Cybersecurity Training for the Enterprise

2018 Rochester Security Summit

Dennis M. Allen

Technical Manager, Cyber Education and Training

CERT/SEI/CMU

I guide an outstanding group of cybersecurity professionals at the Software Engineering Institute that create cutting edge training programs for the federal government and DoD.

Lightning Safety (video)

#1 - “Lightning Safety: Interview with a Cloud” - Produced by LDS Church

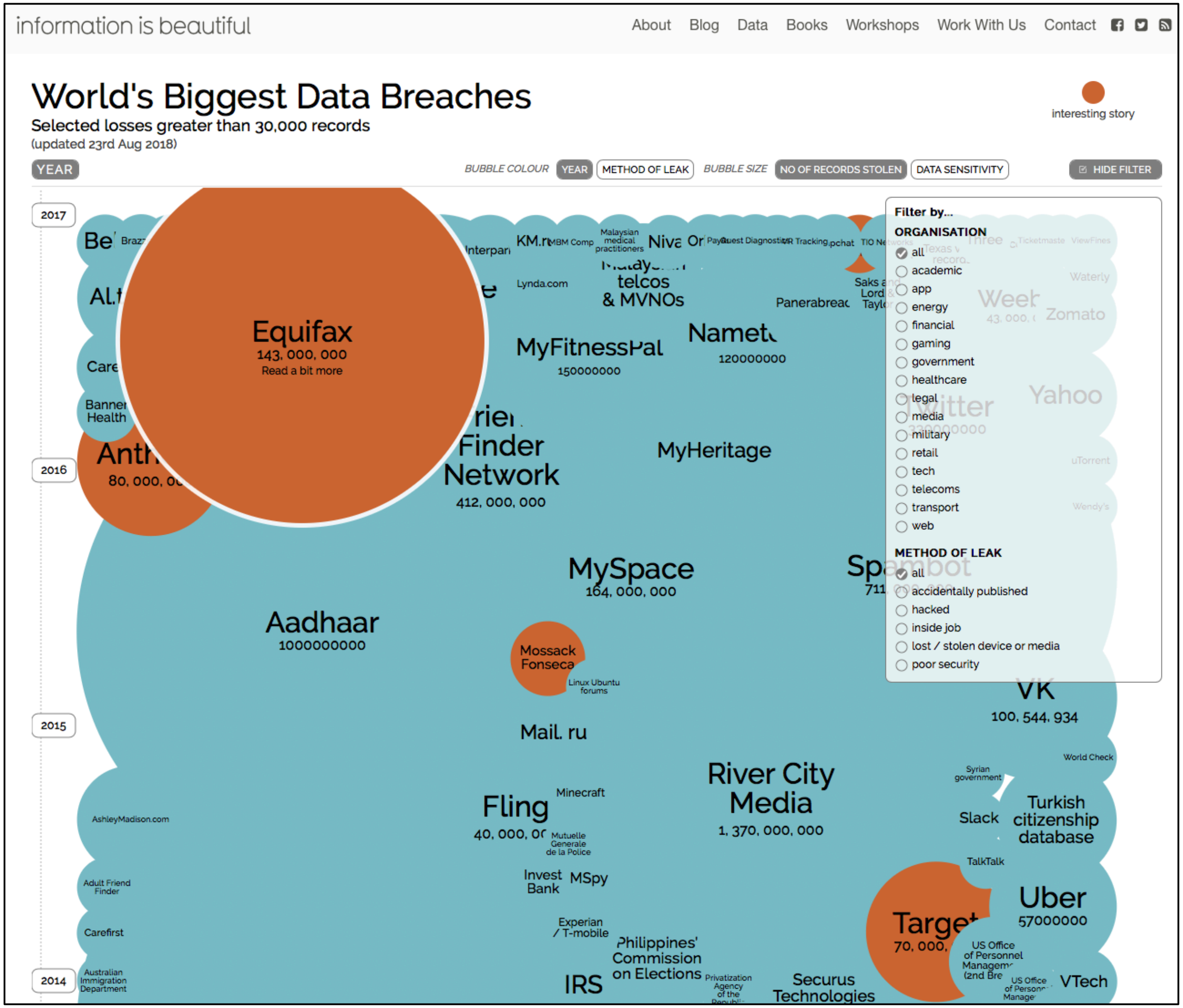
Why show this video?

- Invoke feeling or emotion
  - In this case, humor
- Clear teaching points
  - Still need learning objectives
- Short
  - 2 minutes
- Dynamic
  - Interweaving interview and animations
- Background audio
  - Even background music can stimulate senses and maintain engagement

What did we learn?

- Don’t stand next to metal, poles, or trees
- Don’t run into an open field
- Don’t stand with feet apart
- Do get in the car
- Can strike from 10 miles away

Evolving Cybersecurity Landscape



information is beautiful

About Blog Data Books Workshops Work With Us Contact

World's Biggest Data Breaches

Selected losses greater than 30,000 records

(updated 23rd Aug 2018)

BUBBLE COLOUR [✓ YEAR] METHOD OF LEAK

BUBBLE SIZE [✓ NO OF RECORDS STOLEN] DATA SENSITIVITY

HIDE FILTER

Filter by...

ORGANISATION

- ☑ all
- ○ academic
- ○ app
- ○ energy
- ○ financial
- ○ gaming
- ○ government
- ○ healthcare
- ○ legal
- ○ media
- ○ military
- ○ retail
- ○ tech
- ○ telecoms
- ○ transport
- ○ web

METHOD OF LEAK

- ☑ all
- ○ accidentally published
- ○ hacked
- ○ inside job
- ○ lost / stolen device or media
- ○ poor security

Source: Information is Beautiful - World's Biggest Data Breaches
http://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks

What kind of cybersecurity training?

Key (training) takeaways from the 2018 Verizon Data Breach Investigations Report (VBDIR)

53,000 recorded incidents and 2,216 confir	• Awareness (real threats, you ARE a target)
Use of stolen credentials is the top action v • 43,000 accesses via stolen credentials	• Need multifactor authentication • Need better password practices
Email is the most common attack vector at • 49% of non-POS malware was installed • Phishing and “pretexting” represent 98 • 4% of people will fall victim of a phishin • In a phishing campaign, 1st click average minutes	• Need to protect email • Need Phishing training • Implement proactive benign campaigns (catch and release)
System admin is the top internal threat act	• Insider Threat Training
68% of breaches took months or longer to	• Incident Detection and Handling Training
37% of malware hashes appear only once	• 63% blocked by anti malware?
Ransomware represented 56% of malware	• Implement & verify DR solutions

Popular Learning Models

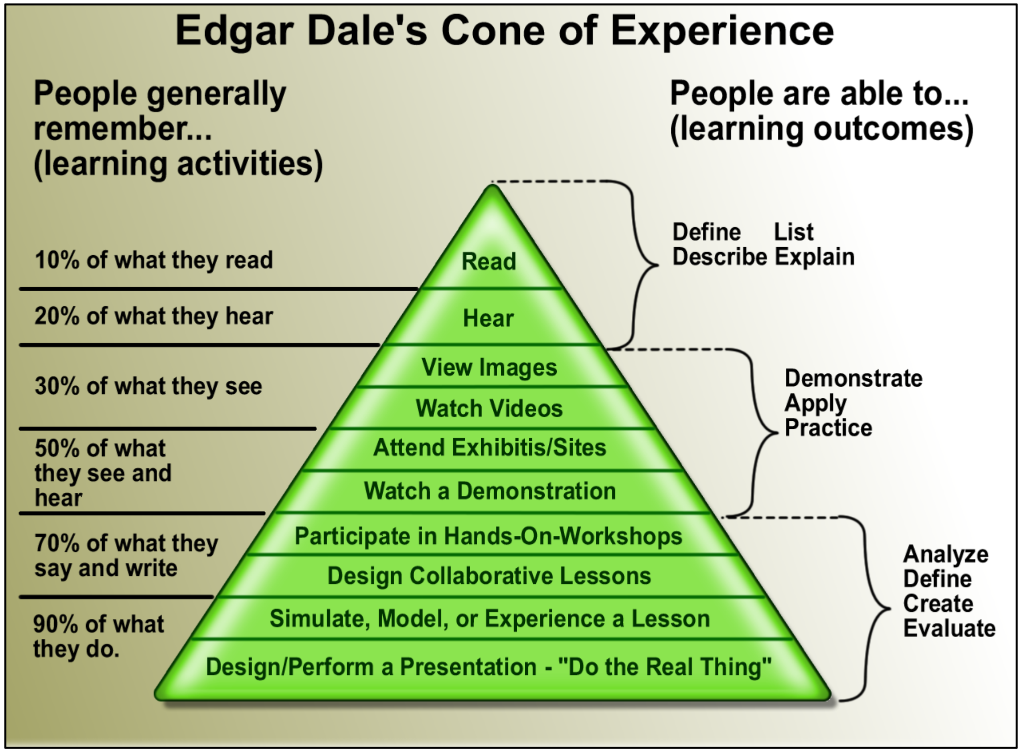

Edgar Dale's Cone of Experience
People generally remember... (learning activities)
People are able to... (learning outcomes)
10% of what they read
20% of what they hear
30% of what they see
50% of what they see and hear
70% of what they say and write
90% of what they do.
Read
Hear
View Images
Watch Videos
Attend Exhibitis/Sites
Watch a Demonstration
Participate in Hands-On-Workshops
Design Collaborative Lessons
Simulate, Model, or Experience a Lesson
Design/Perform a Presentation - "Do the Real Thing"
Define List
Describe Explain
Demonstrate
Apply
Practice
Analyze
Define
Create
Evaluate

Image Source: https://en.wikipedia.org/wiki/File:Cone_of_learning_export_11x17.png

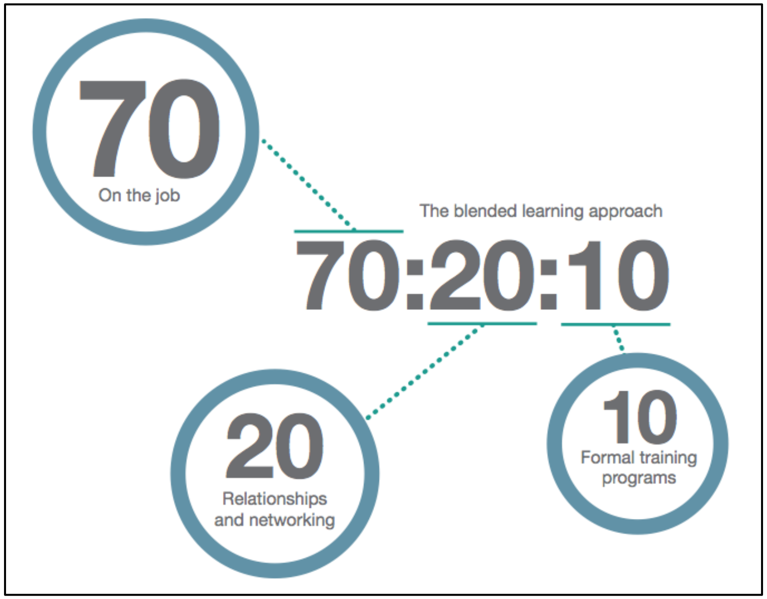


Image Source: https://publicsector.wa.gov.au/workforce/leadership/leading-regions/blended-learning

