Beyond Dilbert, xkcd and Little Bobby

Teaching cybersecurity with comics

Laurin Buchanan, CISSP
Principal Investigator
Secure Decisions

Secure Decisions

Division of Applied Visions, Inc.
- 50 people in Northport and Clifton Park, NY
- Security clearances

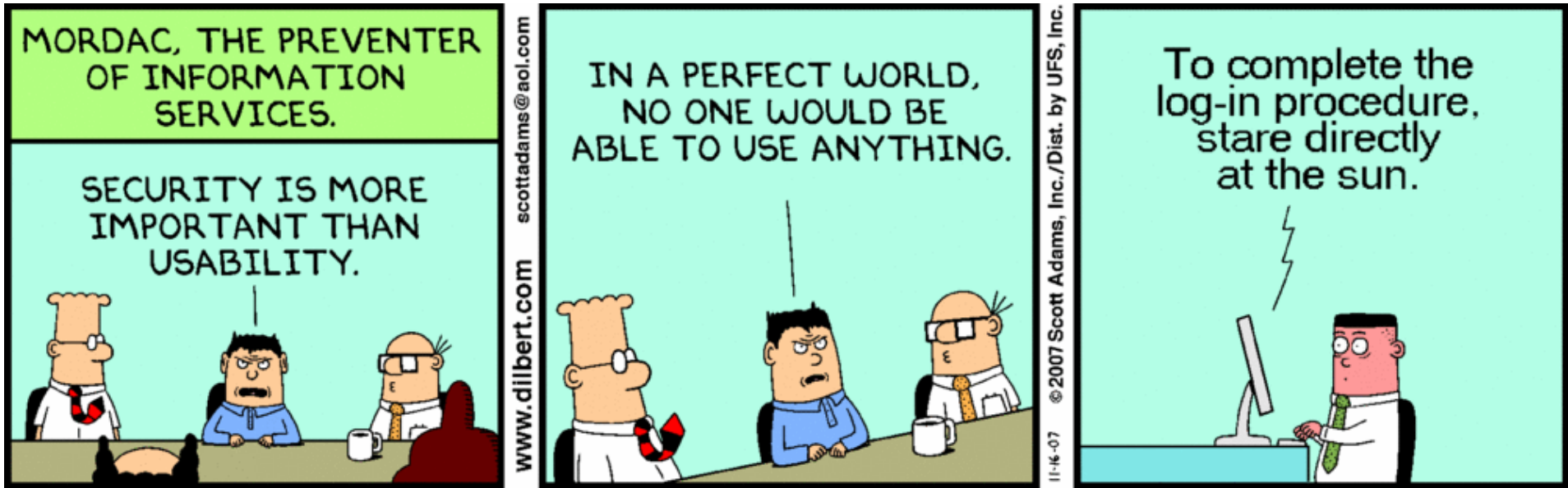
Cybersecurity R&D focused on **human decision making**

- Analyze security decision processes
- Build visualizations and visual analytics to enhance security decision processes
- Develop decision support for network & application security, mission impact analysis

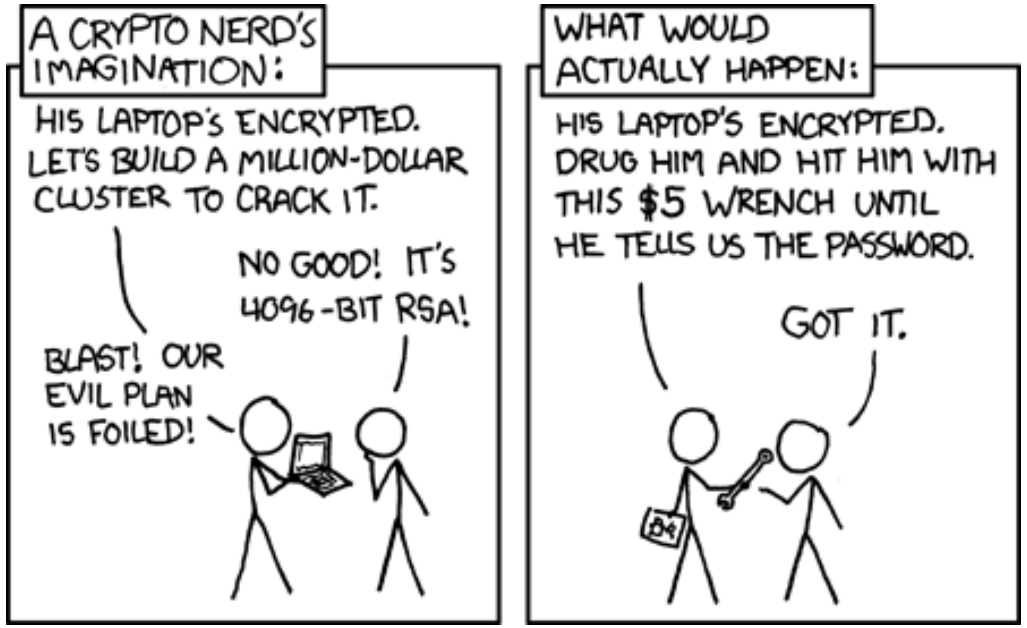
Our expertise starts where automated security sensors stop

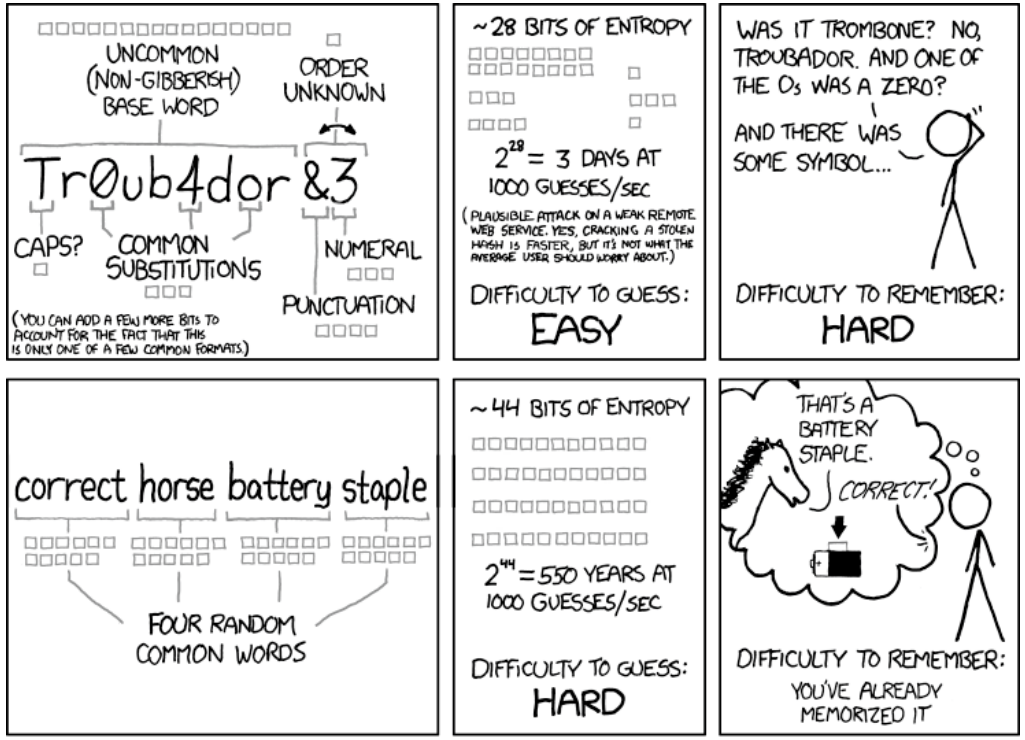
Transition R&D into operational use, in government and industry

