

The Importance of Agile End User Training in Improving a Company's Security Posture



CompTIA[®]

Instructor Network

CompTIA

Stephen Schneider



CompTIA Instructor Network Program Manager,
Product Manager, Security+

sschneider@CompTIA.org



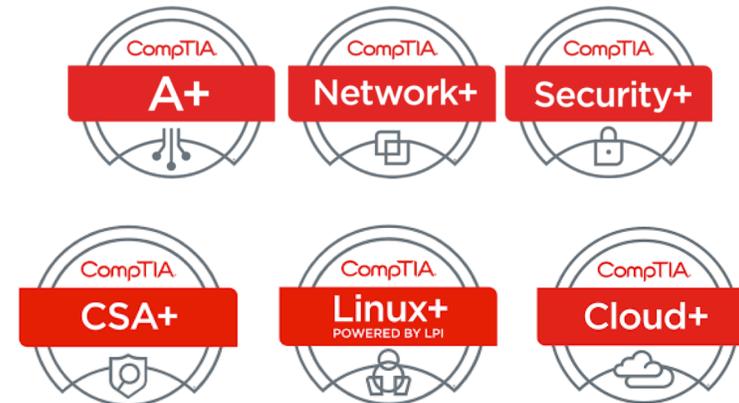
@TeachCompTIA

Stephen is responsible for assisting instructors internationally get the most out of CompTIA certifications. The goal of the network is to help instructors with best practices, strategies and tools to help lead a successful training event and help their students attain certification.

CompTIA is . . .

The voice of the world's information technology (IT) industry.

- ✓ **Non-profit:** We are the world's largest IT trade association advancing the global interests of IT professionals.
- ✓ **Philanthropic:** CompTIA's Creating IT Futures Foundation helps provide opportunity for the unemployed and under-employed to gain access to careers in IT.
- ✓ **A force for change through advocacy:** CompTIA promotes sound public policy at the state and federal level to advance the digital economy.
- ✓ **Membership:** With our acquisition of the Association of IT Professionals, we have extended our reach to IT Professionals worldwide. We also have thousands of corporate members.
- ✓ **A leader in IT certifications:** With over 2 million certified professionals, CompTIA offers IT professionals a roadmap for establishing and advancing their careers.





