



EXCLUSIVE

THE CYBERHERO ADVENTURES

DEFENDERS OF THE DIGITAL UNIVERSE

DEFENDING YOUR HEALTH!



Medigy
Innovation Network

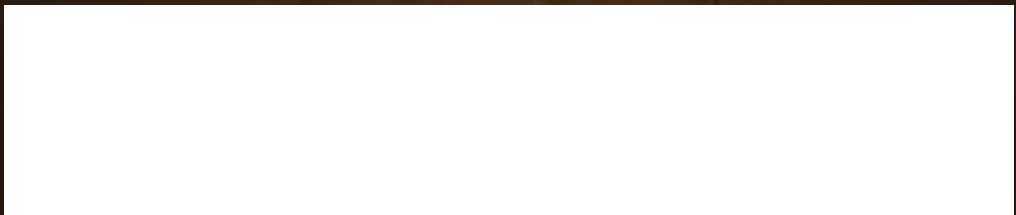
THANK YOU!

ONE OF THE MANY LESSONS THAT I'VE LEARNED AS THE VICTIM OF A FIFTEEN YEAR SERIES OF INSIDER CYBER CRIMES IS THAT THE ONLY TIME PEOPLE HEAR ABOUT HACKS IS WHEN THE HACKERS ARE SUCCESSFUL. THIS LIFE-CHANGING ENDEAVOR IS DEDICATED TO ALL OF THE UNSUNG, REAL-LIFE CYBER HEROES AND LAW ENFORCEMENT PROFESSIONALS WHO TOIL WITHOUT FANFARE OR ACKNOWLEDGEMENT EVERY DAY TO DEFEND US ALL AT WORK, HOME AND SCHOOL.

THIS INCREDIBLE JOURNEY WOULD NOT HAVE BEEN POSSIBLE WITHOUT THE UNWAVERING SUPPORT OF MY BEAUTIFUL, INTELLIGENT, CHARMING AND FUNNY BETTER-HALF, VALERIE AND OUR TWO AMAZING DAUGHTERS, SARA AND ILANA. THEY HAVE AND WILL ALWAYS BE AN INSPIRATION TO ME AND TO EVERYONE WHOSE LIVES THEY TOUCH. TO MY 90-YEAR-YOUNG MOMMY... IT'S ONLY GOING TO GET BETTER!

WORDS CAN'T ADEQUATELY EXPRESS MY GRATITUDE TO THE MEMBERS OF THE CYBERMAN SECURITY, LLC ADVISORY BOARD. THEY HAVE HELD MY HAND AND SHARED THEIR MORE-THAN-100-YEARS OF COLLECTIVE EXPERIENCE IN CYBER SECURITY AND TECHNOLOGY WITH THE PATIENCE OF SAINTS. THEIR REAL-WORLD EXPERIENCES AS DEPICTED IN THE CYBER HERO ADVENTURES WILL ENLIGHTEN, EMPOWER, AND ENTERTAIN PEOPLE OF ALL AGES AND HELP KEEP EVERYONE SAFE WHILE ONLINE.

AND LAST, BUT NOT LEAST, TO JULIO ALVAREZ AND THE INCREDIBLY TALENTED TEAM AT CREATURE ENTERTAINMENT, THANK YOU FOR YOUR STUNNING CREATIVITY, INCREDIBLE TALENT AND FOR TURNING OUR DREAM INTO A REALITY!




- GARY L. BERMAN, CREATOR
THE CYBERHERO ADVENTURES:
DEFENDERS OF THE DIGITAL UNIVERSE
CEO, CYBERMAN SECURITY, LLC

TO LEARN MORE ABOUT
SPONSORSHIPS OR TO CREATE A
CUSTOM EDITION FOR YOUR
ORGANIZATION, PLEASE EMAIL
GARY@CYBERHERONETWORK.COM

www.cyberheronetwork.com

WHO DO YOU TRUST?



**DON'T FALL
FOR VENDOR
BS!**

Use [Medigy.com](https://www.Mediggy.com) to discover
the tools that your fellow
healthcare cyberheroes use!

BLUVECTOR®

A COMCAST COMPANY

**We detect
threats
others don't**

Learn more at

www.bluvector.io



Cyberlitica

Enterprise Threat Intelligence



Dark Web & Domain Monitoring

Chatroom-Surveillance

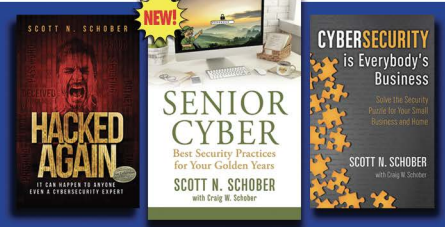
SMB Cyber Survival Kit

<https://www.cyberlitica.com/>

SOMEWHERE...A CYBERCRIMINAL IS BREACHING A WIRELESS DEVICE AND STEALING VALUABLE DATA, BUT FEAR NOT... WIRELESS WARRIOR IS HUNTING DOWN DANGEROUS HACKERS!!!



MEET THE REAL WIRELESS WARRIOR! SCOTT SCHOBER RUNS A TOP WIRELESS SECURITY FIRM & ALSO WRITES THESE BEST-SELLING CYBERSECURITY BOOKS...



YORKIE-PRO!!!

WIRELESS THREAT DETECTOR ABLE TO IDENTIFY AND LOCATE NEARBY DEVICES INCLUDING WICKED WI-FI, SHADY CELLULAR, BAD BLUETOOTH, AND MUCH MORE...



SENTRYHOUND-PRO!!!

SECURE ENTRYWAYS AND CORRIDORS WITH POWERFUL, FERROUS DETECTION.

ABLE TO DETECT HIDDEN PERSONAL ELECTRONICS, ON OR OFF, THESE SENSOR POLES CAN BE DEPLOYED ANYWHERE AS A SINGLE OR DUAL-POLE PORTAL IN HIGH FOOT TRAFFIC AREAS.

DETECT CONTRABAND DEVICES THAT FOOL METAL DETECTORS AND AVOID FALSE TRIGGERS!



WALLHOUND-PRO!!!

PROTECTING GOV'T, MILITARY & LAW ENFORCEMENT FACILITIES, THIS WIRELESS THREAT DETECTION MONITOR CAN BE MOUNTED ANYWHERE TO ALERT AUTHORITIES TO AN ARRAY OF UNSECURE WIRELESS DEVICES.

SECURE STAFF & VISITORS FROM MALWARE ATTACKS AND MUCH MORE...