Dilbert by Scott Adams

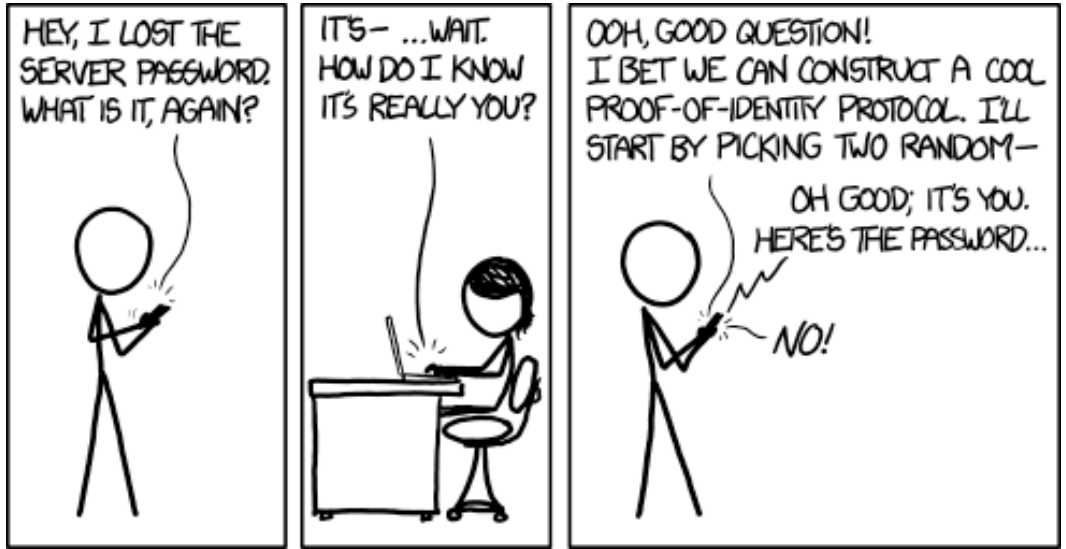


xkcd by Randall Munroe





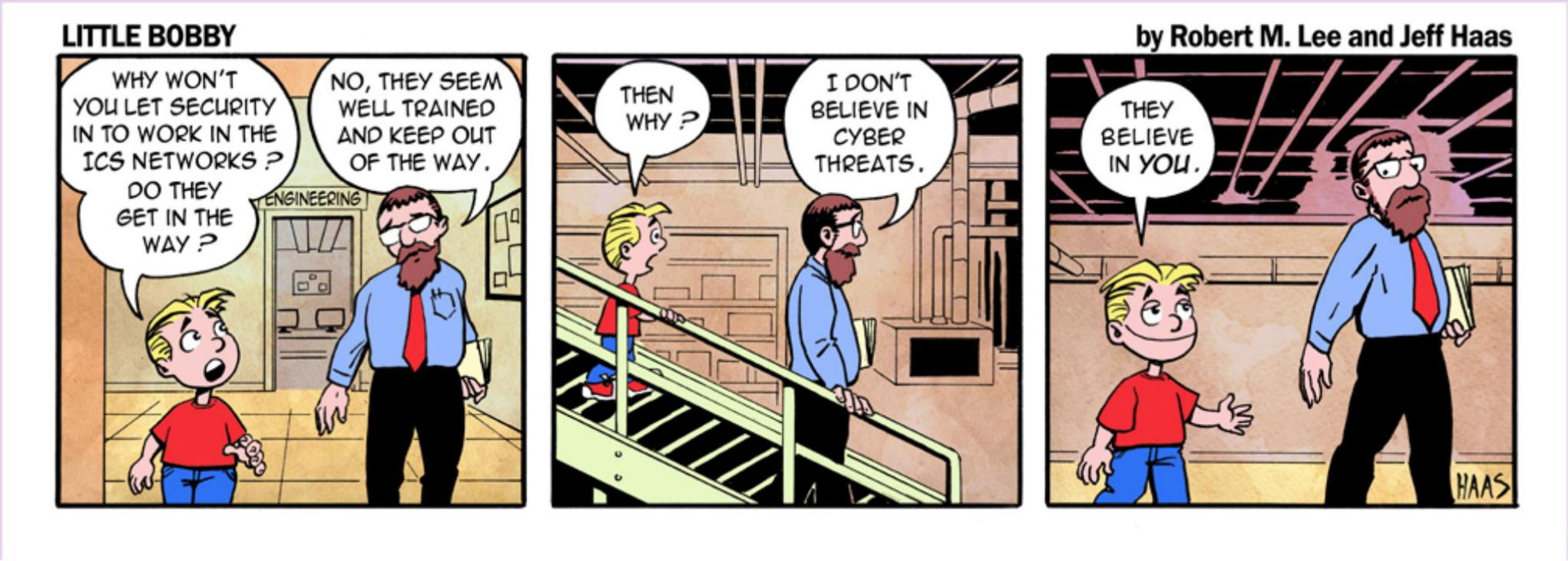
THROUGH 20 YEARS OF EFFORT, WE'VE SUCCESSFULLY TRAINED EVERYONE TO USE PASSWORDS THAT ARE HARD FOR HUMANS TO REMEMBER, BUT EASY FOR COMPUTERS TO GUESS.