Instructor Led Training (ILT)

Similar Tools/Terms

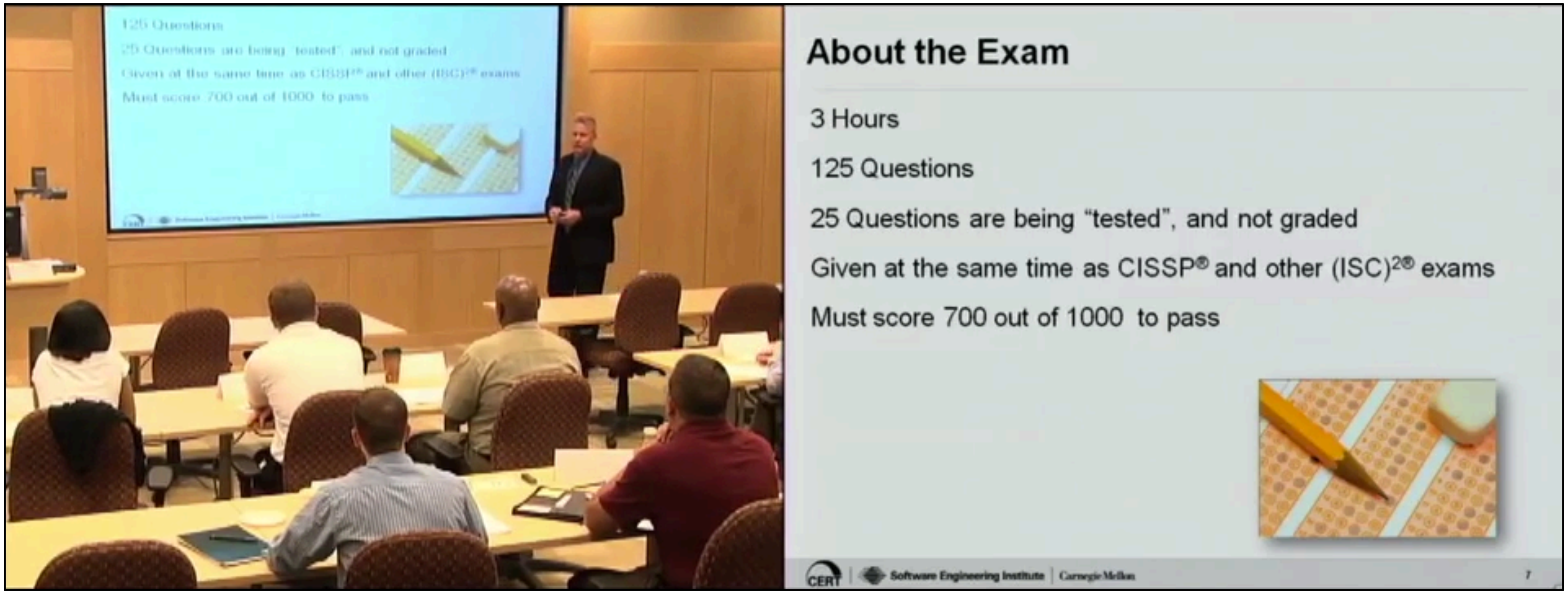
- Classroom Training
- Traditional Training

Use Cases

- "Sage on the stage"
- Team building
- Certification Preparation
- Often combined with hands-on

Advantages/Disadvantages

- Can "tweak" per delivery but generally long development cycles
- 20-80 hours of dev. per 1 hr of delivery
- Course availability challenges
- Travel and other expenses
- 70:20:10



About the Exam

3 Hours

125 Questions

25 Questions are being "tested", and not graded

Given at the same time as CISSP® and other (ISC)²® exams

Must score 700 out of 1000 to pass

Computer Based Training (CBT)

Similar Tools/Terms

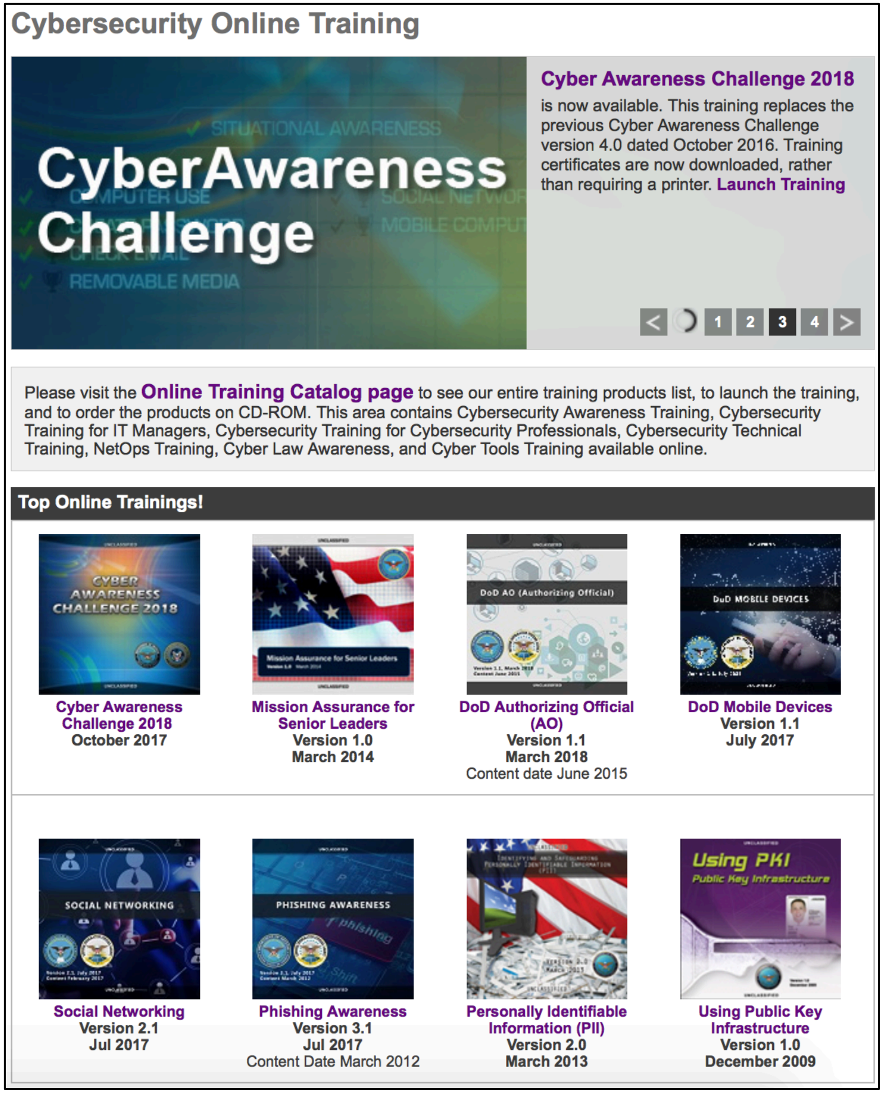
- Web Based Training (WBT)
- eLearning

Use Cases

- “Guy on the side” (e.g. YouTube)
- Awareness/Knowledge building
- Limited Skill development
- Certification preparation

Advantages/Disadvantages

- Self-paced
- Numerous distribution methods
- Automated completion tracking
- Varied cost models
  - 50-300 hours of dev. per 1 hr of delivery
- Consistent delivery
- 70:20:10



Cybersecurity Online Training

Cyber Awareness Challenge 2018
is now available. This training replaces the previous Cyber Awareness Challenge version 4.0 dated October 2016. Training certificates are now downloaded, rather than requiring a printer. **Launch Training**

Please visit the **Online Training Catalog page** to see our entire training products list, to launch the training, and to order the products on CD-ROM. This area contains Cybersecurity Awareness Training, Cybersecurity Training for IT Managers, Cybersecurity Training for Cybersecurity Professionals, Cybersecurity Technical Training, NetOps Training, Cyber Law Awareness, and Cyber Tools Training available online.

Top Online Trainings!

Cyber Awareness Challenge 2018
October 2017

Mission Assurance for Senior Leaders
Version 1.0
March 2014

DoD Authorizing Official (AO)
Version 1.1
March 2018
Content date June 2015

DoD Mobile Devices
Version 1.1
July 2017

Social Networking
Version 2.1
Jul 2017

Phishing Awareness
Version 3.1
Jul 2017
Content Date March 2012

Personally Identifiable Information (PII)
Version 2.0
March 2013

Using Public Key Infrastructure
Version 1.0
December 2009

CYBER AWARENESS CHALLENGE 2018
Mission Assurance for Senior Leaders
DoD AO (Authorizing Official)
DoD MOBILE DEVICES
SOCIAL NETWORKING
PHISHING AWARENESS
Using PKI
Public Key Infrastructure

https://iase.disa.mil/eta/Pages/index.aspx

Game Based Learning (GBL)

Similar Tools/Terms

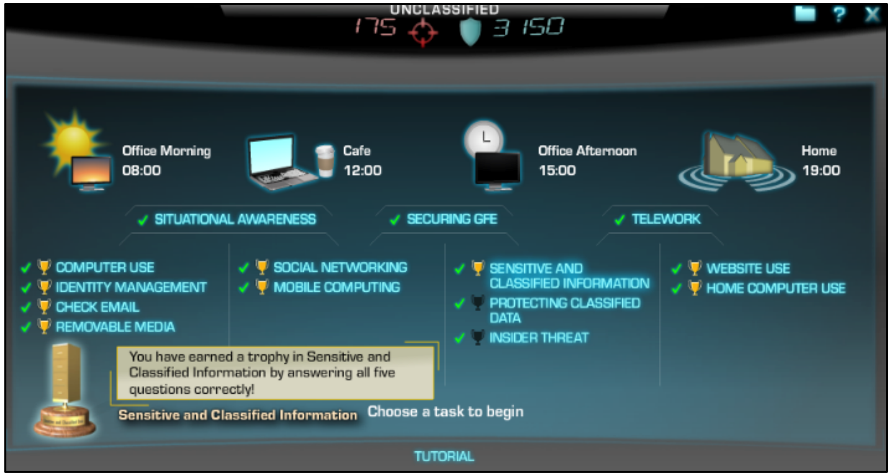
- NOT just “gamification”

Use Cases

- Any

Advantages/Disadvantages

- Fun, Different, and Engaging
- Consistent but Dynamic
- Self-paced
- Costly to develop
  - 300+ hours of dev. per 1 hr of delivery*
- 70:**20**:**10**



Office Morning 08:00 | Cafe 12:00 | Office Afternoon 15:00 | Home 19:00

✓ SITUATIONAL AWARENESS
✓ COMPUTER USE
✓ IDENTITY MANAGEMENT
✓ CHECK EMAIL
✓ REMOVABLE MEDIA

✓ SECURING GFE
✓ SOCIAL NETWORKING
✓ MOBILE COMPUTING
✓ SENSITIVE AND CLASSIFIED INFORMATION
✓ PROTECTING CLASSIFIED DATA
✓ INSIDER THREAT

✓ TELEWORK
✓ WEBSITE USE
✓ HOME COMPUTER USE

You have earned a trophy in Sensitive and Classified Information by answering all five questions correctly!