CompTIA
Instructor Network



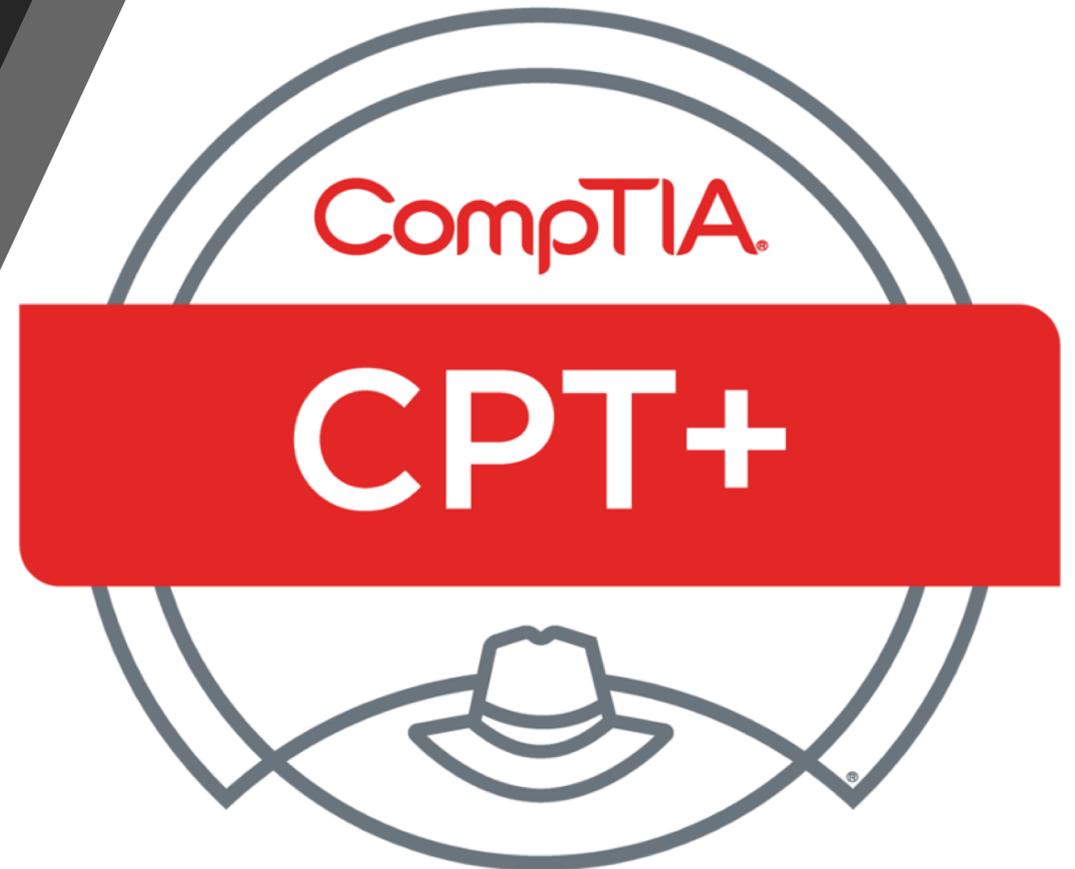
CompTIA.
Instructor Network

Announcements



Upcoming Events

- CompTIA CPT+ BETA EXAM – January 31, 2018
 - Time still available to take the beta exam for a little while longer
- CompTIA CPT+ Sneak
 - January 30, 2018
 - Inside look at CPT+ objectives
 - Provides an idea as to what to expect on CPT+ Exam
 - Registration link <http://bit.ly/2kMxEK7>
- Exam will be available Q3





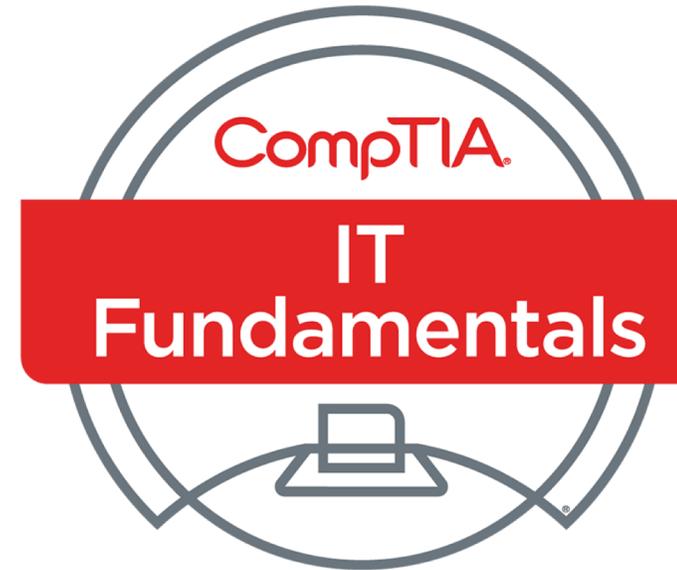
Upcoming Events – CASP TTT

- April 10th - May 16th
- Covers all objectives, not **just** new topics.
- Content will be presented as if you were a student
- Opportunity to Interact with instructor and other participants
- Training material will be provided
- **Teaching strategies and delivery best practices**
- **Demonstrations of different activities and labs**
- Homework activities will be assigned



ITF beta exam

- The updated CompTIA IT Fundamentals exam coming in Q3 2018!
- Our beta exam will be available on February 21st, 2018.