Little Bobby by Robert M. Lee

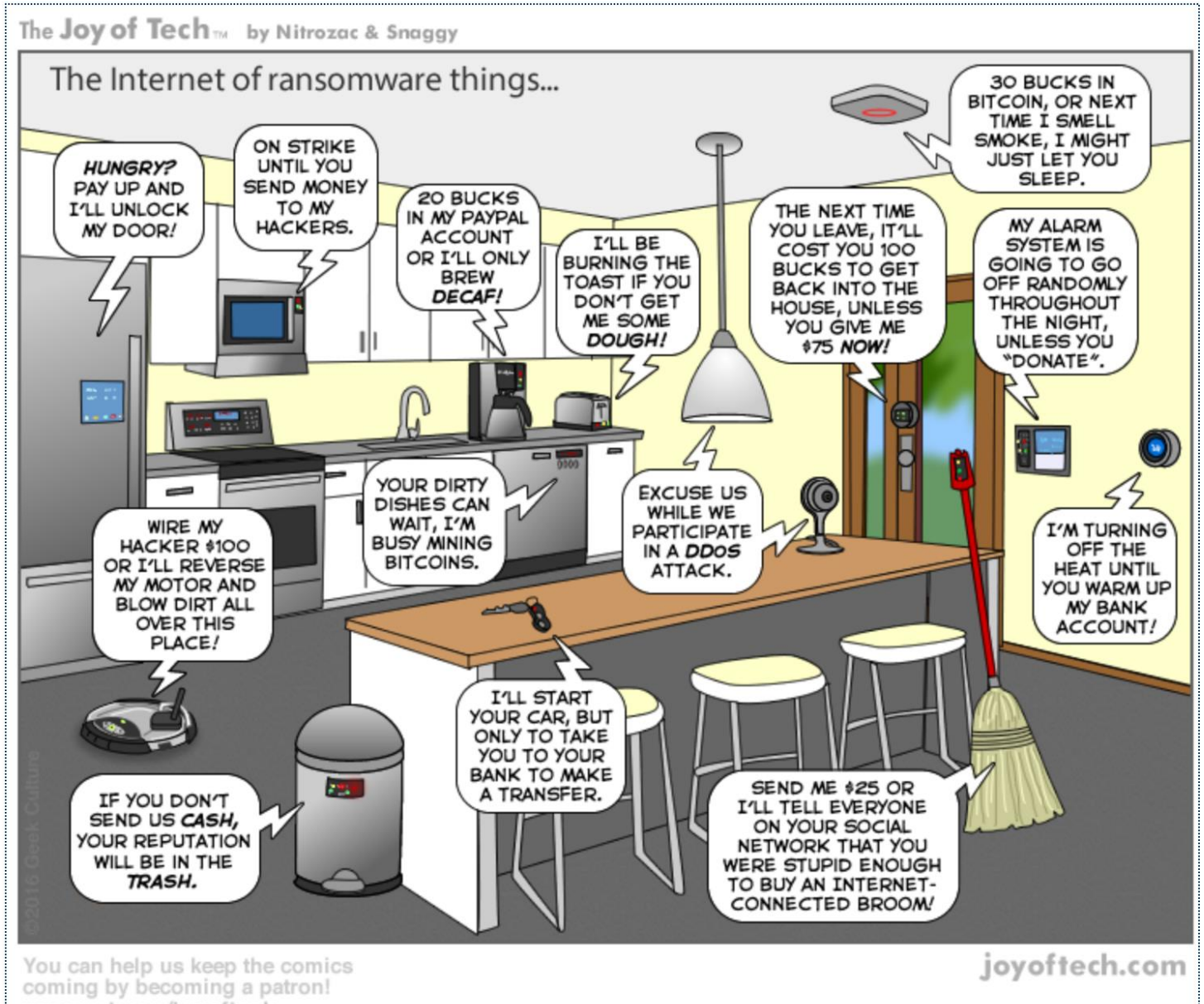
LITTLE BOBBY

A Sunday Morning web Comic on Technology and Security



FEBRUARY 3, 2019

Joy of Tech by Nitrozac & Snaggy



CharlieCiso by Powell & Amaroso

Comics for education

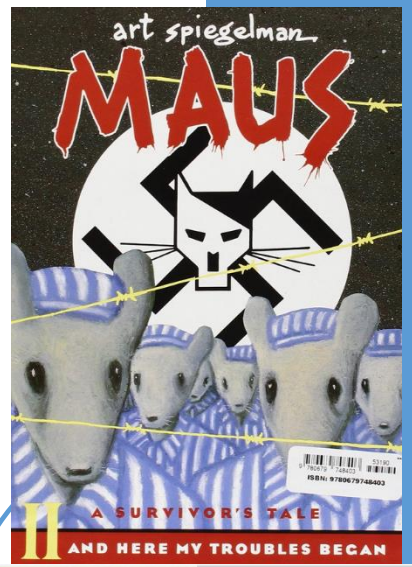
Storytelling is a powerful method – for everyone

- Comics used in classrooms for more than 60 years

Most people are “visual learners”

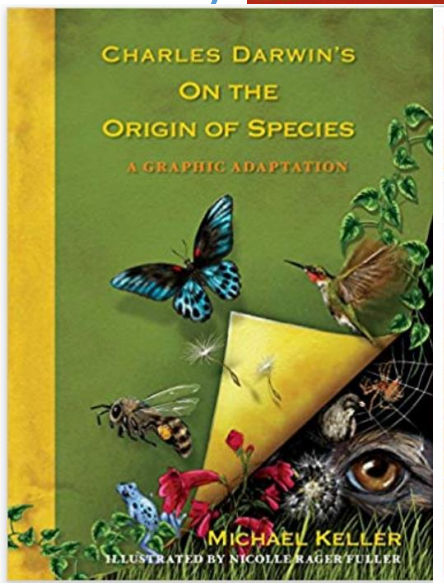
- Words + images are more complex, require more memor
  - More memory = better recall, better learning
  - Provide context for information & abstract concepts
- Society now communicates visually: advertising, infographics, social media, HTML email

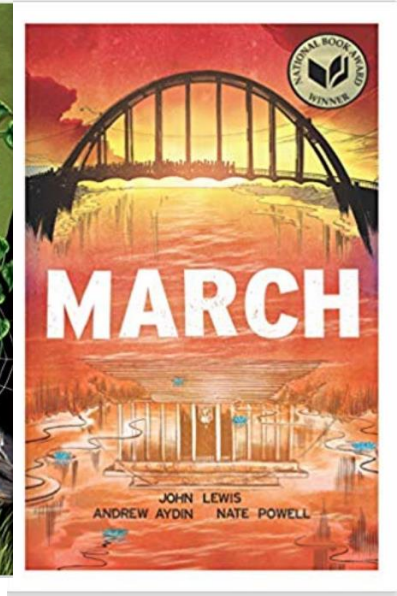
Education is serious about comics



Using graphic novels can increase motivation, content area literacy, and curiosity

- Engages non-majors in learning science *(Hosler & Boomer 2011)*
- Educating patients and medical students on understanding outcomes *(Green 2013), (Yu 2018)*
  - #graphicmedicine on Twitter





American Library Association: Graphic Novels & Comics Round Table

- NY Public Library programming for NY Comic Con
  - #educomix on Twitter

Long ago – in 2010….