BOOKS + PRODUCTS AVAILABLE ON AMAZON.COM OR DIRECTLY FROM WWW.BVSYSTEMS.COM



BERKELEY VARITRONICS SYSTEMS, INC. IS A 50 YEAR OLD, PRIVATELY OWNED BUSINESS AND A PROUD MEMBER OF CYBER HERO ADVENTURES. ALL PRODUCTS MADE IN THE USA.

THE CYBERHERO ADVENTURES

DEFENDERS OF THE DIGITAL UNIVERSE!



Gary Berman

*writer
creator*

**George Antoniou
PhD**

*writer
technical
advisor*

Daniel Dulitzky

*pencils
character
design
colors*

Rey Acevedo

inks

Andres Labrada

cover art

Colors by Splash!

cover colors

Julio Alvarez

*writer
letterist
colors
design
product
mgmt*

John Ulloa

*design
advisor*

© 2021 Cyberman Security, LLC

All characters, the distinctive likenesses thereof and all related indicia are trademarks of Cyberman Security, LLC. The stories, characters and incidents featured in this publication are entirely fictional. Any similarities to persons, living or dead, are purely coincidental.

Disclaimer:

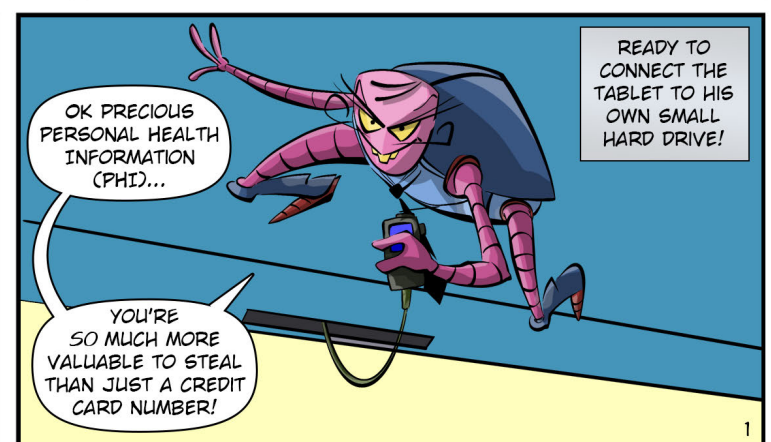
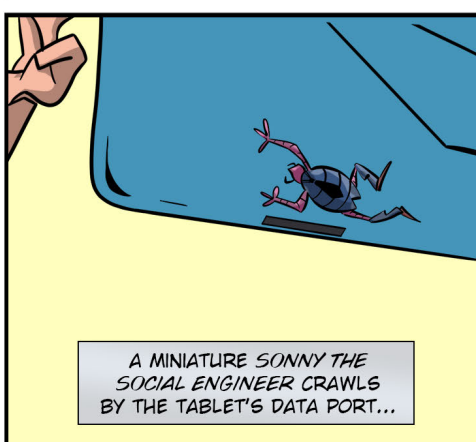
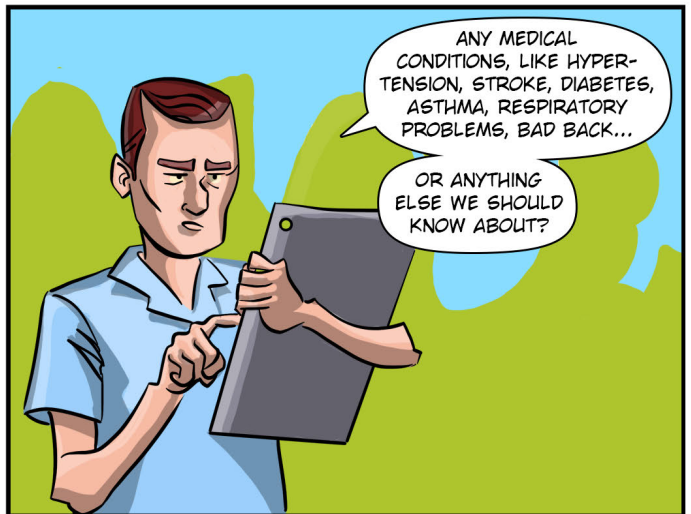
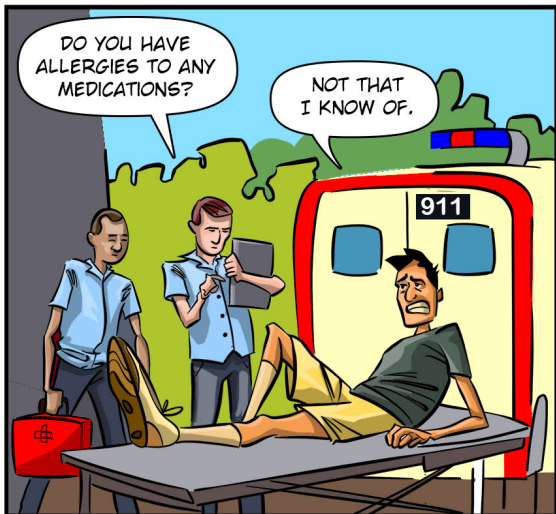
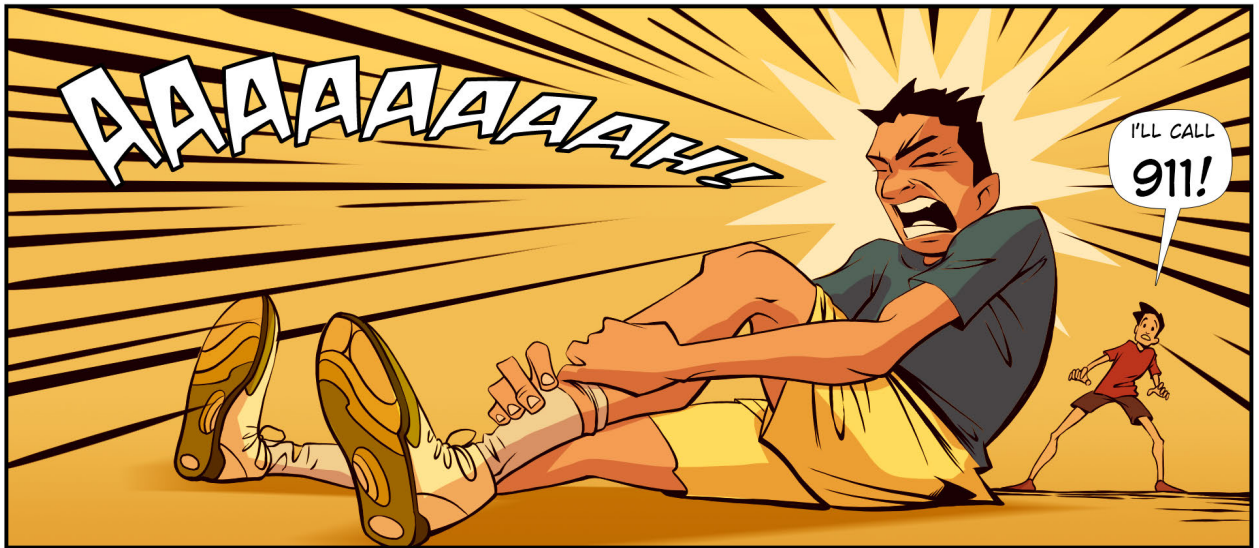
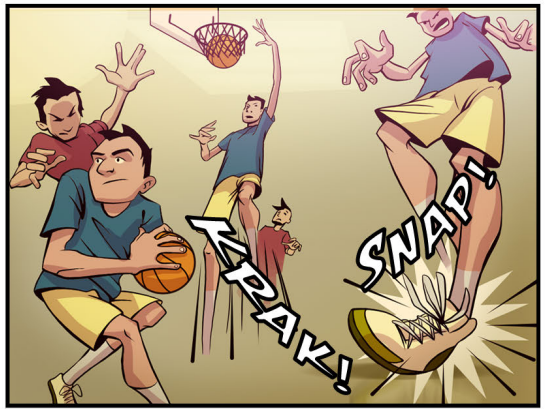
Cyberman Security, LLC is the publisher of The Cyber Hero Adventures: Defenders of the Digital Universe. The content and information in this publication is very general and provided as a service, for informational purposes only. We try to keep our themes timely and relevant and present our ideas in an entertaining, thought-provoking way. However, the information and material in this publication should not and cannot be relied upon, whether for business, commercial or personal purposes. Everyone's situation is different and you should always consult professionals who can review your particular situation and provide you with advice and guidance appropriate to your particular circumstances. So we are clear, neither Cyberman Security, LLC or any of its officers, managers, owners, employees, agents or representatives are or can be held responsible or liable if you choose to refer to or use any of the information in this publication and the risk of doing so is solely and exclusively yours.