Partner Webinar February 28:
Recording: <http://bit.ly/2FY1Smk>

ITF Sneak Peek: March 13!
Recording: <http://bit.ly/2FxrjMH>

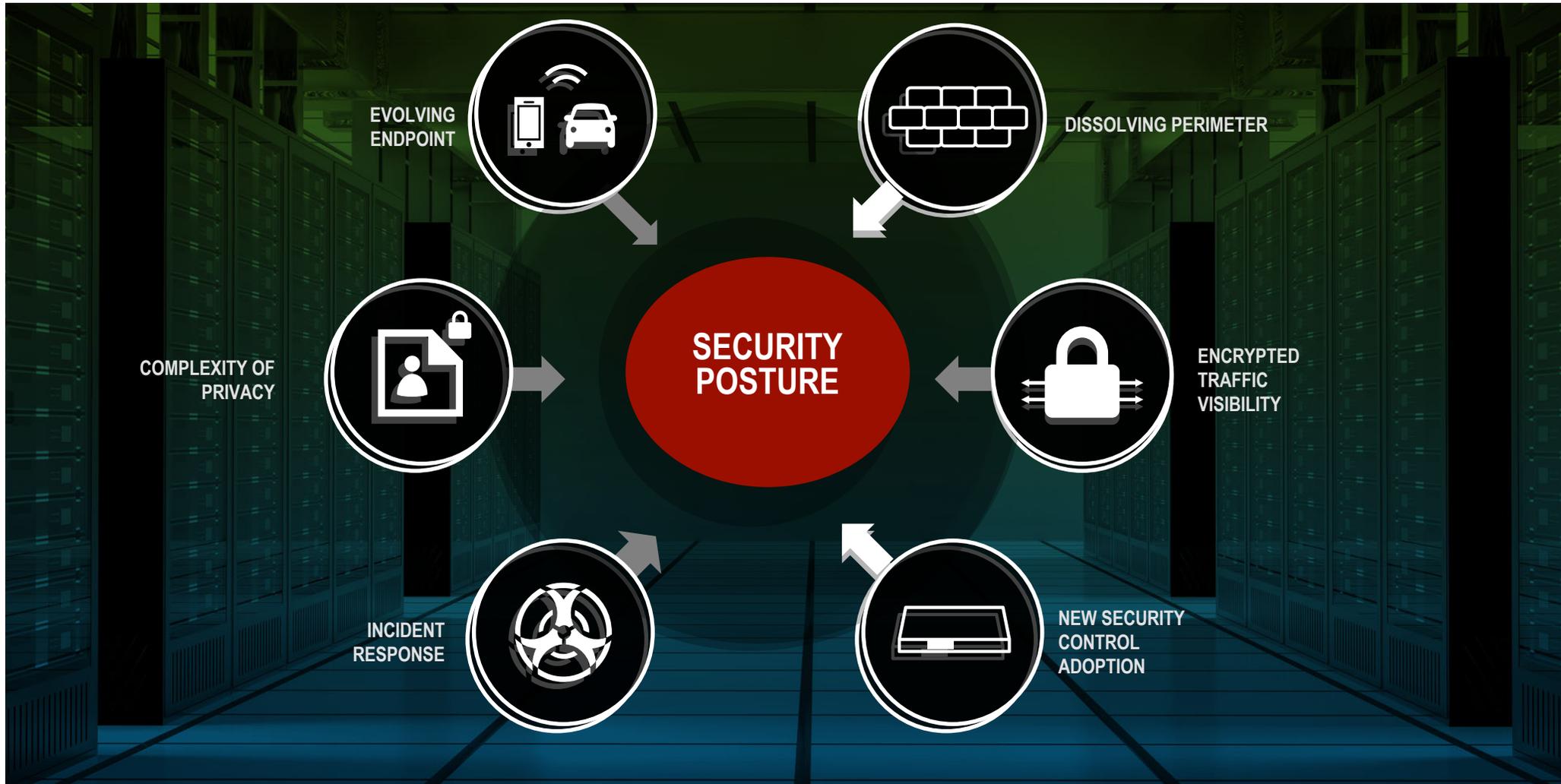
So let's talk Network Resiliency

- Current Trends
- Looking to the future
- Should I turn to the clouds?
- Today's security strategy
- Disturbing Trends
- How do you make a resilient network?
- Where is the rocket science?



Current trends

The changing security landscape – increasing the “attack surface”



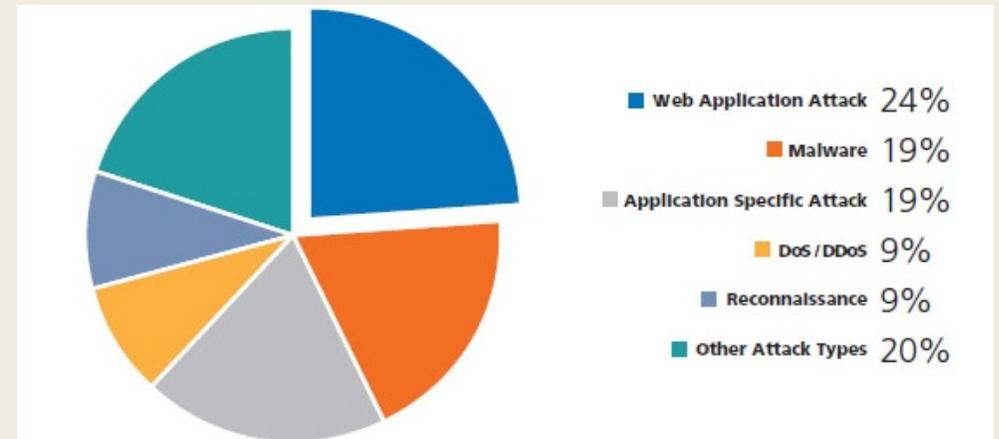


What security issues are we facing in the future?

- In some ways, the usual problems
- Each affects network resilience
- But, notice:
 - Web and malware remain at the top
 - 20% of attacks is “Other.” What does that mean?