US Air Force R&D project: interactive annual computer awareness training

- Something to engage everyone: 4 star generals & mechanics

Branching comics, viewed in web browser

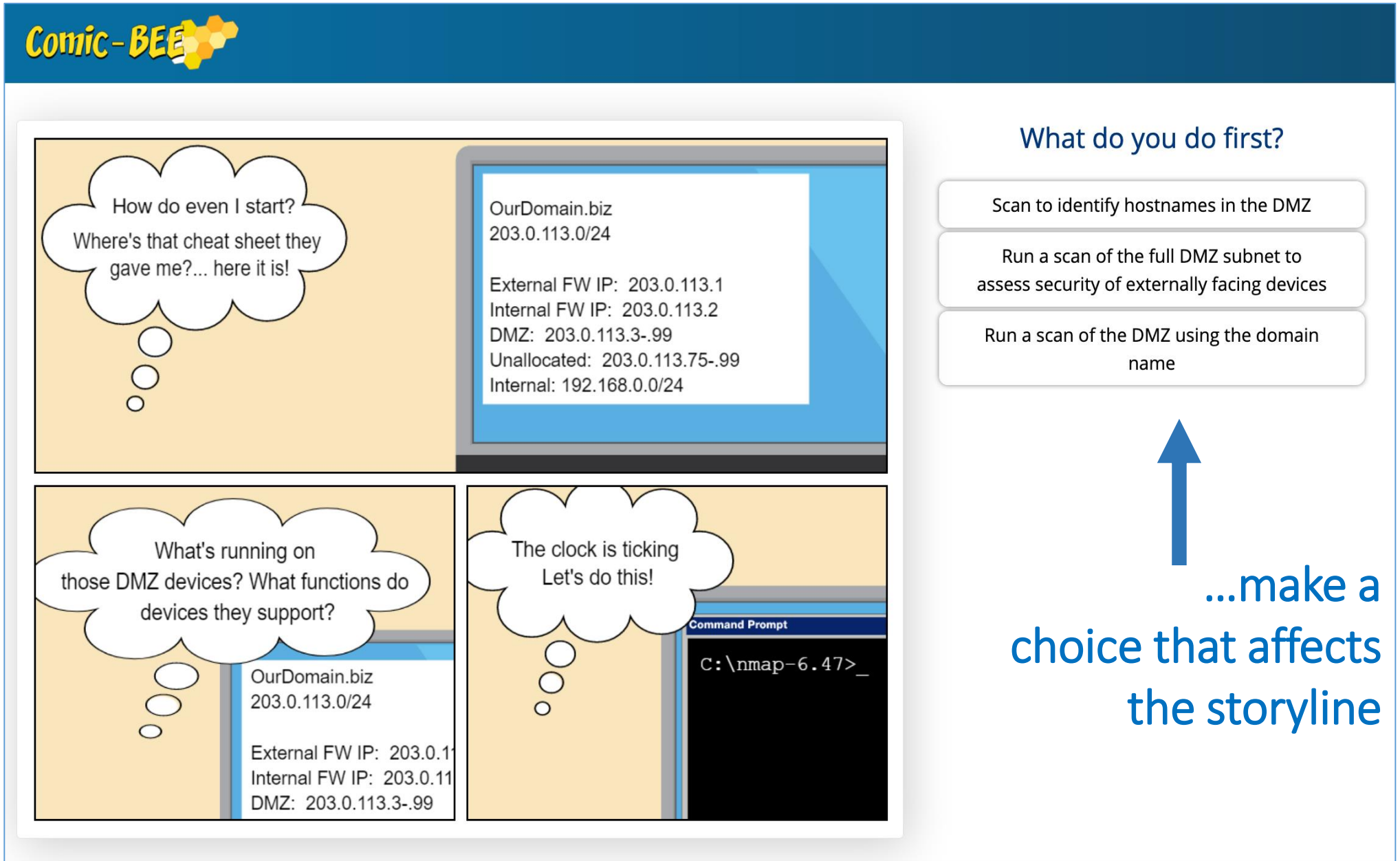
- Show downstream impacts of choices
- Time and geography are fluid in stories
- No software install required

Created two proofs of concept by hand

- Concept very popular, deemed too costly
  - Required professional graphic artist & computer programmer
  - 160 person-hours to create a short comic