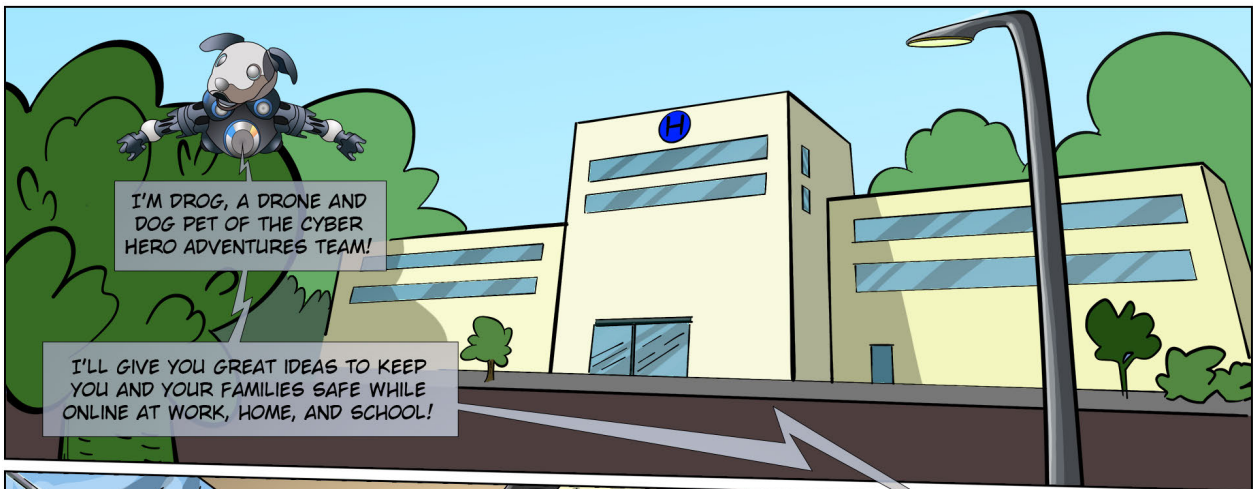
WWW.CYBERHERONETWORK.COM

Printed in
the USA

PART ONE

ENJOY THE NEXT CHAPTER OF THE INCREDIBLE, TRUE STORIES OF CYBER CRIME AND THE REAL-LIFE CYBER HEROES WHO KEEP US SAFE AT WORK, HOME AND SCHOOL!





I'M DROG, A DRONE AND DOG PET OF THE CYBER HERO ADVENTURES TEAM!

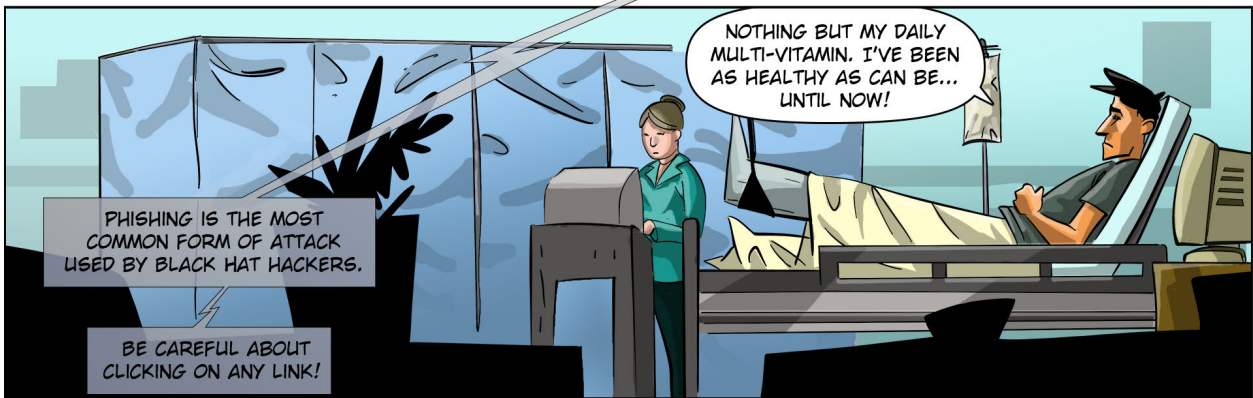
I'LL GIVE YOU GREAT IDEAS TO KEEP YOU AND YOUR FAMILIES SAFE WHILE ONLINE AT WORK, HOME, AND SCHOOL!