Sensitive and Classified Information

Choose a task to begin

https://iatraining.disa.mil/eta/disa_cac2018/launchPage.htm

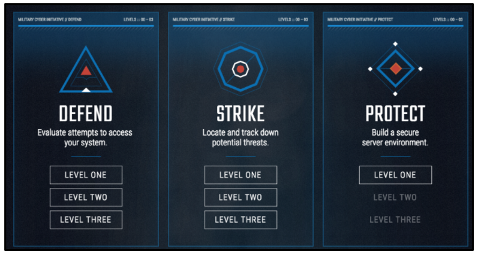
An educational game brought to you by Trend Micro

Copyright © 2015 Trend Micro Incorporated. All rights reserved.

This is for entertainment purposes only.

http://targetedattacks.trendmicro.com/

http://my.nps.edu/web/c3o/cyberciege


MILITARY CYBER INITIATIVE // DEFEND
LEVELS :: 00 - 03
MILITARY CYBER INITIATIVE // STRIKE
LEVELS :: 00 - 03
MILITARY CYBER INITIATIVE // PROTECT
LEVELS :: 00 - 03

DEFEND
Evaluate attempts to access your system.
LEVEL ONE
LEVEL TWO
LEVEL THREE

STRIKE
Locate and track down potential threats.
LEVEL ONE
LEVEL TWO
LEVEL THREE

PROTECT
Build a secure server environment.
LEVEL ONE
LEVEL TWO
LEVEL THREE

https://www.cybermission.tech/

* http://www.chapmanalliance.com/howlong/

Training Exercises

Similar Tools/Terms

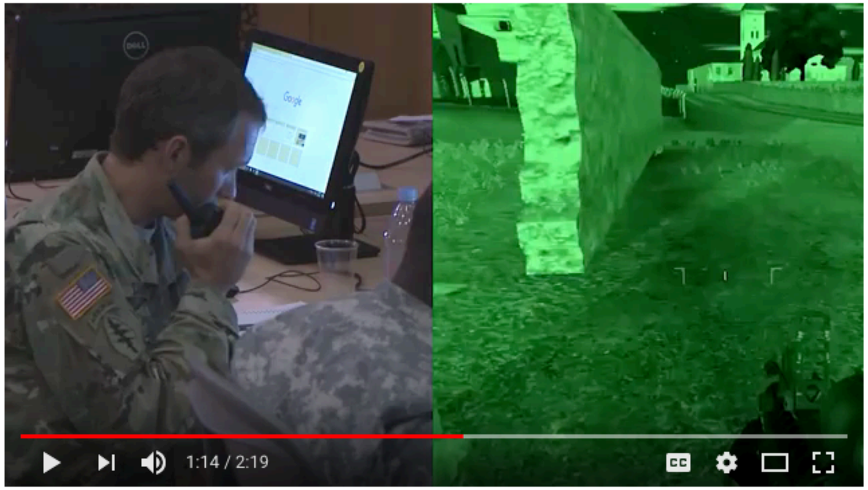
- Simulations
- Dress Rehearsal

Use Cases

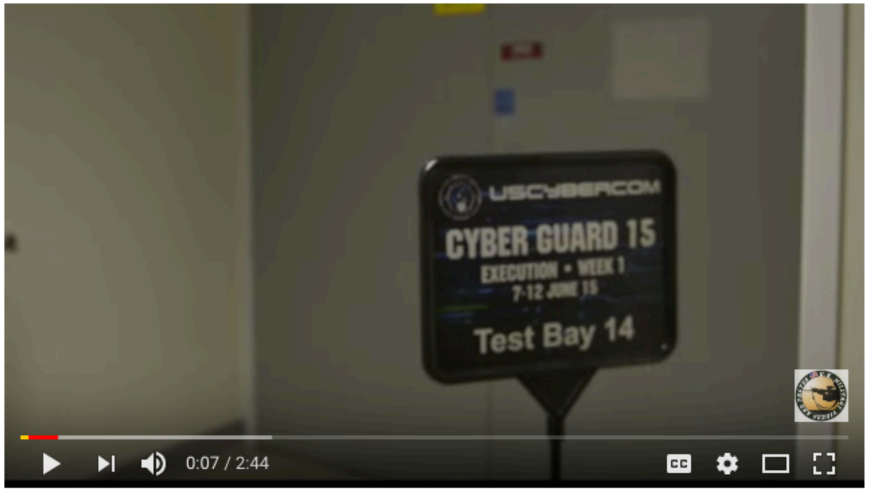
- Advanced Skill Development
- Experience Building
- Readiness Assessment
- Tabletop Exercises

Advantages/Disadvantages

- Training or Assessment?
- Can be expensive to setup
- Difficult to coordinate participants
- Superior evaluation of Procedures, and Command & Control
- 70:20:10

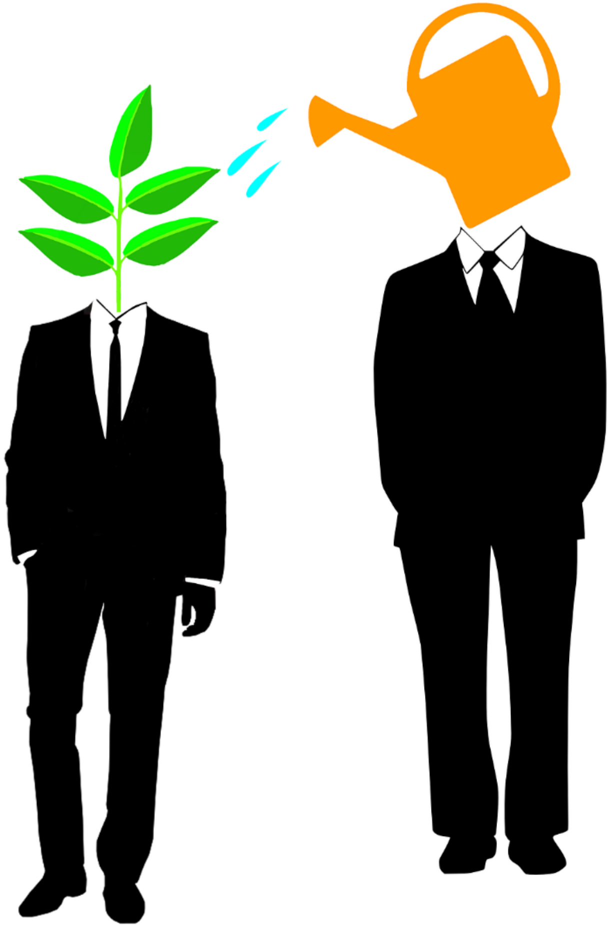


Cyber X Games 2017



Cyber Guard 15

On the Job Training (OJT)



Similar Tools/Terms

- Learn by doing
- Job Instruction Training (JIT)

Use Cases

- Onboarding
- Apprenticeship/Internship
- Job Rotation
- Mentoring

Advantages/Disadvantages

- Requires active supervision
- Dependent on knowledge, skills, and expertise of SME
- Inconsistent training environment
- What is your mistake tolerance?
- 70:20:10

Every Day Learning (EDL)

Similar Tools/Terms

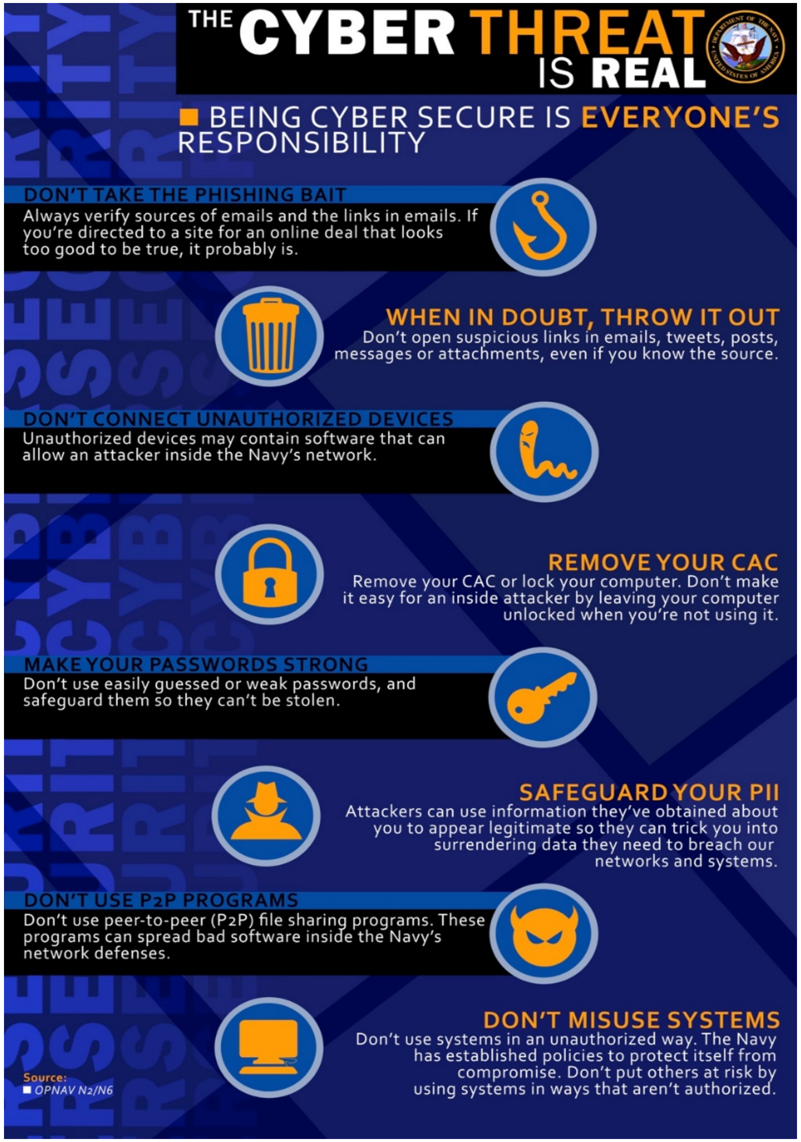
- Active Training

Use Cases

- Penetration Testing & Red Teaming
- Benign Spear Phishing campaigns
- OPSEC Posters

Advantages/Disadvantages

- Defining success metrics can be difficult
- Apply a consistent standard
- Provide timely after action reviews, lessons learned, remedial training, and/or rewards
- **70**:20:10



THE CYBER THREAT IS REAL

BEING CYBER SECURE IS EVERYONE'S RESPONSIBILITY

DON'T TAKE THE PHISHING BAIT
Always verify sources of emails and the links in emails. If you're directed to a site for an online deal that looks too good to be true, it probably is.