Top 3 Industries Targeted

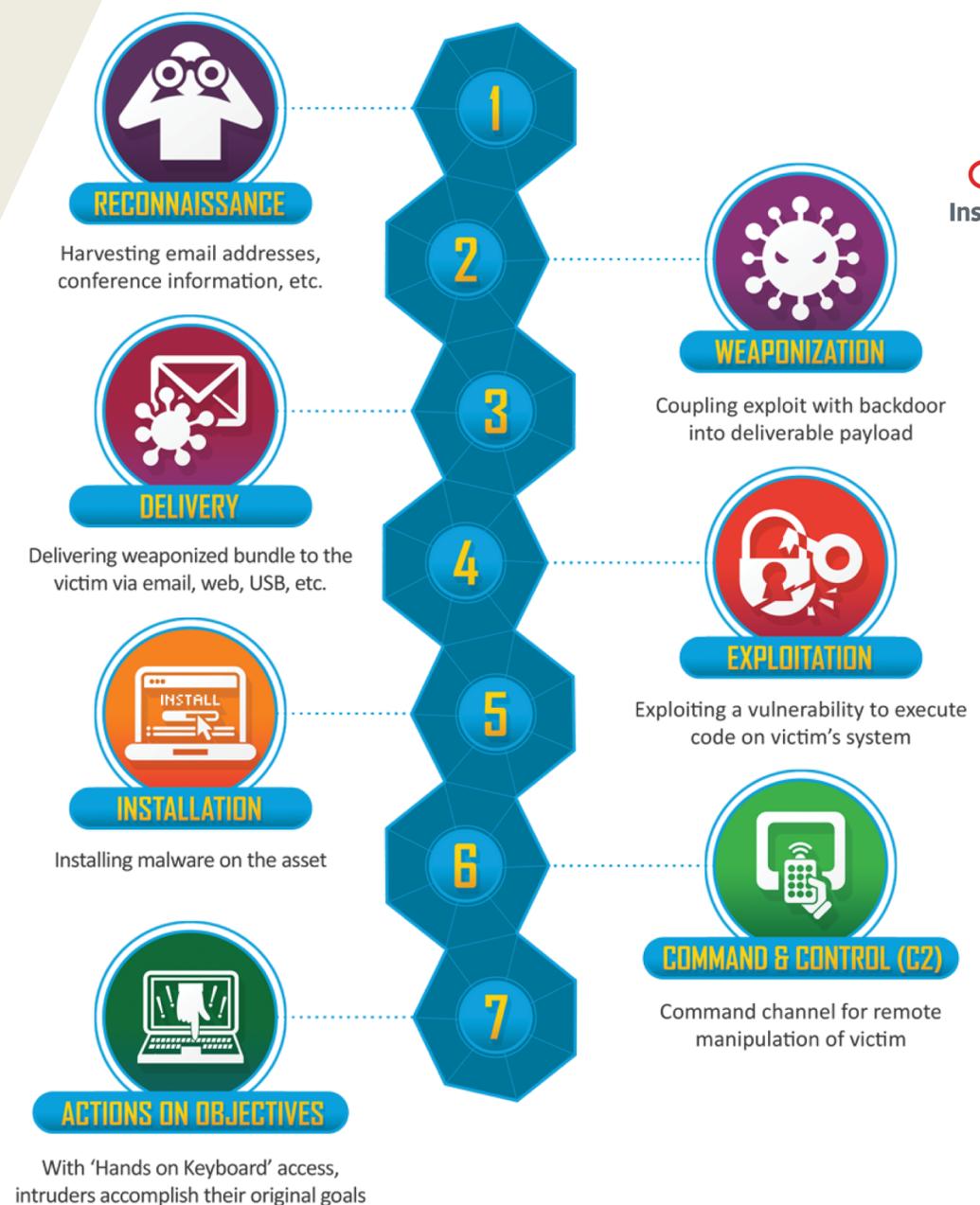
1.  **45%** IT SERVICES/CLOUD/SAAS
2.  **23%** FINANCIAL SERVICES
3.  **14%** PUBLIC SECTOR



Today's attack strategies and tactics

ATP

- Long-term infiltration
 - Requires significant reconnaissance
 - Highly-skilled individuals
 - Traditionally state-sponsored
 - Multi-team attacks
- Persistent issues
 - **Silo-based communication**
 - Weak authentication
 - End point issues
 - IoT
 - Mobile devices
 - No practical monitoring
 - **Few practical metrics**
 - Covert channels
 - Cloud implementations
 - Don't know business



<https://www.lockheedmartin.com/us/what-we-do/aerospace-defense/cyber/cyber-kill-chain.html>

Ransomware

- One of the biggest issues today
 - How it gets in
 - What it can do to a company
 - Where is the help desk in all of this?
- How to address it
 - Training
 - Removal / payment
 - Creating a resilient presence
 - Properly pivot resources



“It’s a 1-billion dollar a year business that is now in the cloud.”