WE'RE GOING TO NEED A LIST OF ANY MEDICATIONS YOU TAKE...

MEDICAL PROVIDERS SHOULD ALWAYS WEAR A BADGE!

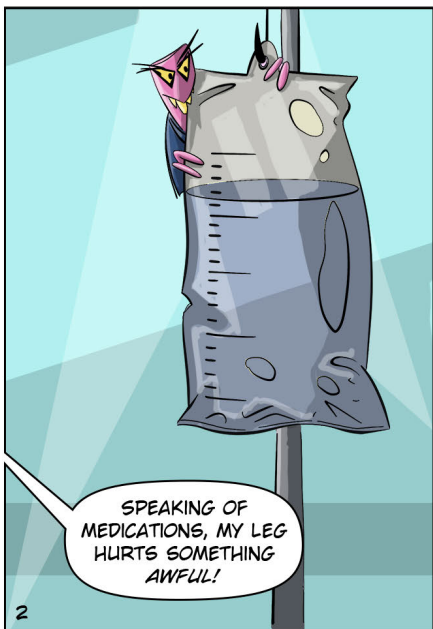
HOWEVER, CLEVER SOCIAL ENGINEERS USE A TECHNIQUE CALLED "TAILGATING" TO SNEAK INTO A SECURE AREA BY WALKING CLOSELY BEHIND A LEGITIMATE PERSON THROUGH SECURITY!



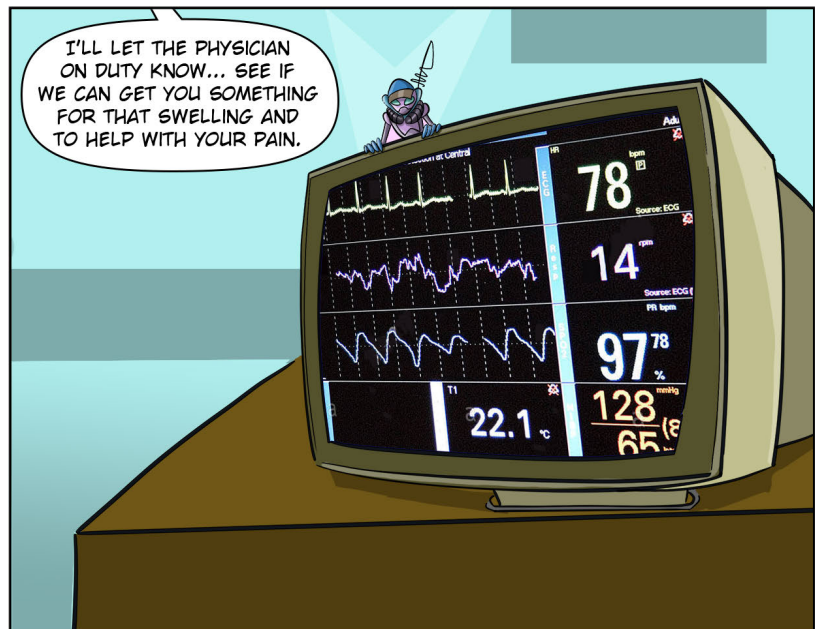
NOTHING BUT MY DAILY MULTI-VITAMIN. I'VE BEEN AS HEALTHY AS CAN BE... UNTIL NOW!

PHISHING IS THE MOST COMMON FORM OF ATTACK USED BY BLACK HAT HACKERS.

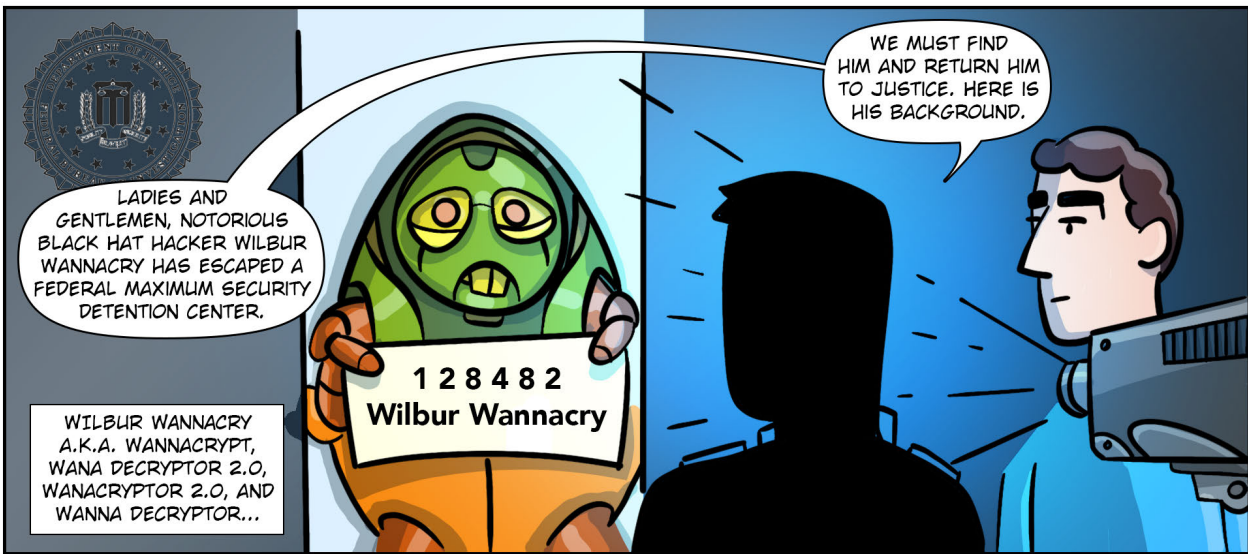
BE CAREFUL ABOUT CLICKING ON ANY LINK!



SPEAKING OF MEDICATIONS, MY LEG HURTS SOMETHING AWFUL!



I'LL LET THE PHYSICIAN ON DUTY KNOW... SEE IF WE CAN GET YOU SOMETHING FOR THAT SWELLING AND TO HELP WITH YOUR PAIN.