WHEN IN DOUBT, THROW IT OUT
Don't open suspicious links in emails, tweets, posts, messages or attachments, even if you know the source.

DON'T CONNECT UNAUTHORIZED DEVICES
Unauthorized devices may contain software that can allow an attacker inside the Navy's network.

REMOVE YOUR CAC
Remove your CAC or lock your computer. Don't make it easy for an inside attacker by leaving your computer unlocked when you're not using it.

MAKE YOUR PASSWORDS STRONG
Don't use easily guessed or weak passwords, and safeguard them so they can't be stolen.

SAFEGUARD YOUR PII
Attackers can use information they've obtained about you to appear legitimate so they can trick you into surrendering data they need to breach our networks and systems.

DON'T USE P2P PROGRAMS
Don't use peer-to-peer (P2P) file sharing programs. These programs can spread bad software inside the Navy's network defenses.

DON'T MISUSE SYSTEMS
Don't use systems in an unauthorized way. The Navy has established policies to protect itself from compromise. Don't put others at risk by using systems in ways that aren't authorized.

Source:
OPNAV N2/N6

Image Source: http://navylive.dodlive.mil/2017/10/12/navy-cybersecurity-anatomy-of-a-cyber-intrusion

The National Initiative for Cybersecurity Education Cybersecurity Workforce Framework

NIST Special Publication 800-181

FRAMEWORK

This publication serves as a fundamental reference to support a workforce capable of meeting an organization's cybersecurity needs. The NICE Framework supports consistent organizational and sector communication for cybersecurity education, training, and workforce development.

DEVELOPMENT PROCESS

The National Initiative for Cybersecurity Education (NICE) Framework improves communication about how to identify, recruit, develop, and retain cybersecurity talent. It is a resource from which organizations or sectors can develop additional publications or tools that meet their needs to define or provide guidance on different aspects of workforce development, planning, training, and education.

1. **Collected and analyzed reference materials (reports, briefings, job task analyses, etc.) from across the government related to workforce constructs.**

   Some of the reviewed resources include: Office of Personnel Management's occupational standards (OPM, 2010), Job descriptions from the Department of Labor's O*NET database (2010), DoD 8570.01-M Information Assurance Workforce Improvement Program (DoD, 2010), DoD Cyber Workforce Framework, Joint Cyberspace Training and Education Standards (JCT&CS), DoD Counterintelligence in Cyberspace Training and Professional Development Plan, Federal Cybersecurity Workforce Transformation Working Group Report on Cybersecurity Competencies

2. **Refined existing definitions of cybersecurity specialty areas based on collected information**

3. **Conducted focus groups with subject matter experts (SMEs) to identify and define specialty areas not noted in previous versions of the Framework (e.g., Cybersecurity Management and Language Analysis)**

4. **Conducted focus groups to shape category, specialty area, and work role definitions and align and review tasks and KSAs for each work role**

5. **Identified, collected, and wrote new tasks and KSAs, where appropriate**

6. **Refined Framework as necessary through workshops, meetings, and stakeholder input (ongoing)**

CYBERSECURITY WORK CATEGORIES

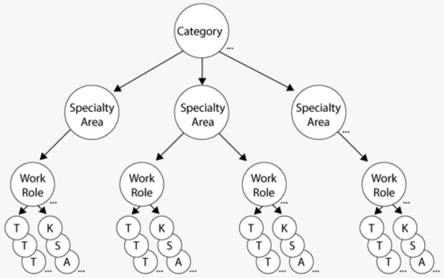
OVERSEE AND GOVERN	OPERATE AND MAINTAIN	INVESTIGATE	COLLECT AND OPERATE	ANALYZE	SECURELY PROVISION	PROTECT AND DEFEND

NICE
NATIONAL INITIATIVE FOR CYBERSECURITY EDUCATION

CONTACT:
nist.gov/nice/framework
NICEframework@nist.gov

WHAT IS THE CYBERSECURITY WORKFORCE?

A workforce with work roles that have an impact on an organization's ability to protect its data, systems, and operations.



CATEGORIES: A high-level grouping of common cybersecurity functions

SPECIALTY AREAS: Represent an area of concentrated work, or function, within cybersecurity and related work

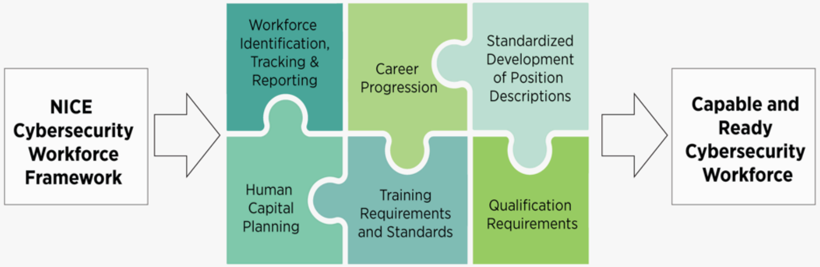
WORK ROLES: The most detailed groupings of cybersecurity and related work, which include a list of attributes required to perform that role in the form of a list of knowledge, skills, and abilities (KSAs) and a list of tasks performed in that role

TASKS: Specific work activities that could be assigned to an individual working in one of the NICE Framework's Work Roles

KSAs: Attributes required to perform Tasks, generally demonstrated through relevant experience or performance-based education and training

BUILDING BLOCKS FOR A CAPABLE AND READY CYBERSECURITY WORKFORCE

The NICE Framework provides employers, current and future cybersecurity workers, training and certification providers, education providers, and technology providers with a national standard for organizing the way we define and talk about cybersecurity work, and what is required to do that work.



NICE Cybersecurity Workforce Framework

Workforce Identification, Tracking & Reporting

Career Progression

Standardized Development of Position Descriptions

Human Capital Planning

Training Requirements and Standards

Qualification Requirements

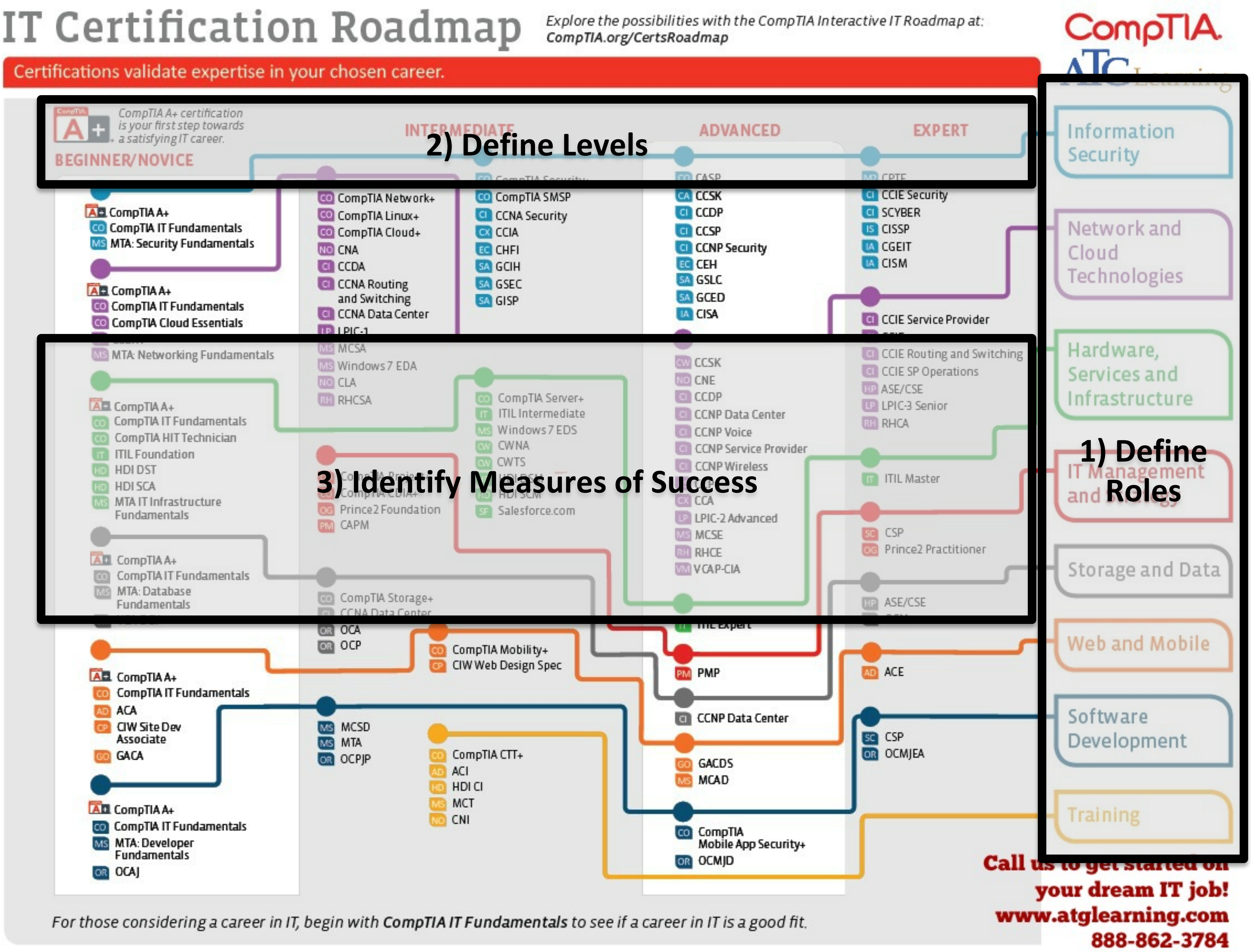
Capable and Ready Cybersecurity Workforce

NIST National Institute of Standards and Technology U.S. Department of Commerce

‘Sample’ NICE Roles

https://niccs.us-cert.gov/nice-cybersecurity-workforce-framework-work-roles

Category (7)	Specialty Are (33)	Work Role (52)
Securely Provision	Risk Management	Authorizing Official
		Security Control Assessor
	Systems Architecture	Enterprise Architect
		Security Architect
Operate and Maintain	Database Administration	Database Administrator
		Data Analyst
	Network Services	Network Operations Specialist
	Systems Administration	System Administrator
Oversee and Govern	Executive Cyber Leadership	Executive Cyber Leadership
	Acquisition and Program/ Project Management	Program Manager
		IT Project Manager



IT Certification Roadmap

Explore the possibilities with the CompTIA Interactive IT Roadmap at: ***CompTIA.org/CertsRoadmap***

CompTIA

ATG Learning

Certifications validate expertise in your chosen career.