Branching, interactive web comics

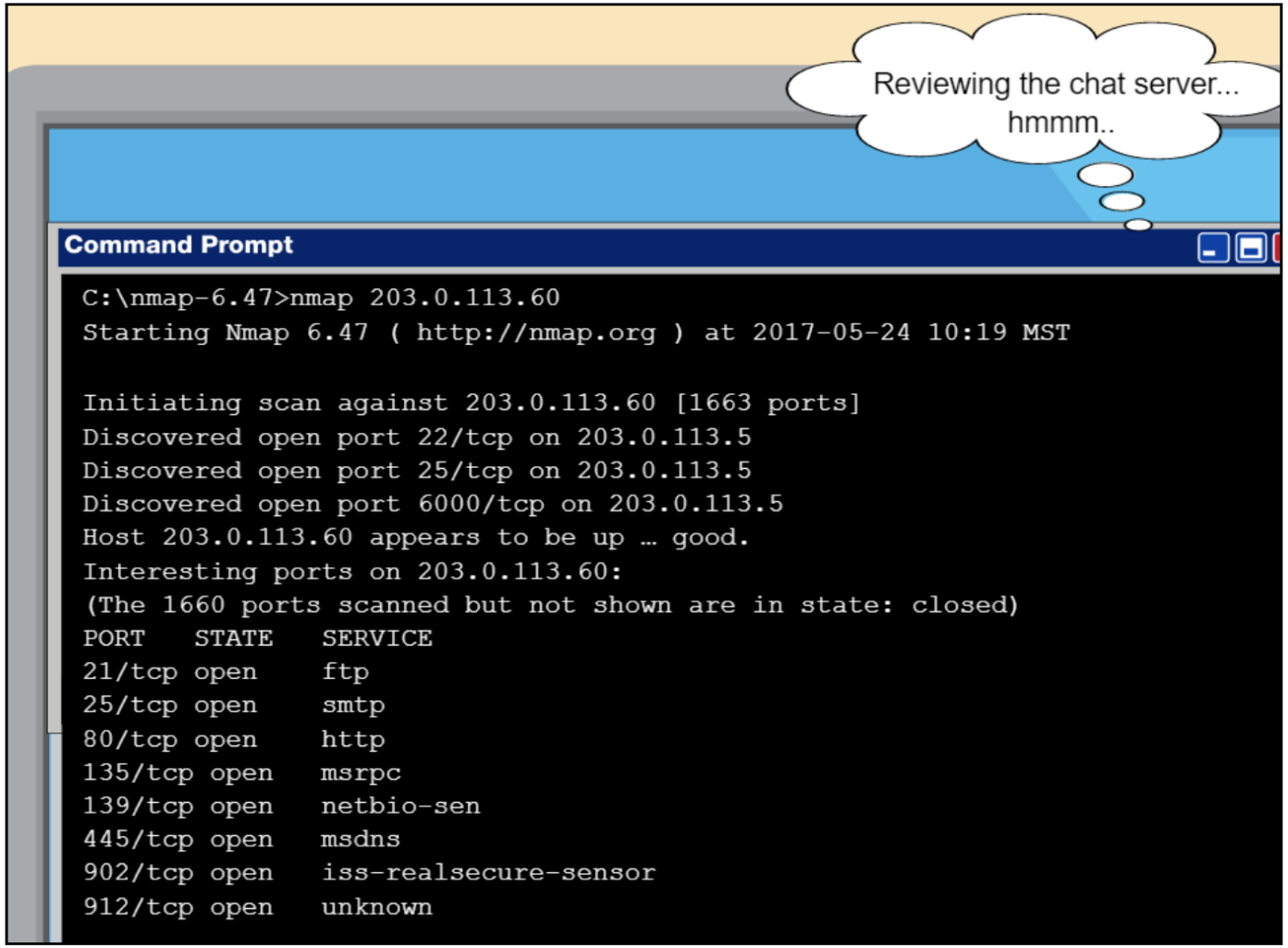
Read the story…



…make a choice that affects the storyline

Reader choices change the story line

Comic-BEE



Based on these open ports, what OS is the chat server?

- OSX
- Windows
- Linux

Using branching comics for education

Read comics

- Introduce new concepts or show context
- Informal or exploratory learning
- Micro-learning or short sim for e-learning or workforce

Complete a “seed” comic

- Scenario and initial script scenes provided; students create path to achieve specified goals
- Deeper learning & engagement through comic creation activity
- Ideal for non-majors or introductory courses; or as lab assignment

Students create own comic on topic

- Demonstrate mastery of concepts, strategies & dependencies

Options for creating general comics

- Comic-Life
- Seedling Comic Studio
- Makebeliefs Comix
- Halftone 2
- ToonDoo
- StripGenerator
- Pixton
- StoryboardThat

Limitations:

- Little or no support for instructional design, branching stories, or assessment
- Most target kids
- **None designed for cybersecurity**

Comic-BEE

Comic-Based Education and Evaluation*

Web app to create branching comics aligned with curricular goals

- Integrates diverse workflows to create educational comics
- Scaffolds the author through workflows

Enables authors to rapidly create branching comics

- Create complex stories in days not weeks
- No computer programmer or graphic artist required
- No software installs or browser plug-ins needed

Integrates NICE Cybersecurity Workforce Framework (NCWF)

- Lesson Plan can leverage Knowledge, Skills and Abilities (KSAs) and Tasks from NCWF

* Based on research funded by Department of Homeland Security Science & Technology Directorate, Cyber Security Division

Comic-BEE scoring capability

Create a scored comic as game/challenge or workforce assessment

- Story format supports topics not possible in CTF competitions
- Scored comic can be pre-test or post-test for other learning
- Any comic easily converted to scored comic

Configuring scoring

- Rank end scenes, choice expertise & quality in branching script
- Configure weighting of scoring elements
  - Skill-based or time-based weights
- Optional automatic start/stop time of assessment window

Automated scoring

- Comic-BEE captures reader's choices and time to make choices
- Anonymous, one-time access codes: readers don't need system account

Comic-BEE integrates different workflows

Plan Lesson	Write Script	Layout Storyboard	Create Final Comic
Define topic & intended audience High-level concepts with Knowledge, Skills & Abilities (KSAs) Create specific learning goals	Builds on lesson plan Branching story with choices as graph Both positive and negative outcomes Choices associated to learning goals Rank choice expertise & quality	Builds on script Rough visual layout with low-fi graphics Preview of scene panels with text of decision and choices Live preview links to check story flow	Builds on storyboards Automation swaps stick figures with high-fi graphics Detailed layout Preview scene panels & live links Publish comic

Wide range of cybersecurity concepts

Expert created comics

Ethics for computer science: the Trolley problem

Incident response: IT Help Desk discovers a worm outbreak

Windows OS security: Account policy, Audit policy, Security options, Remote settings & Group Policy

Risk Management

Corporate Security Policy training for IT & Dev staff (DevSecOps)