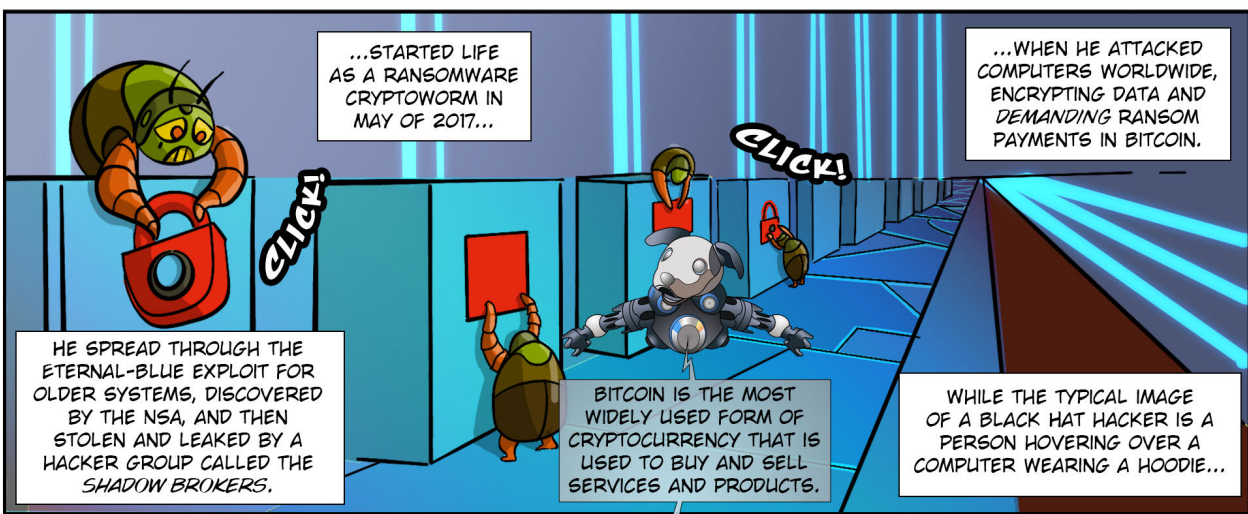


LADIES AND GENTLEMEN, NOTORIOUS BLACK HAT HACKER WILBUR WANNACRY HAS ESCAPED A FEDERAL MAXIMUM SECURITY DETENTION CENTER.

WE MUST FIND HIM AND RETURN HIM TO JUSTICE. HERE IS HIS BACKGROUND.

WILBUR WANNACRY A.K.A. WANNACRYPT, WANACRYPTOR 2.0, WANACRYPTOR 2.0, AND WANNA DECRYPTOR...

1 2 8 4 8 2
Wilbur Wannacry



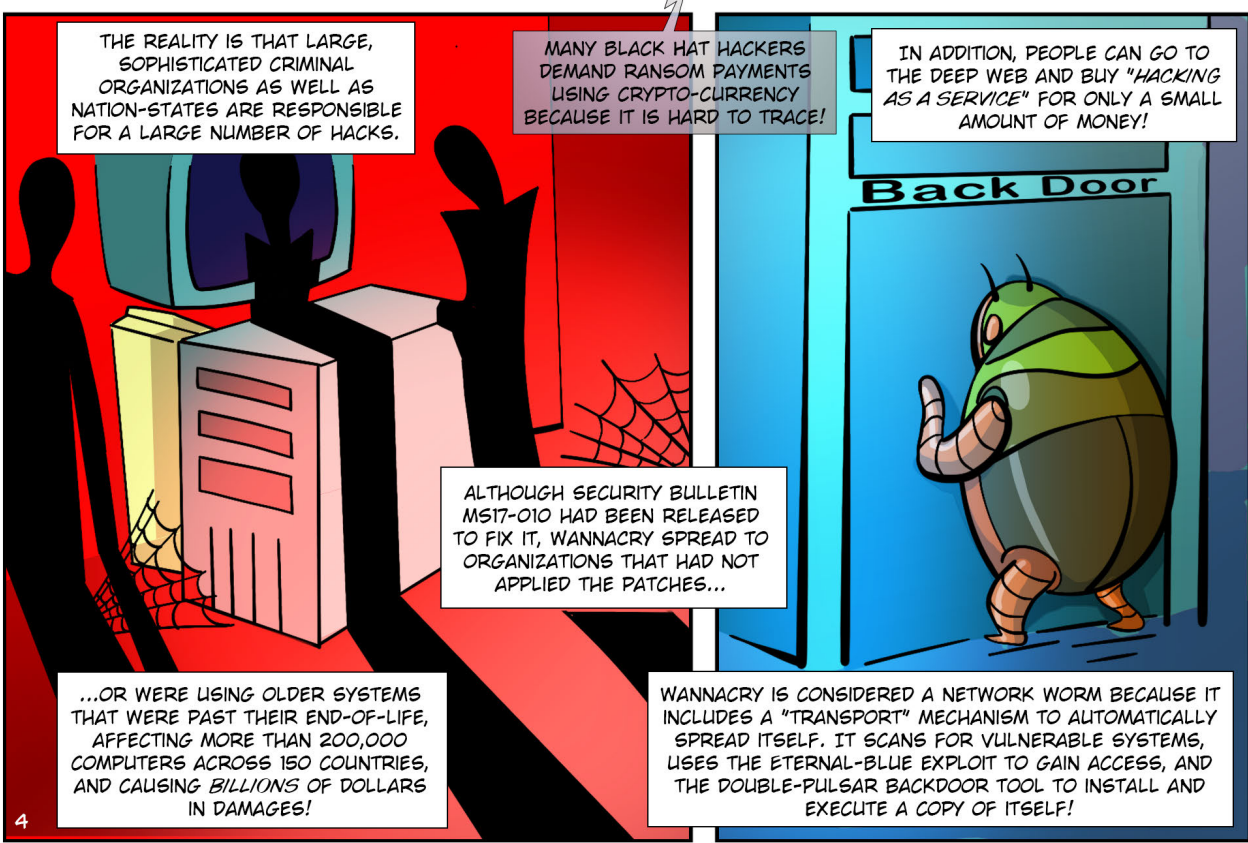
...STARTED LIFE AS A RANSOMWARE CRYPTOWORM IN MAY OF 2017...

...WHEN HE ATTACKED COMPUTERS WORLDWIDE, ENCRYPTING DATA AND DEMANDING RANSOM PAYMENTS IN BITCOIN.

HE SPREAD THROUGH THE ETERNAL-BLUE EXPLOIT FOR OLDER SYSTEMS, DISCOVERED BY THE NSA, AND THEN STOLEN AND LEAKED BY A HACKER GROUP CALLED THE SHADOW BROKERS.

BITCOIN IS THE MOST WIDELY USED FORM OF CRYPTOCURRENCY THAT IS USED TO BUY AND SELL SERVICES AND PRODUCTS.

WHILE THE TYPICAL IMAGE OF A BLACK HAT HACKER IS A PERSON HOVERING OVER A COMPUTER WEARING A HOODIE...