CompTIA A+ certification is your first step towards a satisfying IT career.

2) Define Levels

BEGINNER/NOVICE

INTERMEDIATE

ADVANCED

EXPERT

1) Define Roles

Information Security

Network and Cloud Technologies

Hardware, Services and Infrastructure

IT Management and Strategy

Storage and Data

Web and Mobile

Software Development

Training

3) Identify Measures of Success

Beginner/Novice:

- CompTIA A+
- CompTIA IT Fundamentals
- MTA: Security Fundamentals

- CompTIA A+
- CompTIA IT Fundamentals
- CompTIA Cloud Essentials
- MTA: Networking Fundamentals

- CompTIA A+
- CompTIA IT Fundamentals
- CompTIA HIT Technician
- ITIL Foundation
- HDI DST
- HDI SCA
- MTA IT Infrastructure Fundamentals

- CompTIA A+
- CompTIA IT Fundamentals
- MTA: Database Fundamentals

- CompTIA A+
- CompTIA IT Fundamentals
- ACA
- CIW Site Dev Associate
- GACA

- CompTIA A+
- CompTIA IT Fundamentals
- MTA: Developer Fundamentals
- OCAJ

Intermediate:

- CompTIA Network+
- CompTIA Linux+
- CompTIA Cloud+
- CNA
- CCDA
- CCNA Routing and Switching
- CCNA Data Center
- LPIC-1
- MCSA
- Windows 7 EDA
- CLA
- RHCSA

- CompTIA Security+
- CompTIA SMSP
- CCNA Security
- CCIA
- CHFI
- GCIH
- GSEC
- GISP

- CompTIA Server+
- ITIL Intermediate
- Windows 7 EDS
- CWNA
- CWTS
- HDI DSM
- HDI SCM
- Salesforce.com

- CompTIA Project+
- CompTIA CDIA+
- Prince2 Foundation
- CAPM

- CompTIA Storage+
- CCNA Data Center
- OCA
- OCP

- CompTIA Mobility+
- CIW Web Design Spec

- MCSD
- MTA
- OCPJP

- CompTIA CTT+
- ACI
- HDI CI
- MCT
- CNI

Advanced:

- CASP
- CCSK
- CCDP
- CCSP
- CCNP Security
- CEH
- GSLC
- GCED
- CISA

- CCSK
- CNE
- CCDP
- CCNP Data Center
- CCNP Voice
- CCNP Service Provider
- CCNP Wireless
- CCA
- LPIC-2 Advanced
- MCSE
- RHCE
- VCAP-CIA

- ITIL Expert

- PMP

- CCNP Data Center

- GACDS
- MCAD

- CompTIA Mobile App Security+
- OCMJD

Expert:

- CPTE
- CCIE Security
- SCYBER
- CISSP
- CGEIT
- CISM

- CCIE Service Provider
- CCIE Routing and Switching
- CCIE SP Operations
- ASE/CSE
- LPIC-3 Senior
- RHCA

- ITIL Master

- CSP
- Prince2 Practitioner

- ASE/CSE

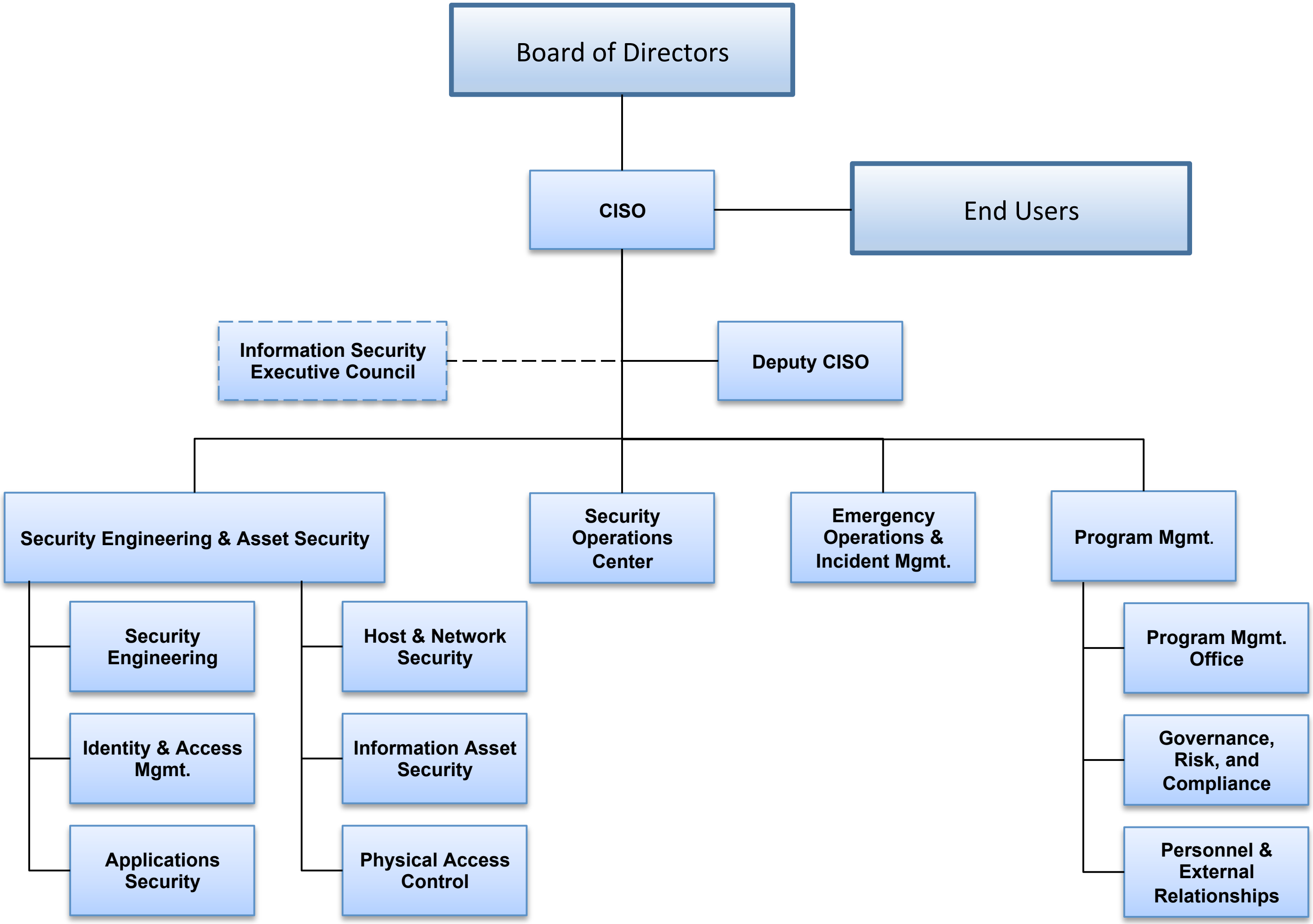
- ACE

- CSP
- OCMJEA

For those considering a career in IT, begin with ***CompTIA IT Fundamentals*** *to see if a career in IT is a good fit.*

Call us to get started on your dream IT job!
www.atglearning.com
888-862-3784

Example Security Organization


Board of Directors
CISO
End Users
Information Security Executive Council
Deputy CISO
Security Engineering & Asset Security
Security Operations Center
Emergency Operations & Incident Mgmt.
Program Mgmt.
Security Engineering
Identity & Access Mgmt.
Applications Security
Host & Network Security
Information Asset Security
Physical Access Control
Program Mgmt. Office
Governance, Risk, and Compliance
Personnel & External Relationships

Source: Structuring the CISO Organization
https://resources.sei.cmu.edu/asset_files/TechnicalNote/2015_004_001_446198.pdf

Training by Target Group

Training is most effective when it is targeted to a particular group (WIIFM)

<table>
<tr><td>Board of Directors, & C-Suite</td><td>• Spear phishing/ whaling</td><td rowspan="3">• Formal Education
• Internal Org & Ops
• Risk Management
• Crisis Communications
• Industry Compliance</td><td rowspan="5">• <b>Professional Associations</b>

• Informal Training (e.g. Podcasts)</td><td rowspan="6">• Securing mobile

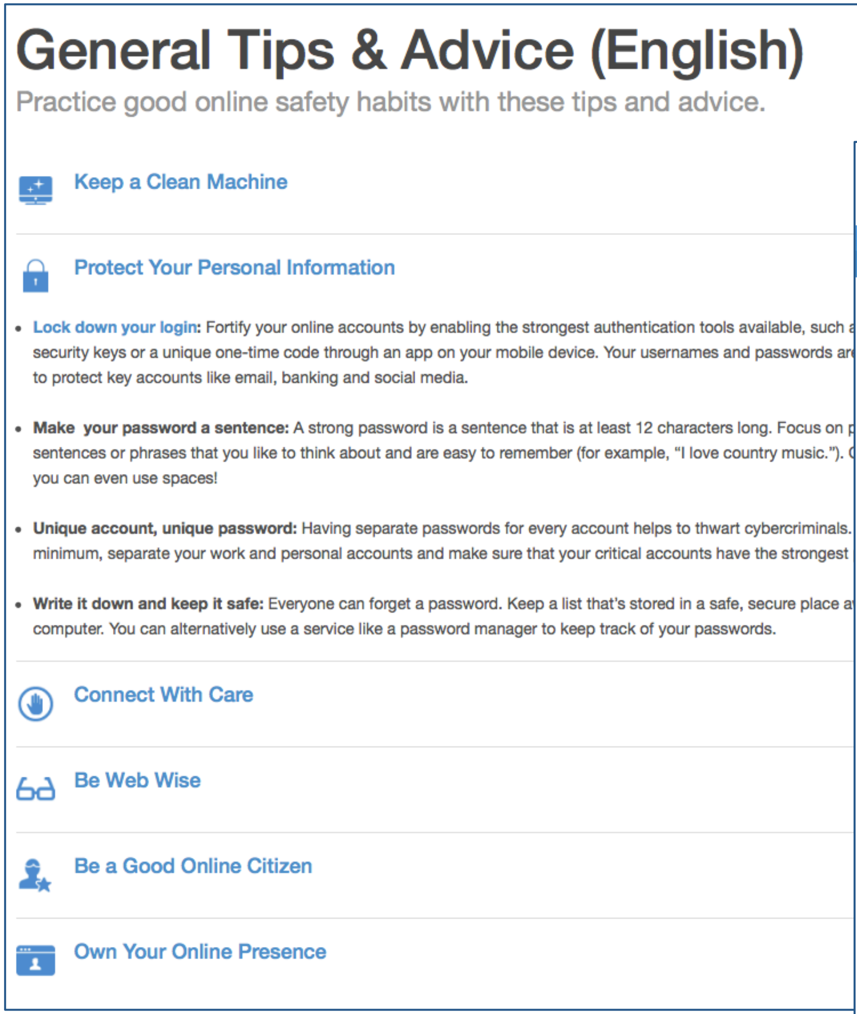
• Acceptable use

• IA Awareness

• Phishing Awareness

• Social Engineering</td></tr>
<tr><td rowspan="2">Senior Leaders & Managers</td><td>• Leadership
• Project mgmt</td></tr>
<tr><td rowspan="2">• Industry certs
• Best practices
• Insider threat</td></tr>
<tr><td rowspan="2">Administrators/ Developers</td><td rowspan="2">• Auth & Access
• Vuln & Patch mgmt
• Configuration mgmt
• Change mgmt
• Tools & OS
• Conferences/Workshops</td></tr>
<tr><td></td></tr>
<tr><td>End Users</td><td></td><td></td><td></td></tr>
</table>

STOPTHINKCONNECT.ORG



General Tips & Advice (English)

Practice good online safety habits with these tips and advice.