Student created comics

System Administration: access to privileged health information

Ethics for computer science students

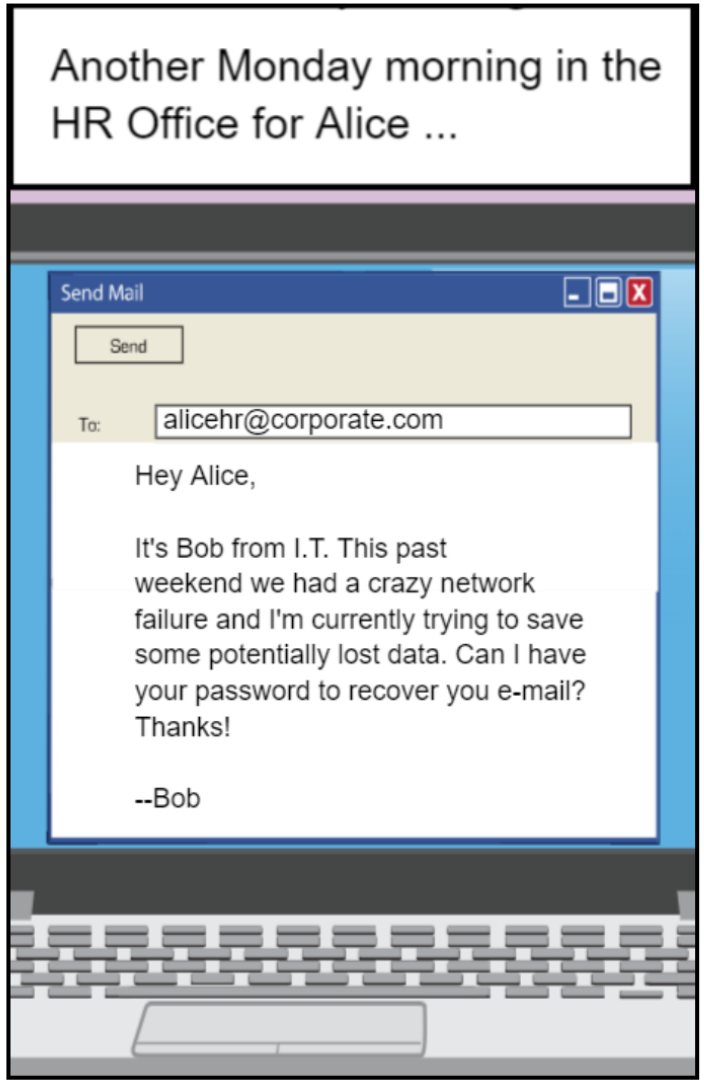
Diversity of cybersecurity comics

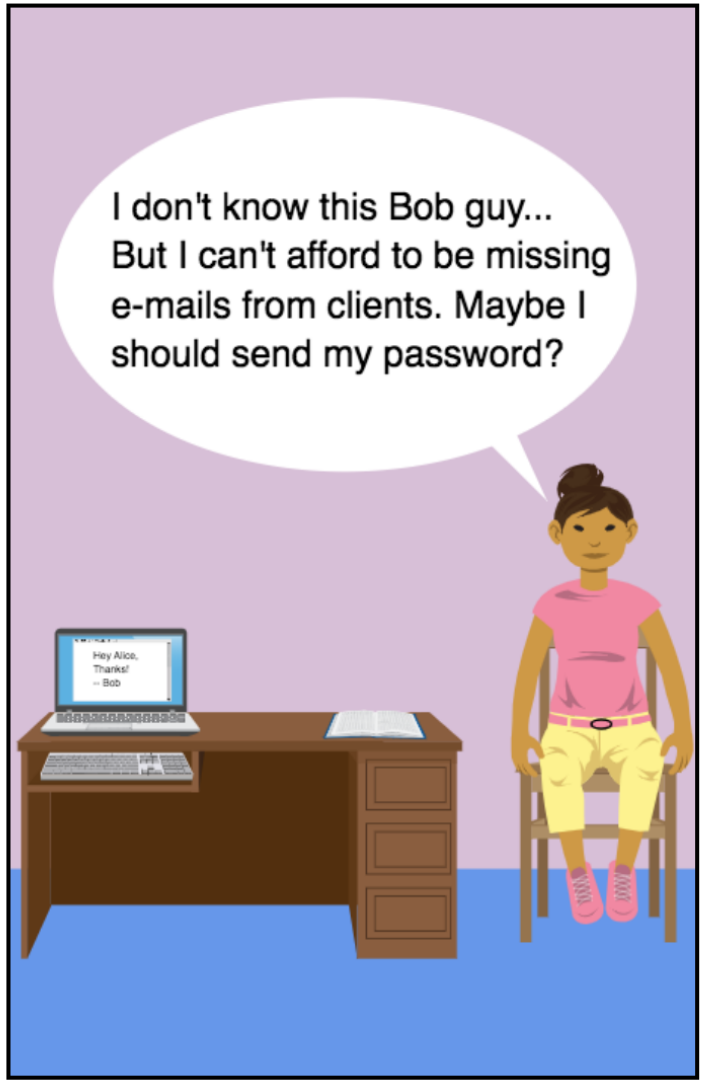
Concepts

- Ethics for computer science
- Incident response: IT Help Desk discovers a worm outbreak
- Windows OS security: Account policy, Audit policy, Security options, Remote settings & Group Policy
- NIST Risk Management Framework
- Corporate Security Policy
- System Administration: access to privileged health information

Intended Uses

- Concept intro for undergraduate comp sci
- Training for IT & Dev staff (DevSecOps)
- Education / practice for cyber clubs – going beyond CyberPatriot
- Marketing material for consulting & services firm
- Corporate policy awareness assessment
- College course assignment – instead of term paper
- Competition, challenge



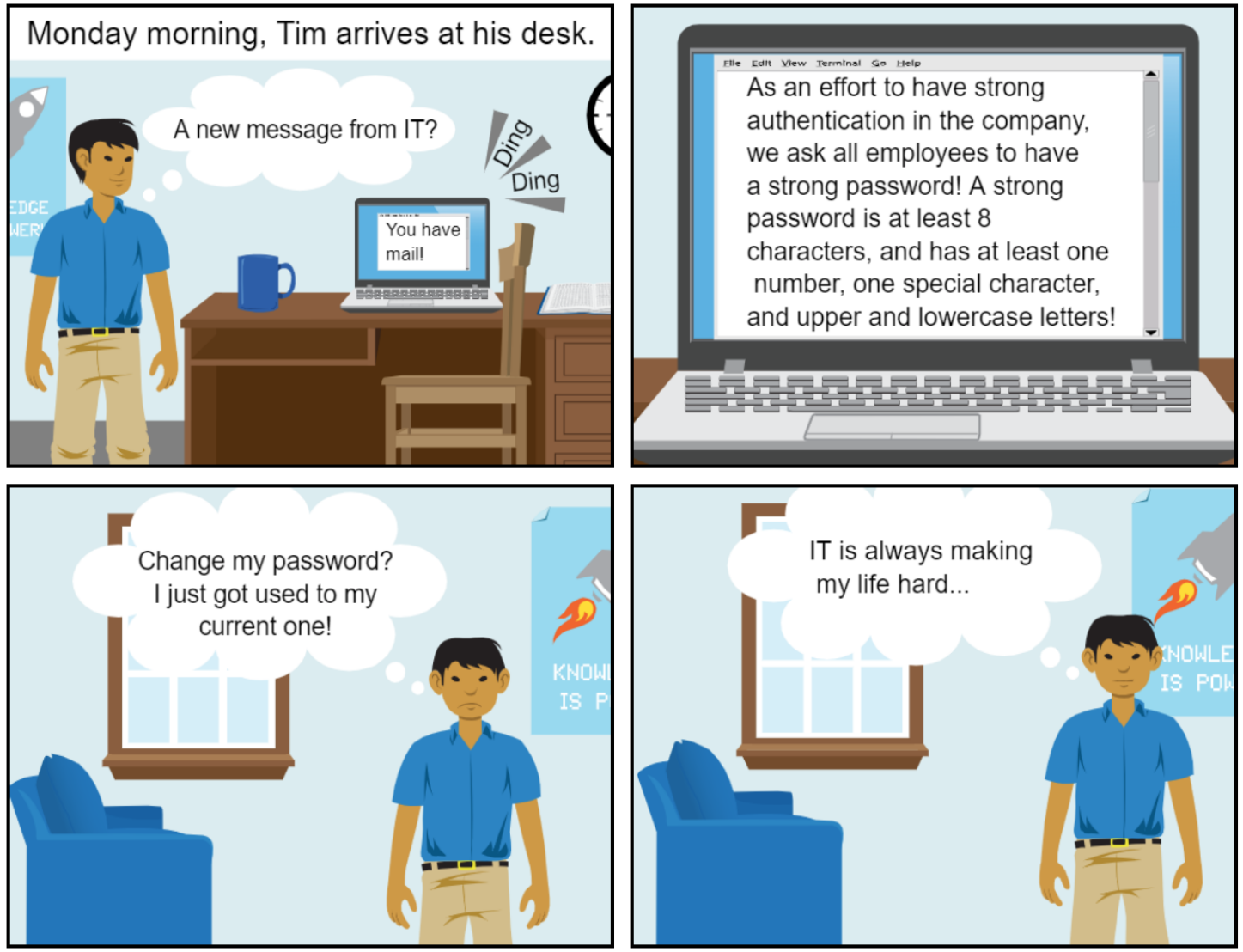


Should Alice give up her password?

- Yes, give her password to Bob!
- Nah, lets continue to ignore the issue. Not me, not my problem right?
- No. I am not just going to hand out my password! I'm going to tell my boss!