THE REALITY IS THAT LARGE, SOPHISTICATED AS WELL AS NATION-STATES ARE RESPONSIBLE FOR A LARGE NUMBER OF HACKS.

MANY BLACK HAT HACKERS DEMAND RANSOM PAYMENTS USING CRYPTO-CURRENCY BECAUSE IT IS HARD TO TRACE!

IN ADDITION, PEOPLE CAN GO TO THE DEEP WEB AND BUY "HACKING AS A SERVICE" FOR ONLY A SMALL AMOUNT OF MONEY!

ALTHOUGH SECURITY BULLETIN MS17-010 HAD BEEN RELEASED TO FIX IT, WANNACRY SPREAD TO ORGANIZATIONS THAT HAD NOT APPLIED THE PATCHES...

...OR WERE USING OLDER SYSTEMS THAT WERE PAST THEIR END-OF-LIFE, AFFECTING MORE THAN 200,000 COMPUTERS ACROSS 150 COUNTRIES, AND CAUSING BILLIONS OF DOLLARS IN DAMAGES!

WANNACRY IS CONSIDERED A NETWORK WORM BECAUSE IT INCLUDES A "TRANSPORT" MECHANISM TO AUTOMATICALLY SPREAD ITSELF. IT SCANS FOR VULNERABLE SYSTEMS, USES THE ETERNAL-BLUE EXPLOIT TO GAIN ACCESS, AND THE DOUBLE-PULSAR BACKDOOR TOOL TO INSTALL AND EXECUTE A COPY OF ITSELF!

LATER THAT NIGHT...

WE'VE HAD A GOOD HARVEST THIS MONTH!

WE'VE STOLEN A LOT OF DATA...

...AND WE HAVE SEVERAL LAYERS OF TREASURE HERE!

SO WE'LL EXECUTE THIS JOB IN SEVERAL PHASES...



Net		Amount of a Class	
16	14	255.255	1/8
32	25	255.255.255	1/4
64	25	255.192	1/2
128	25	55.128	

DARK WEB EVIL EMPIRE H.Q.

BELIEVE IT OR NOT, THERE IS A VERY SOPHISTICATED RATING SYSTEM...

FIRST WE'LL SELL OFF THE DATABASE OF 48,000 PATIENTS FROM THE CLINIC IN HINDSBORO.

WE CAN SELL THAT DATABASE AS "CERTIFIED FRESH" INFORMATION TO MULTIPLE BUYERS...

FOR ILLEGAL PRODUCTS AND SERVICES USED BY CRIMINALS.

HINDSBORO CLINICS & HOSPITALS
PATIENT DATABASE

USERNAME: _____
PASSWORD: _____

...IN A SHORT TIME FRAME, BEFORE THE DATA GETS ABUSED AND OVERUSED!

Search for anything | All Categories

Feedback forum > Feedback profile

profile

evilinfoempire (989 ☆)

Positive Feedback (last 12 months): 99.5%
[How is Feedback percentage calculated?]

Member since: Feb-05-06 in United States

WE GOTTA KEEP OUR RATING HIGH!

Detailed seller ratings (last 12 months)		
1 month	6 months	12 months
80	366	647
1	1	4
0	1	3

Criteria: Item as described (★★★★★), Communication (★★★★★)

seller | Search seller feedback | Feedback as a buyer | All Feedback | Feedback left for

THAT SHOULD PUT SOME SPENDING CASH IN OUR POCKETS RIGHT AWAY!

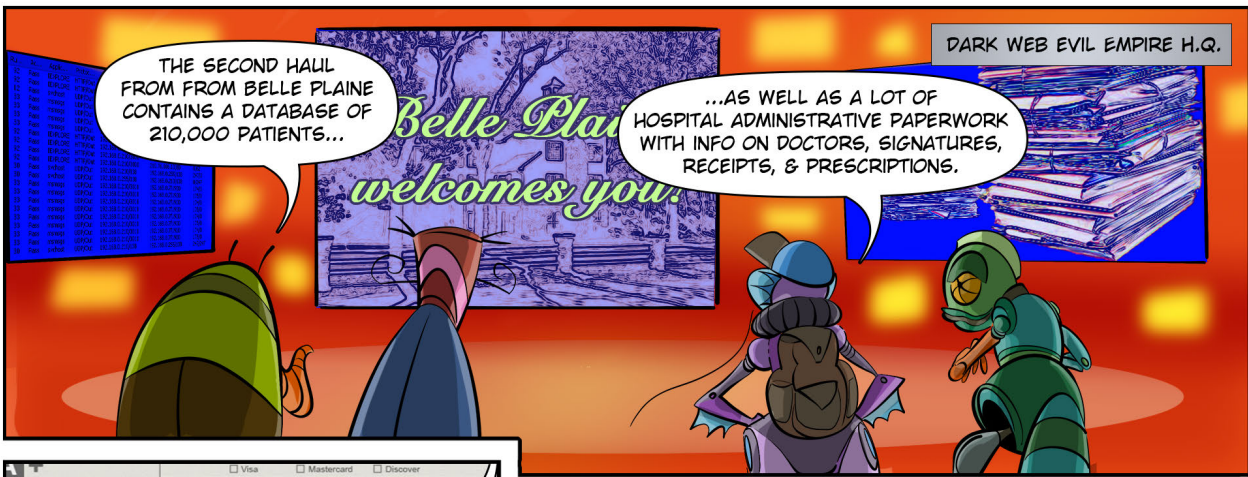
OF COURSE, WE'LL STRIP OUT THE PATIENT FINANCIAL INFORMATION AND SELL THAT SEPARATELY!

PERSONAL HEALTH INFORMATION (PHI) IS VERY VALUABLE TO CRIMINALS...

...WHO USE THE INFORMATION FOR SOCIAL ENGINEERING AND IDENTITY THEFT...

...INCLUDING INSURANCE COVERAGE, BANK ACCOUNT NUMBERS, AND A LOT MORE!

BANK



DARK WEB EVIL EMPIRE H.Q.

THE SECOND HALL FROM FROM BELLE PLAINE CONTAINS A DATABASE OF 210,000 PATIENTS...

...AS WELL AS A LOT OF HOSPITAL ADMINISTRATIVE PAPERWORK WITH INFO ON DOCTORS, SIGNATURES, RECEIPTS, & PRESCRIPTIONS.