Keep a Clean Machine

Protect Your Personal Information

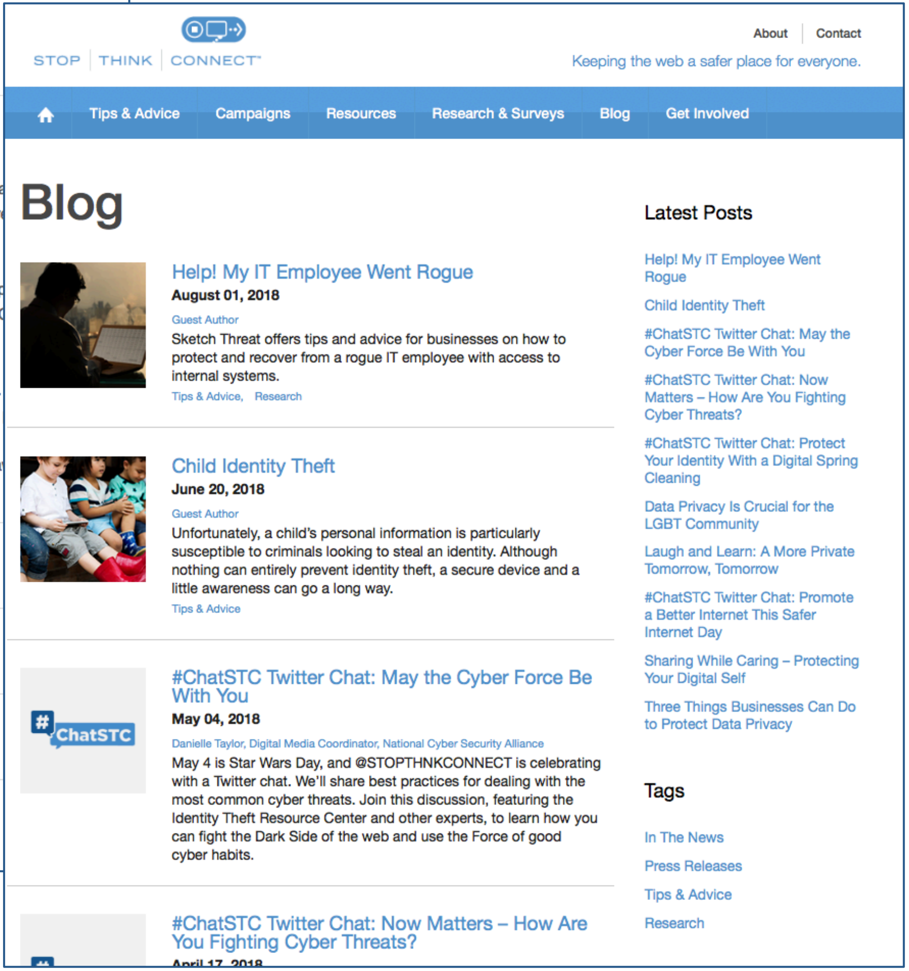
- **Lock down your login:** Fortify your online accounts by enabling the strongest authentication tools available, such a security keys or a unique one-time code through an app on your mobile device. Your usernames and passwords are to protect key accounts like email, banking and social media.
- **Make your password a sentence:** A strong password is a sentence that is at least 12 characters long. Focus on p sentences or phrases that you like to think about and are easy to remember (for example, "I love country music."). O you can even use spaces!
- **Unique account, unique password:** Having separate passwords for every account helps to thwart cybercriminals. minimum, separate your work and personal accounts and make sure that your critical accounts have the strongest
- **Write it down and keep it safe:** Everyone can forget a password. Keep a list that's stored in a safe, secure place a computer. You can alternatively use a service like a password manager to keep track of your passwords.

Connect With Care

Be Web Wise

Be a Good Online Citizen

Own Your Online Presence



STOP | THINK | CONNECT™

About | Contact

Keeping the web a safer place for everyone.

Tips & Advice | Campaigns | Resources | Research & Surveys | Blog | Get Involved

Blog

Help! My IT Employee Went Rogue

August 01, 2018

Guest Author

Sketch Threat offers tips and advice for businesses on how to protect and recover from a rogue IT employee with access to internal systems.

Tips & Advice, Research

Child Identity Theft

June 20, 2018

Guest Author

Unfortunately, a child's personal information is particularly susceptible to criminals looking to steal an identity. Although nothing can entirely prevent identity theft, a secure device and a little awareness can go a long way.

Tips & Advice

#ChatSTC Twitter Chat: May the Cyber Force Be With You

May 04, 2018

Danielle Taylor, Digital Media Coordinator, National Cyber Security Alliance

May 4 is Star Wars Day, and @STOPTHNKCONNECT is celebrating with a Twitter chat. We'll share best practices for dealing with the most common cyber threats. Join this discussion, featuring the Identity Theft Resource Center and other experts, to learn how you can fight the Dark Side of the web and use the Force of good cyber habits.

#ChatSTC Twitter Chat: Now Matters – How Are You Fighting Cyber Threats?

April 17, 2018

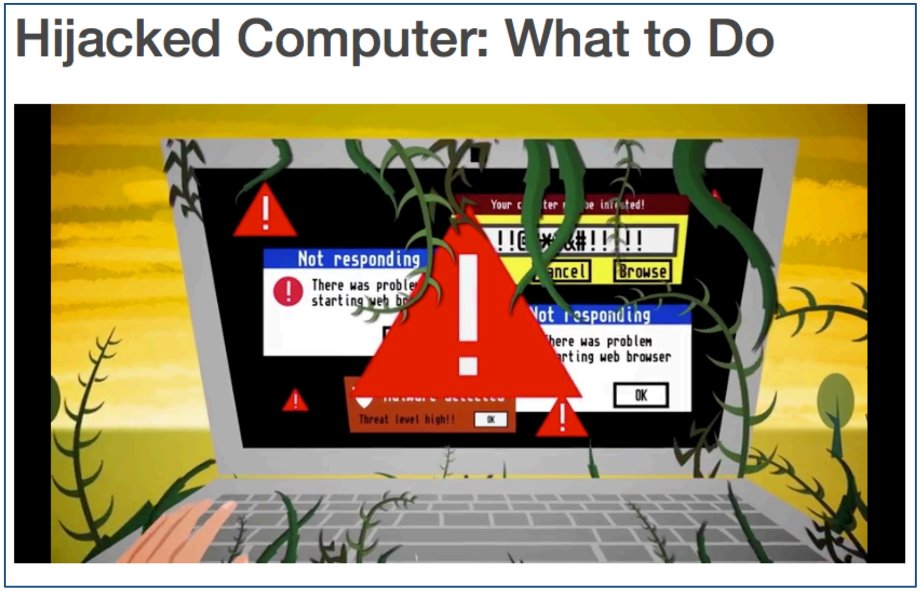
Latest Posts

- Help! My IT Employee Went Rogue
- Child Identity Theft
- #ChatSTC Twitter Chat: May the Cyber Force Be With You
- #ChatSTC Twitter Chat: Now Matters – How Are You Fighting Cyber Threats?
- #ChatSTC Twitter Chat: Protect Your Identity With a Digital Spring Cleaning
- Data Privacy Is Crucial for the LGBT Community
- Laugh and Learn: A More Private Tomorrow, Tomorrow
- #ChatSTC Twitter Chat: Promote a Better Internet This Safer Internet Day
- Sharing While Caring – Protecting Your Digital Self
- Three Things Businesses Can Do to Protect Data Privacy

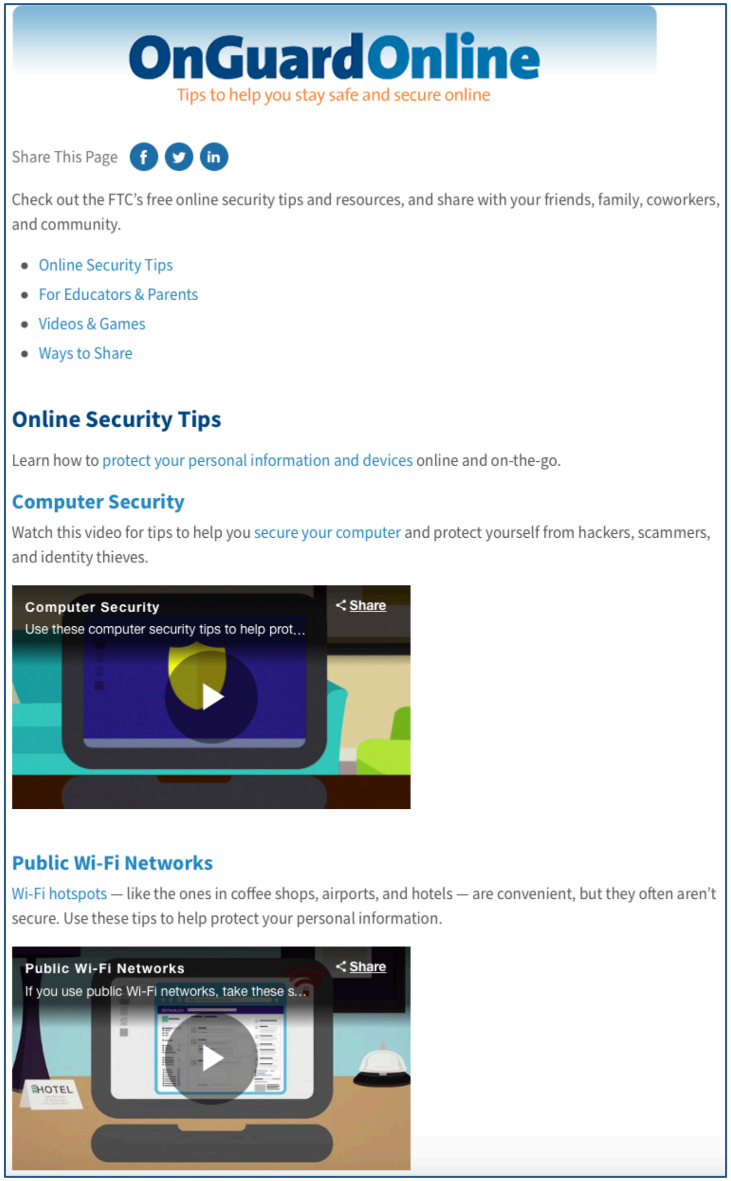
Tags

- In The News
- Press Releases
- Tips & Advice
- Research

ONGUARDONLINE.GOV



Hijacked Computer: What to Do



OnGuardOnline

Tips to help you stay safe and secure online

Share This Page

Check out the FTC's free online security tips and resources, and share with your friends, family, coworkers, and community.