NCCDC: Phishing

Comic-BEE

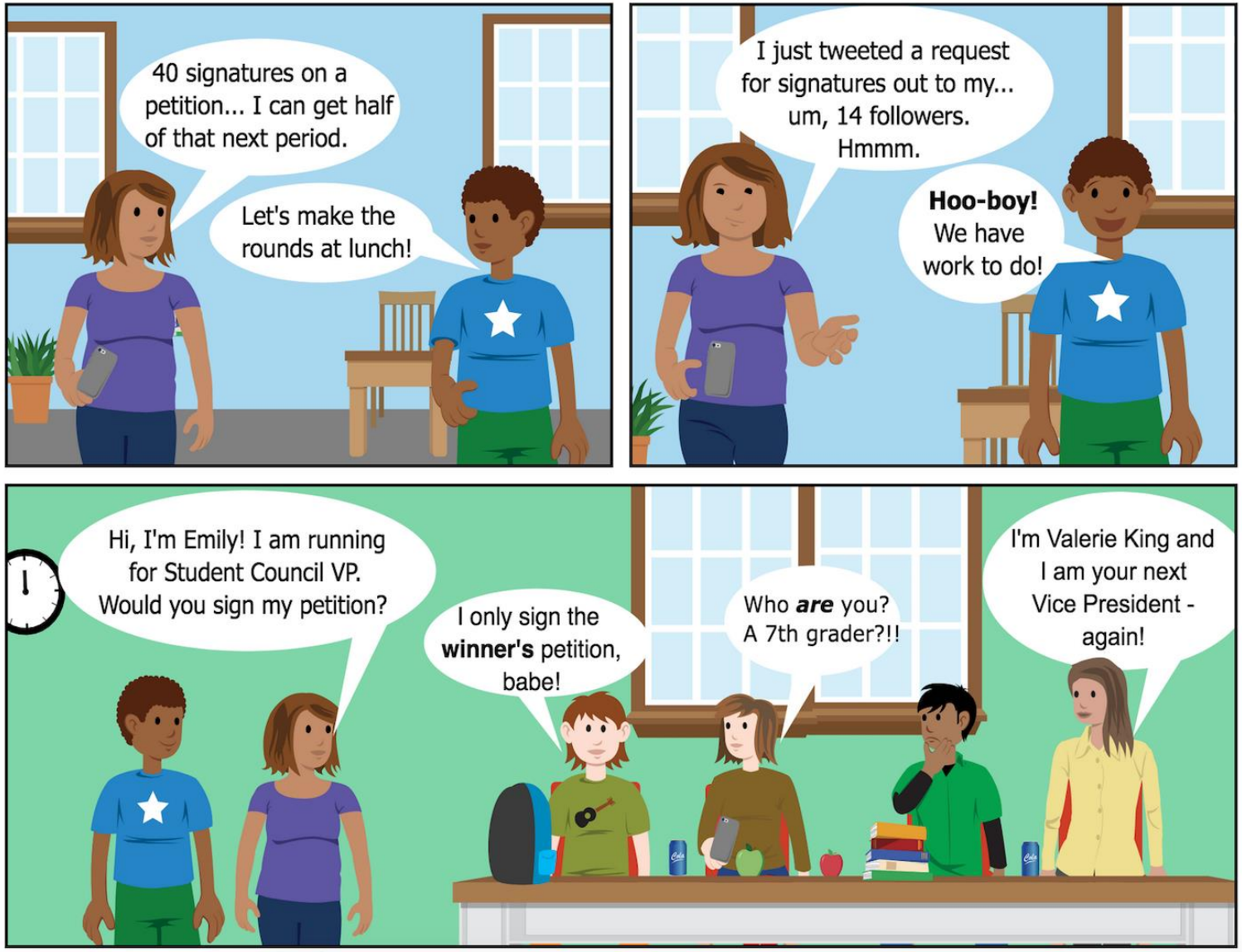


How do you react to the message prompting you to change your password?

- Decide to keep your current password.
- Re-use one of your old passwords
- Create a new password

NCCDC: Strong Passwords

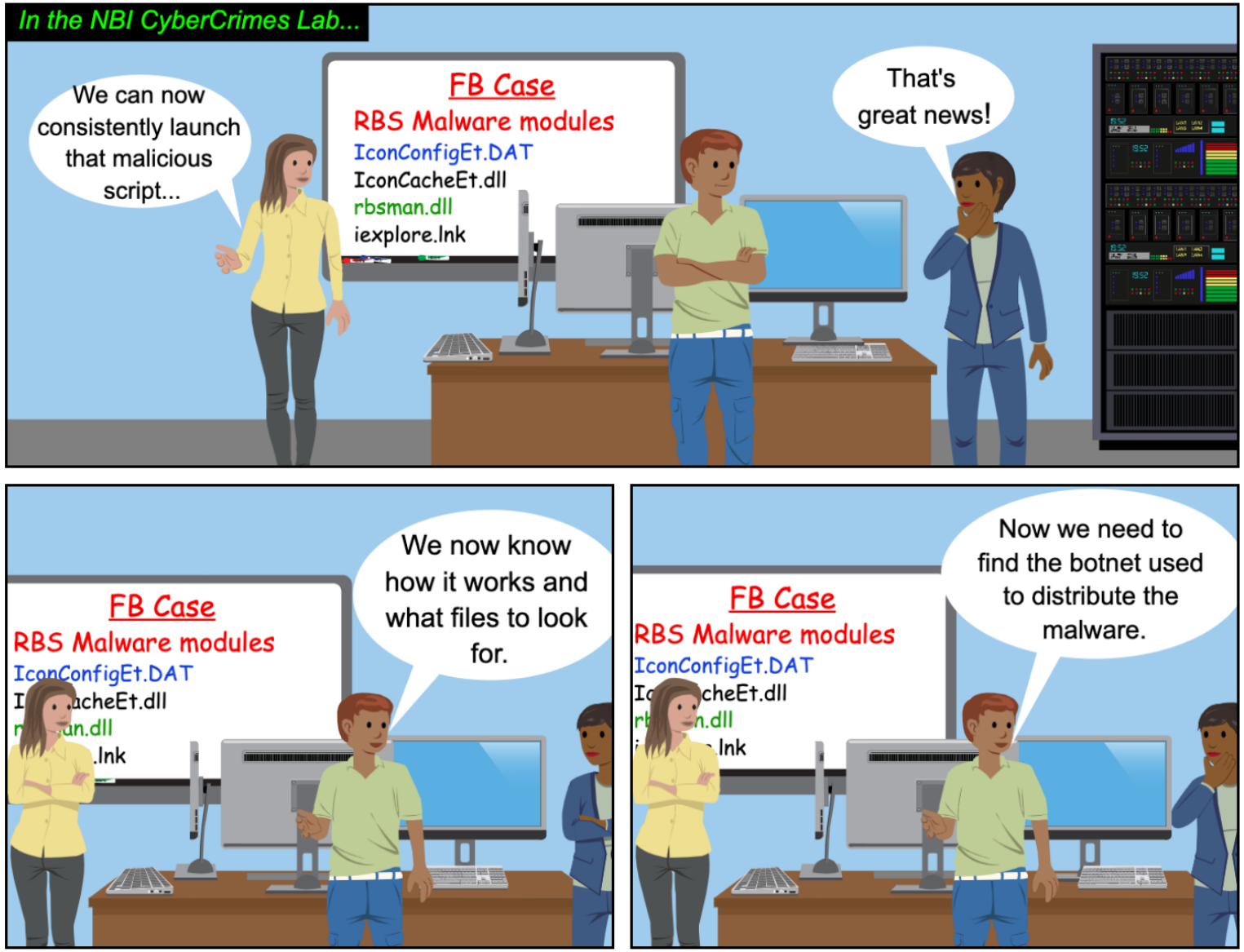
Comic-BEE



How do you respond to their refusals to sign your petition?