ACME HealthCare
 123 Street Avenue
 Seattle, WA 98101
 Phone: 555 555 5555

Larry Jones
 456 Avenue Road
 Seattle, WA 98101

YOUR STATEMENT

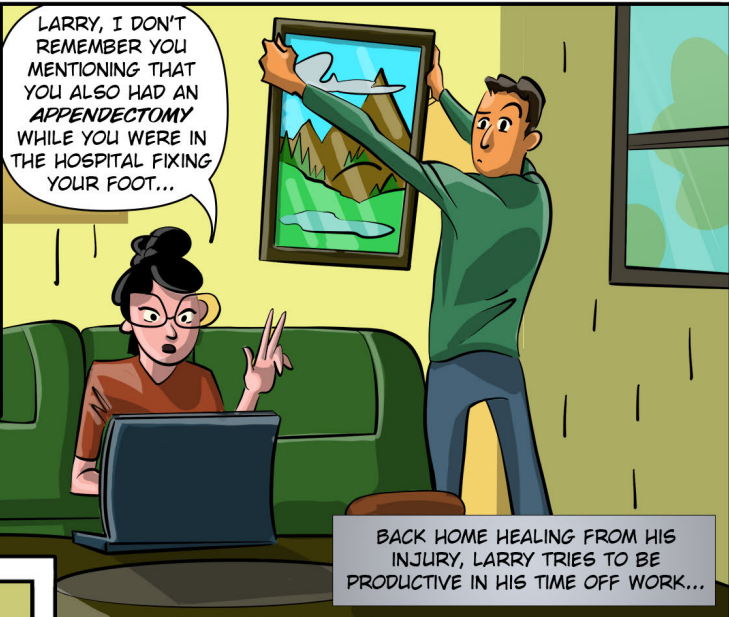
As an employee of ACME HealthCare appreciate the opportunity to care for you. Please verify the accuracy of the insurance information below and review your account summary and balance due. If you do not have health insurance, you may be eligible for a government-sponsored program. For information, please visit www.coverageforall.org.

Customer Service Representatives are available to assist you with any questions you have, applications for financial assistance and options for payment arrangements.

Statement Date: August 14, 2019 SHC Number: [REDACTED]

SUMMARY OF PATIENT SERVICES	INSURANCE INFORMATION
Radiology \$764.00	PRIMARY
Therapy Services \$754.00	SECONDARY
TOTAL CHARGES \$1,518.00	ACME may also pursue payment from a third party if permitted by Seattle Law. If we do, adjustments may no longer be applicable. We expect you to pay when allowed.

WE CAN USE THAT INFORMATION TO FORGE BILLS TO MEDICARE AND INSURANCE COMPANIES.



LARRY, I DON'T REMEMBER YOU MENTIONING THAT YOU ALSO HAD AN APPENDECTOMY WHILE YOU WERE IN THE HOSPITAL FIXING YOUR FOOT...

BACK HOME HEALING FROM HIS INJURY, LARRY TRIES TO BE PRODUCTIVE IN HIS TIME OFF WORK...

HealthCard

Larry Jones
 1234 5678 5678 9870

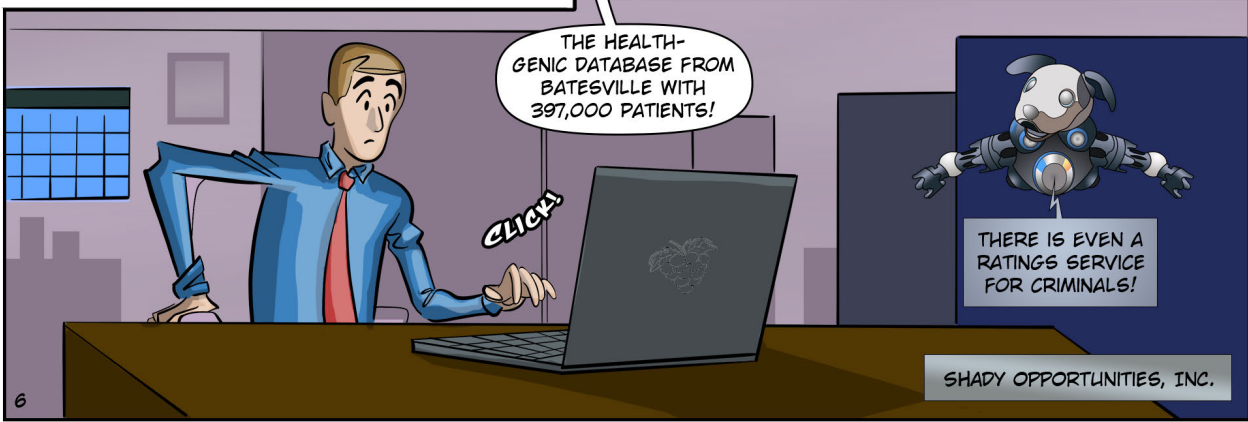


NOT THAT I'M AWARE OF!



BUT THEN THERE'S THE MOTHER LOAD!

DARK WEB EVIL EMPIRE H.Q.



THE HEALTH-GENIC DATABASE FROM BATESVILLE WITH 397,000 PATIENTS!

THERE IS EVEN A RATINGS SERVICE FOR CRIMINALS!

SHADY OPPORTUNITIES, INC.

Firefox File Edit View History Bookmarks Tools Window Help

https://evilinfoempire.org

Web History - Firefox

THIS ONE GOES TO ONLY ONE WELL-QUALIFIED BUYER FOR A QUARTER OF A MIL!

THIS HAUL IS HEAVY WITH IMPORTANT CHARACTERS WITH SOME FASCINATING MEDICAL HISTORIES...

This database contains over 397K patients and over 6700 medical personnel records!

Ownership of this database will be exclusive and only a single copy will be sold.

THIS HAS NOT BEEN LEAKED ANYWHERE AND IT HAS NOT YET BEEN ABUSED!

FOLKS, THIS TRULY IS THE MOTHERLODE!

GIAMME!

CLICK!

HealthGenic

THAT I'M SURE WOULD BE OF INTEREST TO SEVERAL ROGUE NATIONS LOOKING TO DIG UP LEVERAGE ON MUCKITY-MUCKS!