- Online Security Tips
- For Educators & Parents
- Videos & Games
- Ways to Share

Online Security Tips

Learn how to protect your personal information and devices online and on-the-go.

Computer Security

Watch this video for tips to help you secure your computer and protect yourself from hackers, scammers, and identity thieves.

Computer Security

Use these computer security tips to help prot…

Share

Public Wi-Fi Networks

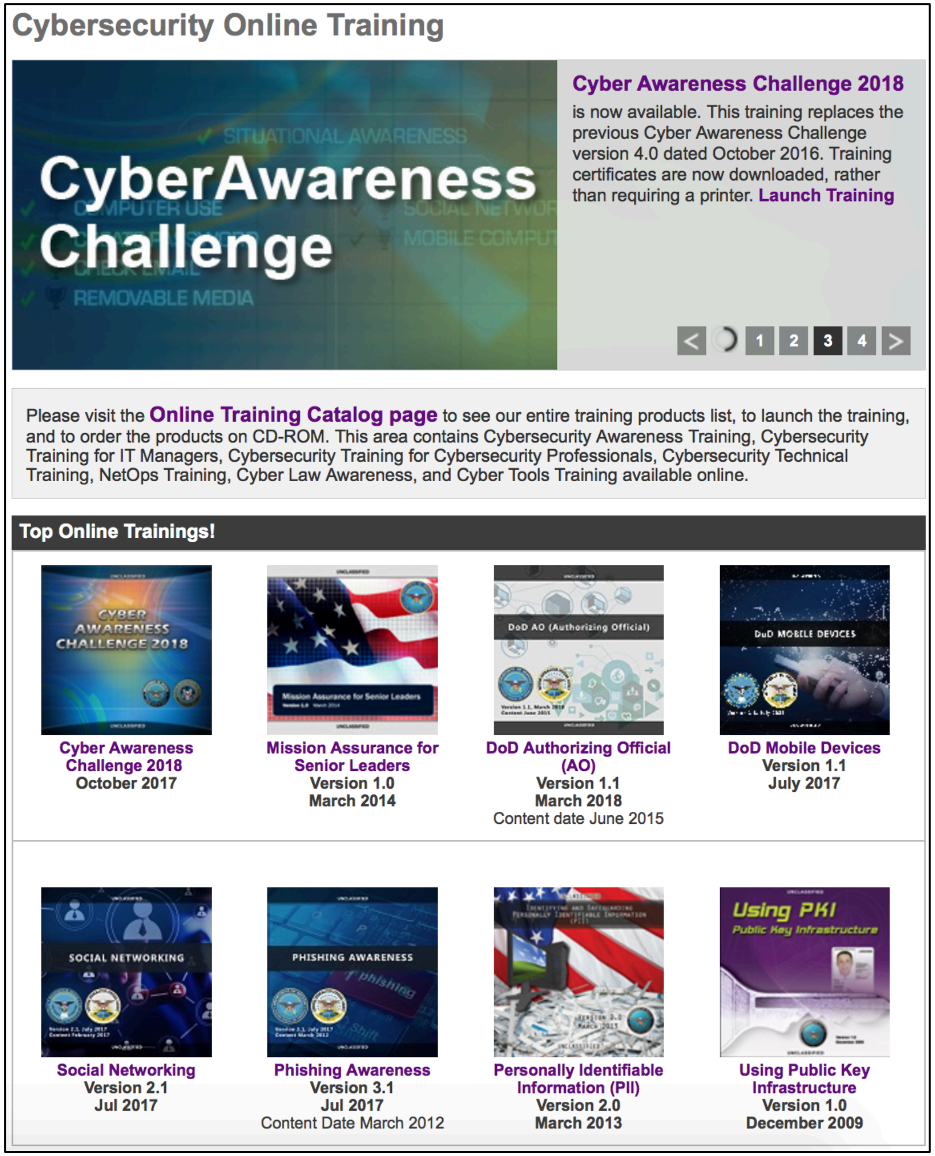
Wi-Fi hotspots — like the ones in coffee shops, airports, and hotels — are convenient, but they often aren't secure. Use these tips to help protect your personal information.

Public Wi-Fi Networks

If you use public Wi-Fi networks, take these s…

Share

ISASE.DISA.MIL



Cybersecurity Online Training

Cyber Awareness Challenge 2018 is now available. This training replaces the previous Cyber Awareness Challenge version 4.0 dated October 2016. Training certificates are now downloaded, rather than requiring a printer. **Launch Training**

Please visit the **Online Training Catalog page** to see our entire training products list, to launch the training, and to order the products on CD-ROM. This area contains Cybersecurity Awareness Training, Cybersecurity Training for IT Managers, Cybersecurity Training for Cybersecurity Professionals, Cybersecurity Technical Training, NetOps Training, Cyber Law Awareness, and Cyber Tools Training available online.

Top Online Trainings!

Cyber Awareness Challenge 2018
October 2017

Mission Assurance for Senior Leaders
Version 1.0
March 2014

DoD Authorizing Official (AO)
Version 1.1
March 2018
Content date June 2015

DoD Mobile Devices
Version 1.1
July 2017

Social Networking
Version 2.1
Jul 2017

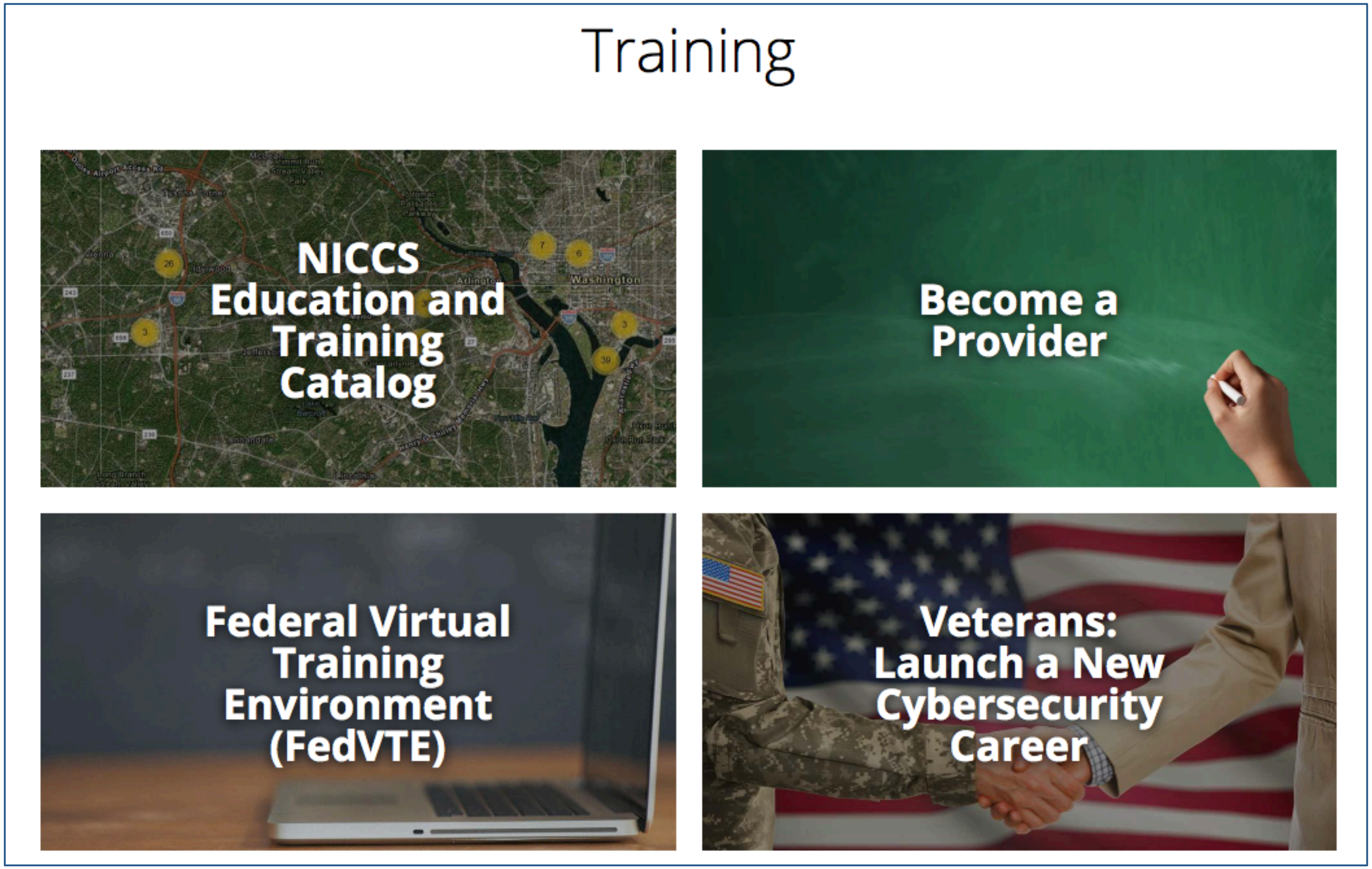
Phishing Awareness
Version 3.1
Jul 2017
Content Date March 2012