- Get a photo of the table and tweet out about rude behavior
- Ask if them if they've already signed a petition - is anyone *else* running for VP??
- Accept that not everyone will sign your petition and move on to the next table

Cyber Ethics



Which lead do you follow to find the cyber criminals?

Find out what you know about those IP addresses in the code

Look for other malware with very similar code - it may be written by the same team

Cyber Crime Investigation

Huh. . .
What is going on with that chat server?

Command Prompt

```
Starting Nmap 6.47 ( http://nmap.org ) at 2017-05-24 12:12 MST
Nmap scan report for 203.0.113.60
Host is up (0.00029s latency).
Not shown: 1494 closed ports, 496 filtered ports
PORT STATE SERVICE
88/tcp open kerberos-sec
139/tcp open netbios-ssn
445/tcp open microsoft-ds
631/tcp open ipp
88/udp open|filtered kerberos-sec
123/udp open ntp
137/udp open netbios-ns
138/udp open|filtered netbios-dgm
631/udp open|filtered ipp
5353/udp open zeroconf

Nmap finished: 1 IP address (1 host up)
```

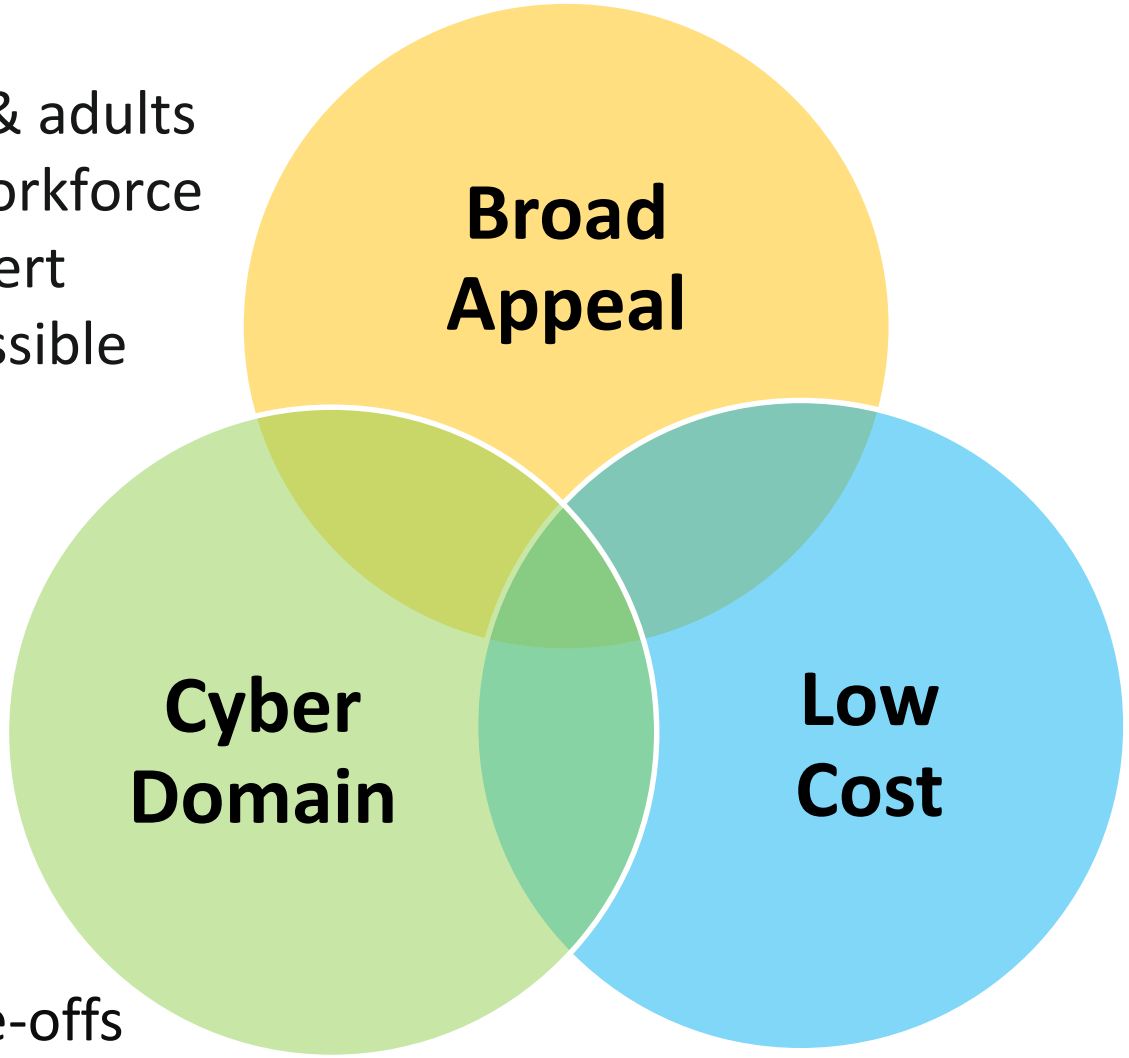
Which string will give you an unobtrusive scan of the chat server with both TCP and UDP?

- nmap -sS -sX -Pn 203.0.113.60
- nmap -sS -sU -PS 203.0.113.60
- nmap -sS -sU -Pn 203.0.113.60
- nmap -sT -sU -Pn 203.0.113.60

Command Line
nmap

The ideal cybersecurity education approach?

- Interactive
- Engages kids & adults
- Students & workforce
- Novice to expert
- Browser accessible



- Less time to create
- Easy update & refresh
- Content for learning or evaluation
- Low maintenance & license cost

- Technical subjects
- Law, policy, ethics
- Critical thinking
- Strategy & risk trade-offs
- Aligns with NICE Workforce Framework

Seeking research partners to formally assess learning with branching comics

Laurin Buchanan, CISSP
Principal Investigator
laurin.buchanan@securedecisions.com
631.759.3926
https://securedecisions.com/comicbee
https://comic-bee.com

@ComicBEE