-- John Dvorak, formerly of the United States Federal Bureau of Investigation (FBI)

“Our organization has been the target of multiple phishing attacks in the past year. We have utilized our helpdesk to communicate with end-users and provide user education regarding how to spot and avoid phishing scams.”



The new things to watch out for on the horizon!

The screenshot shows a web browser window with a single tab titled "IDN Homograph Example". The address bar displays "https://apple.com". The page content includes the heading "Hey there!" followed by a paragraph: "This site is obviously not affiliated with Apple, but rather a demonstration of a flaw in the way unicode domains are handled in browsers. **It is very possible that your browser isn't affected.**" Below this is a link: "Check out the [complete blog post](#) by [Xudong Zheng](#) for more details."

<https://www.theguardian.com/technology/2017/apr/19/phishing-url-trick-hackers>



New unicode domain name phishing attack

The screenshot shows a browser window with the address bar displaying `https://apple.com`. A 'Site Security' overlay is visible, showing a green padlock icon, the text 'apple.com', 'Secure Connection', and 'Verified by: Amazon'. The page content behind the overlay includes the word 'here!' in large bold text, followed by a paragraph: 'Obviously not affiliated with Apple, but rather a demonstration of a flaw in the way unicode domains in browsers. **It is very possible that your browser isn't affected.**' Below this is another line of text: 'Read the [complete blog post](#) by [Xudong Zheng](#) for more details.'



New unicode domain name phishing attack



Hey there!

Page Info - https://apple.com/

General Permissions Security

Website Identity

Website: **apple.com**

Owner: **This website does not supply ownership information.**

Verified by: **Amazon**

Expires on: **Tuesday, June 26, 2018**

Privacy & History

Have I visited this website prior to today? **No**

Is this website storing information (cookies) on my computer? **Yes**

Have I saved any passwords for this website? **No**

Technical Details

Connection Encrypted (TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256, 128)

The page you are viewing was encrypted before being transmitted over the Internet. Encryption makes it difficult for unauthorized people to view information traveling across computers. It is therefore unlikely that anyone read this page as it traveled across the Internet.

Certificate Viewer: "xn--80ak6aa92e.com"

General Details

This certificate has been verified for the following uses:

- SSL Client Certificate
- SSL Server Certificate

Issued To

Common Name (CN) **xn--80ak6aa92e.com**

Organization (O) <Not Part Of Certificate>

Organizational Unit (OU) <Not Part Of Certificate>

Serial Number 0D:88:D5:69:FA:DA:A1:F4:E1:C6:74:C0:BB:FA:4

Issued By

Common Name (CN) Amazon

Organization (O) Amazon

Organizational Unit (OU) Server CA 1B

Period of Validity

Begins On Thursday, May 25, 2017

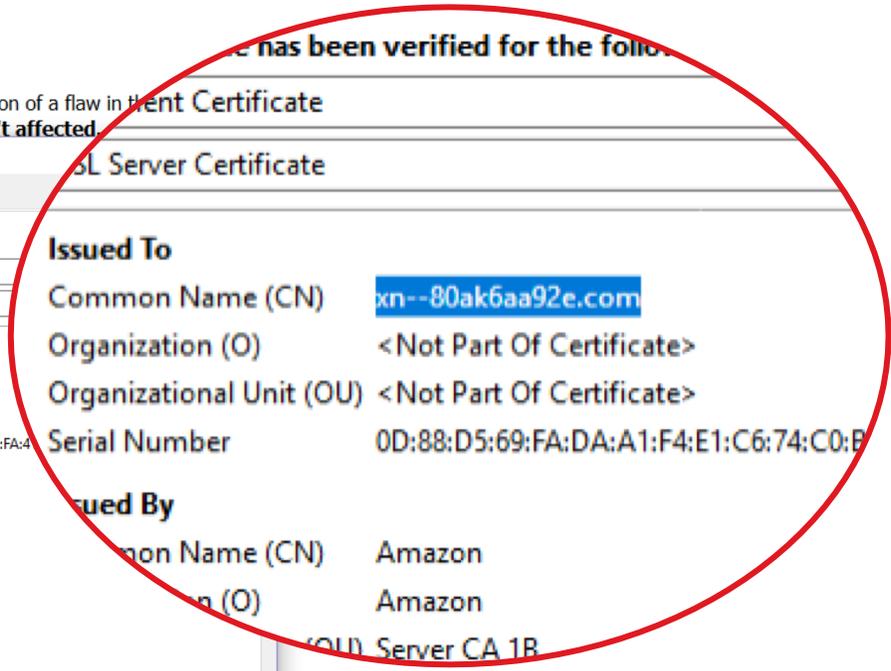
Expires On Tuesday, June 26, 2018

Fingerprints

SHA-256 Fingerprint 1A:8B:59:C0:C9:A1:A7:08:11:4C:C1:AD:9E:E5:FB:AC:4B:52:61:05:48:B5:91:43:B2:22:30:3C:79:C1:8C:C8

SHA1 Fingerprint 67:63:9F:1C:47:CA:2E:01:D7:71:78:A6:82:74:AE:9D:0D:30:DD:C2

Close



The end user...