Personally Identifiable Information (PII)
Version 2.0
March 2013

Using Public Key Infrastructure
Version 1.0
December 2009

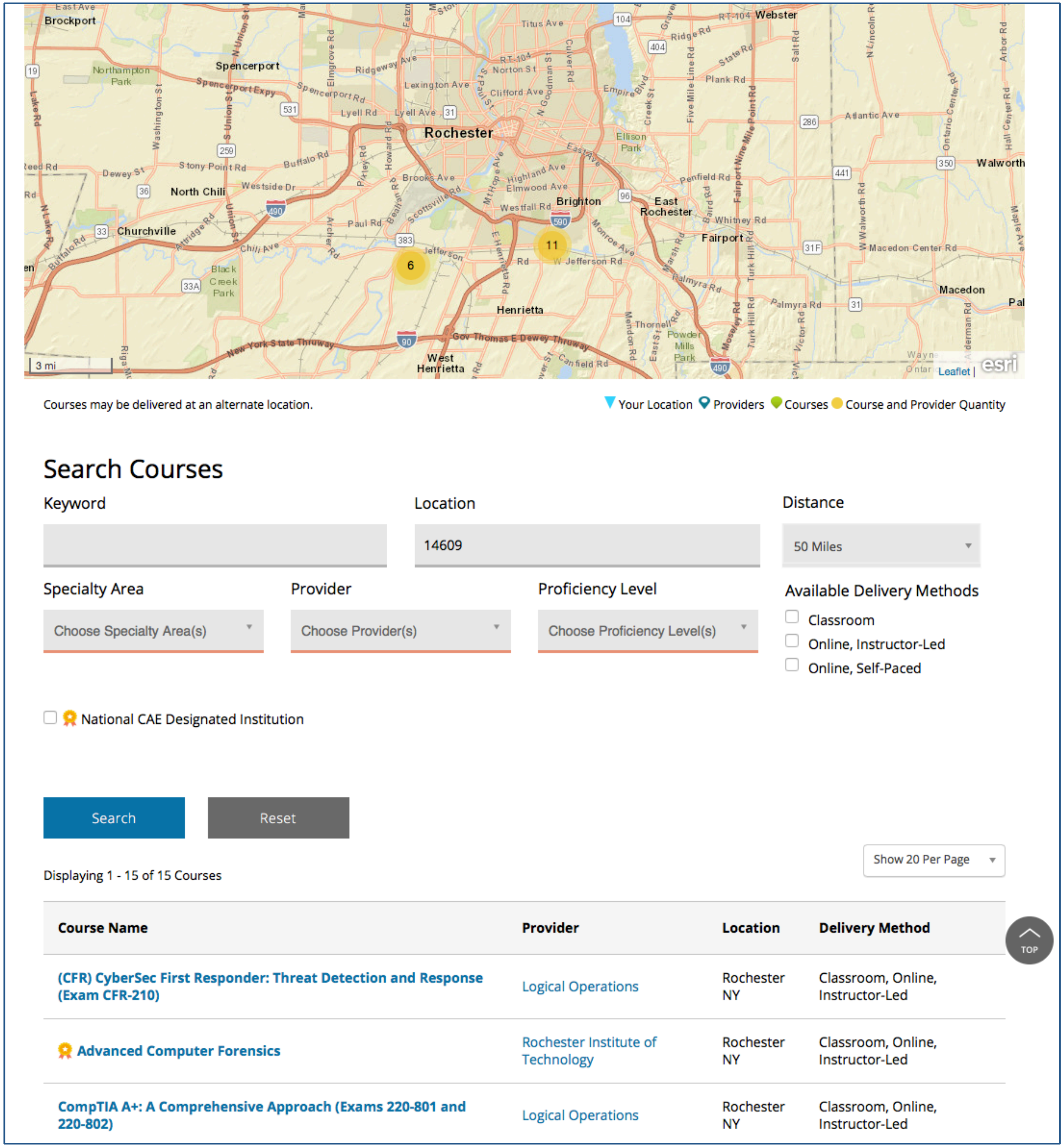
NICCS.US-CERT.GOV

National Initiative for Cybersecurity Careers and Studies


Training
NICCS Education and Training Catalog
Become a Provider
Federal Virtual Training Environment (FedVTE)
Veterans: Launch a New Cybersecurity Career

https://fedvte.usalearning.gov

Sample NICCS Training Catalog Search



Courses may be delivered at an alternate location.

▼ Your Location ● Providers ● Courses ● Course and Provider Quantity

Search Courses

Keyword

Location
14609

Distance
50 Miles ▾

Specialty Area
Choose Specialty Area(s) ▾

Provider
Choose Provider(s) ▾

Proficiency Level
Choose Proficiency Level(s) ▾

Available Delivery Methods
□ Classroom
□ Online, Instructor-Led
□ Online, Self-Paced

□ National CAE Designated Institution

Search   Reset

Show 20 Per Page ▾

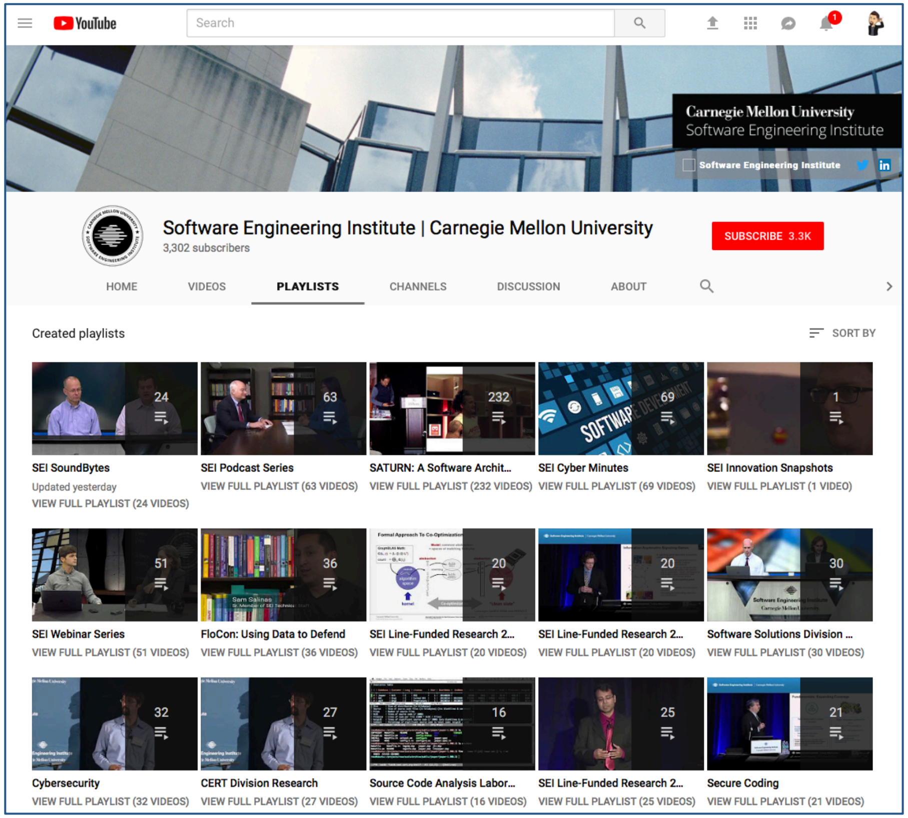
Displaying 1 - 15 of 15 Courses

Course Name	Provider	Location	Delivery Method
(CFR) CyberSec First Responder: Threat Detection and Response (Exam CFR-210)	Logical Operations	Rochester NY	Classroom, Online, Instructor-Led
Advanced Computer Forensics	Rochester Institute of Technology	Rochester NY	Classroom, Online, Instructor-Led
CompTIA A+: A Comprehensive Approach (Exams 220-801 and 220-802)	Logical Operations	Rochester NY	Classroom, Online, Instructor-Led

TOP

Stay Informed

- Podcasts (e.g. GovInfoSecurity, SecurityNow)
- Webinars & Videos (e.g. https://www.youtube.com/user/TheSEICMU)
  - Internal?
- Blogs (e.g. Krebs, Schneier, Tao Security)
- Twitter (e.g. Vendors, @NHISAC, @CYBER, @THEHACKERSNEWS)
- Memberships
  - ISSA
  - OWASP
  - ISACA
  - (ISC)^2
  - IEEE
  - ACM
  - InfraGard


YouTube
Search
Carnegie Mellon University
Software Engineering Institute
Software Engineering Institute
Software Engineering Institute | Carnegie Mellon University
3,302 subscribers
SUBSCRIBE 3.3K
HOME
VIDEOS
PLAYLISTS
CHANNELS
DISCUSSION
ABOUT
Created playlists
SORT BY
24
SEI SoundBytes
Updated yesterday
VIEW FULL PLAYLIST (24 VIDEOS)
63
SEI Podcast Series
VIEW FULL PLAYLIST (63 VIDEOS)
232
SATURN: A Software Archit...
VIEW FULL PLAYLIST (232 VIDEOS)
69
SEI Cyber Minutes
VIEW FULL PLAYLIST (69 VIDEOS)
1
SEI Innovation Snapshots
VIEW FULL PLAYLIST (1 VIDEO)
51
SEI Webinar Series
VIEW FULL PLAYLIST (51 VIDEOS)
36
FloCon: Using Data to Defend
VIEW FULL PLAYLIST (36 VIDEOS)
20
SEI Line-Funded Research 2...
VIEW FULL PLAYLIST (20 VIDEOS)
20
SEI Line-Funded Research 2...
VIEW FULL PLAYLIST (20 VIDEOS)
30
Software Solutions Division ...
VIEW FULL PLAYLIST (30 VIDEOS)
32
Cybersecurity
VIEW FULL PLAYLIST (32 VIDEOS)
27
CERT Division Research
VIEW FULL PLAYLIST (27 VIDEOS)
16
Source Code Analysis Labor...
VIEW FULL PLAYLIST (16 VIDEOS)
25
SEI Line-Funded Research 2...
VIEW FULL PLAYLIST (25 VIDEOS)
21
Secure Coding
VIEW FULL PLAYLIST (21 VIDEOS)

More YouTube Channels

- IT Free Training, http://www.youtube.com/user/itfreetraining
- itTaster, http://www.youtube.com/user/ittaster
- Professor Messer, https://www.youtube.com/user/professormesser
- StormWindLive, https://www.youtube.com/user/StormWindLive
- Eli the Computer Guy, https://www.youtube.com/user/elithecomputerguy
- Microsoft Support Videos, https://www.youtube.com/user/MicrosoftCSSVideo
- DansCourses, http://www.youtube.com/user/danscourses
- InfoSec Institute Training, https://www.youtube.com/user/InfoSecInstitute
- Software Engineering Institute, https://www.youtube.com/user/TheSEICMU
- Hak5 (https://hak5.org), https://www.youtube.com/user/Hak5Darren

EY's Metro Email Service (video)

#1 - "EY's Metro Email Service" - Produced by Cohn Creative Group for EY

What did we learn?

- Key takeaway presented on the screen:

  Don’t trust just anyone with client data. Use approved applications.

- Risk associated with sending work from untrusted home machine to work
  - **Disabled Protections**
  - **Virus**
  - **Lost privacy**
- How email works?
  - Kinda

Contact Information

Dennis M. Allen
Technical Manager, Education & Training
CERT Cyber Workforce Development
https://www.linkedin.com/in/dennis-m-allen
dallen@cert.org