and Giving Levels
- Schedule G – break out contributions



d	Net gain or (loss)			
8a	Gross income from fundraising events (not including $ _____ of contributions reported on line 1c). See Part IV, line 18	8a		
b	Less: direct expenses	8b		
c	Net income or (loss) from fundraising events			

- Electronic return copies
- 2021 tax proposals
- Remote work and payroll

Eleanor A. Livingston, CPA, MST
502.882.4483
eleanor.livingston@mcmcpa.com

PEOPLE MATTER

LEADERS INSPIRE

EXCELLENCE RULES

IRS Circular 230 Disclosure.

- As a result of perceived abuses, the Treasury has recently promulgated Regulations for practice before the IRS. These Circular 230 regulations require all accountants to provide extensive disclosure when providing certain written tax communications to clients. In order to comply with our obligations under these Regulations, we would like to inform you that any advice given in this presentation, including any attachments, cannot be used to avoid penalties which the IRS might impose, because we have not included all of the information required by Circular 230, nor have we performed services that rise to this level of assurance.