- Some say the weakest link
- Some say the ultimate problem
- Some say worse than the outside threat
- Some say the last line of defense
- Many are technology consumers but few are skilled in technology



The end user...

- **91%** of successful data breaches started with a spear phishing attack
- **CEO Fraud** (aka Business Email Compromise) causes \$5.3 billion in damages yearly
- **W-2 Scams** social engineer Accounting/HR to send tax forms to the bad guys
- **Ransomware** is a 1 Billion+ dollar criminal business in 2017, and continues to grow exponentially



Cyber Security Myths

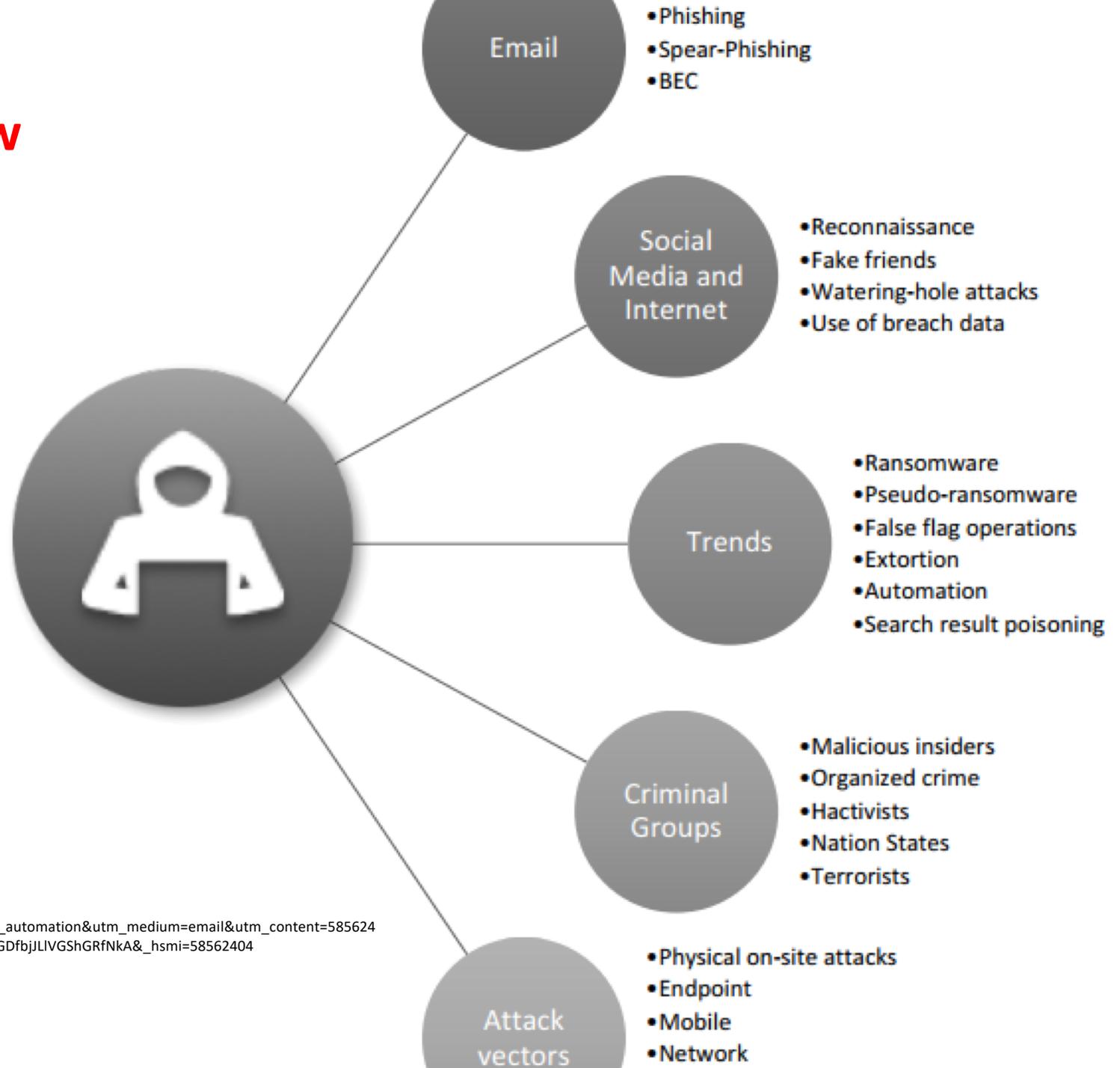


- We have virus software so my computer is protected from everything
- Technology provides full protection
- There's nothing important on my computer
- It's not my job / I'm too busy to worry



What end-users need to know

- Who
- What
- When
- Where
- How



https://www.knowbe4.com/hubfs/PhishingandSocialEngineeringin2018.pdf?t=1513870696549&utm_source=hs_automation&utm_medium=email&utm_content=58562404&_hsenc=p2ANqtz-8Musph_RFNh3JL4_ictXD9GjITNhd3cWYsOEQWIHBeluof36MJ5jjnsbNYICZqGOTy-Y-CyXBNGDfbjLIVGShGRfNkA&_hsmi=58562404



Employers' Primary Cybersecurity Training Methods



Training the end user... the human firewall

1. Prioritize and make your messages and training relevant
2. Test frequently to build secure reflexes
3. Use metrics to reinforce and tell your story
4. Your awareness program operates within the larger context of your organizational culture
5. Think like a marketer, act like an attacker.



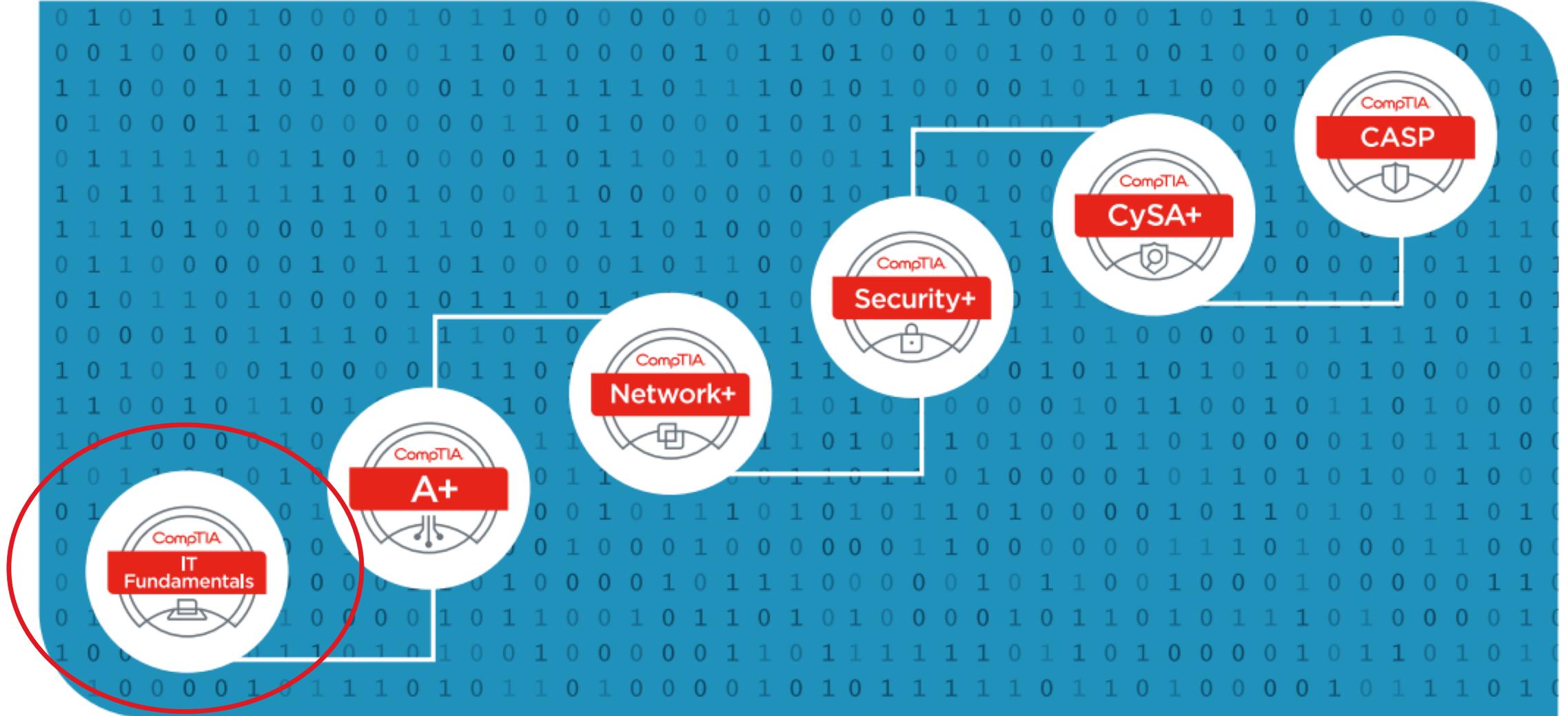
Best practices for end-user training

- Baseline testing
- Train your users
- Phish users
- Analyze data





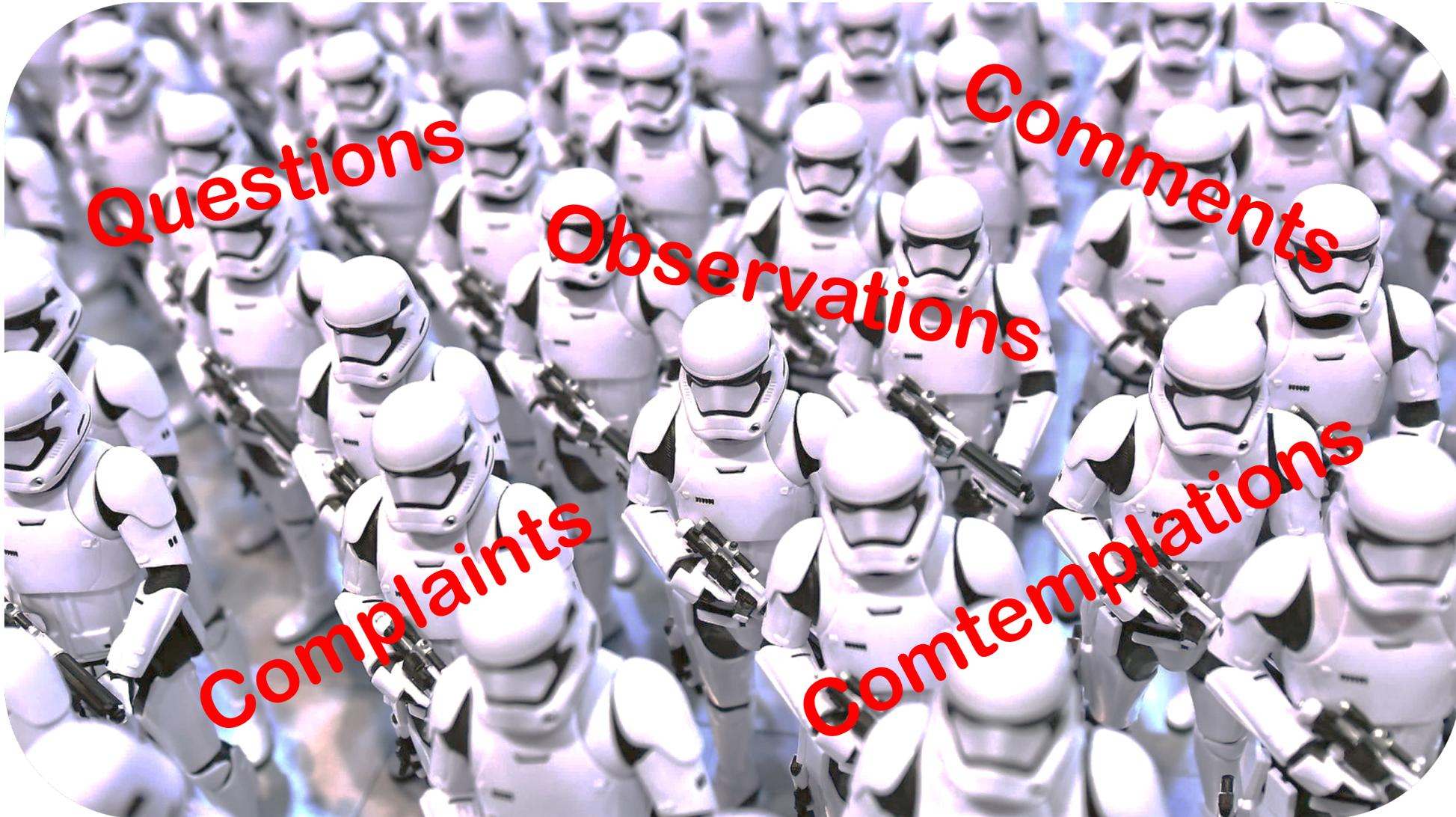
CompTIA Security Pathway



Your Turn ...



CompTIA.
Instructor Network



For more information contact:

CompTIA Instructor Network



Stephen Schneiter
Instructor Network Program
Manager
sschneiter@comptia.org



Tazneen Kasem
Director, Product Development & CIN
CompTIA
tkasem@comptia.org

To join email: CIN@CompTIA.org