ROGUE NATION WAR ROOM

MEDICAL HISTORY

Patient Name: Jorge Villanova Nickname: n/a Age: 46

Name of Physician/Provider: _____ Specialty: _____

Most recent physical examination: _____

Blood Fax Print

26. osteoporosis/osteopenia (e.g. taking hydrocortisone) YES NO
 27. arthritis/rheumatoid arthritis/psoriasis YES NO
 28. diabetes YES NO
 29. cardiac issues YES NO
 30. stroke YES NO
 31. kidney issues YES NO
 32. respiratory disorders (Asthma/COPD/emphysema) YES NO
 33. hypertension and related YES NO
 34. epilepsy or seizure in the past YES NO
 35. mental, psychiatric, or drug use YES NO
 36. HIV/AIDS YES NO
 37. cancer (diagnosed/previously) YES NO
 38. transfusion YES NO
 39. transfusion-transmitted infections YES NO
 40. organ donation YES NO
 41. organ transplant YES NO
 42. sexually transmitted by any other than YES NO
 43. history of other genital health in the last 24 hours (e.g. chlamydia, gonorrhea, or syphilis) YES NO
 44. taking antibiotics for urinary tract infection (e.g. Nitrofurantoin) YES NO
 45. taking drugs for psychiatric treatment YES NO
 46. other self-medication YES NO
 47. over-the-counter medications YES NO
 48. alcohol consumption YES NO
 49. tobacco use YES NO
 50. steroid use (oral, inhaled, topical, or injected) YES NO
 51. immunosuppressant medications YES NO
 52. immunodeficiency YES NO
 53. high cholesterol or taking statins YES NO
 54. diabetes (Type 1 or 2) YES NO
 55. anorexia/bulimia YES NO
 56. alcohol use (acute or chronic) YES NO
 57. kidney problems YES NO

Indicate any medical history, including signs, symptoms, or other factors that may possibly affect your dental treatment. (e.g. braces, Colgate treatment, etc.)

Drug: _____ Purpose: _____ Drug: _____ Purpose: _____

ALL: For an additional sheet if you are taking more than 2 medications

PLEASE ADVISE US IN THE FUTURE OF ANY CHANGE IN YOUR MEDICAL HISTORY OR ANY MEDICATIONS YOU MAY BE TAKING.

Patient's Signature: _____ Date: _____
 Doctor's Signature: _____ Date: _____

IMPORTANT PEOPLE SOLD SEPARATELY!

DARK WEB EVIL EMPIRE H.Q.

I'LL CONTACT THE USUAL VILLAINS WHO BUY OUR STOLEN INFORMATION!

BUT WE'RE NOT DONE YET MY FRIENDS... NOT BY A LONG SHOT!

WE WERE ABLE TO HAUL-IN THESE MASS DUMPS BECAUSE THE HOSPITALS HAD NO SYSTEMS IN-PLACE TO IDENTIFY THREATS IN REAL-TIME.

AND... WE HAVE ONE MORE TRICK UP OUR SLEEVE!



SONNY HOOKED US UP WITH A PERSON ON THE INSIDE TO CREATE FAKE CARE CREDIT ACCOUNTS...

Hospital/Physician Statement

For more information, request an itemized statement, call 1-2367-3309 or (844) 887-5309. patientstatements@cuhsd.org
 Check if address/insurance changes are on back

Addresssee Page 1 of 1

Larry Jones
123 Drury Lane
Outer Space, 12345

5678901234 5678901234 5678901234 5678901234 5678901234

Account Code: 123-ABC-456 Please detach and return top portion with pay

PIN	Account Name	Statement Date	Due Date
123456	Test Patient	04/05/2019	04/28/2019

Service Description	Status	Charges	Payments/Adjustments	Patie Balan
Physician Charges				
Patient: Larry Jones				
Account #: 123456789012345				
Provider: Health Genic				
Date of Service: 04/05/2019				
Location: INSURANCE PAYMENTS/ADJUSTMENTS				
Payment Due:	Current	\$145.00	-\$130.62	

Reverse side for Check payment info, and Financial Assistance Policies.

QUICK PAY

SCAN

Pay Online: <https://upmc.myssecurebill.com/myEasyMatchCode:123-ABC-456>

Physician Total \$145.00
 Hospital Total \$130.62
 Subtotal \$14.38

AMOUNT DUE: \$14.38

...THAT WILL PAY OUT ON OUR FAKE INVOICES!

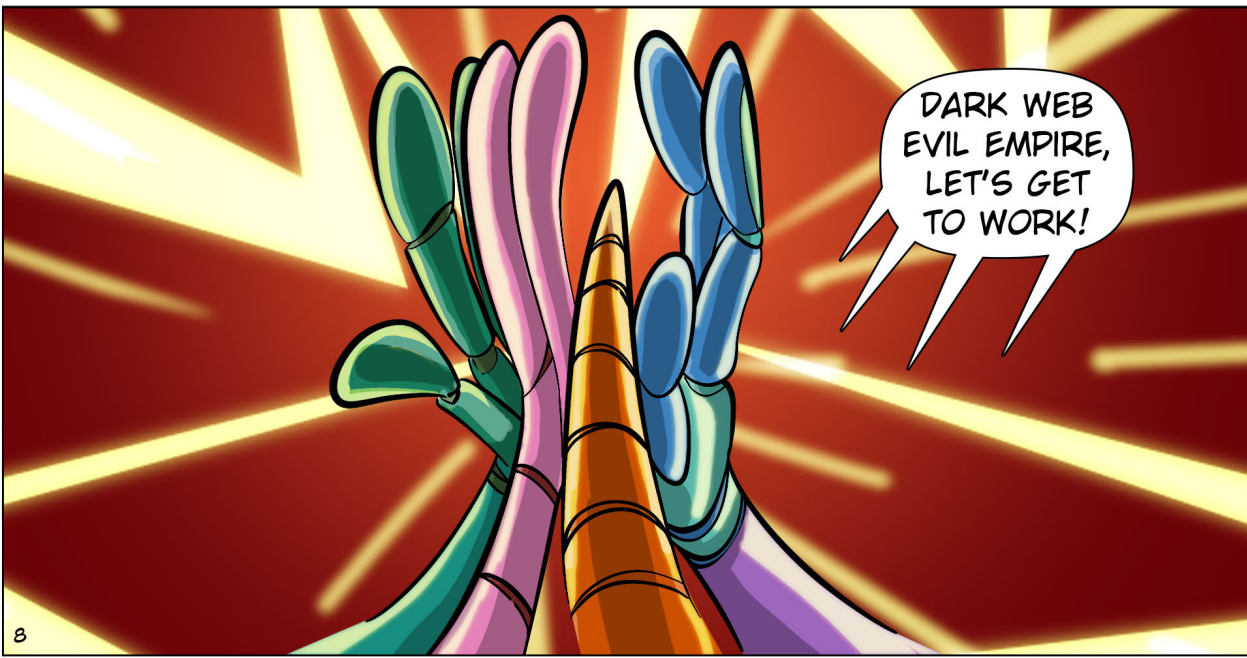


LADIES AND GENTS, WE HAVE TO STRIKE WHILE THE IRON IS HOT!

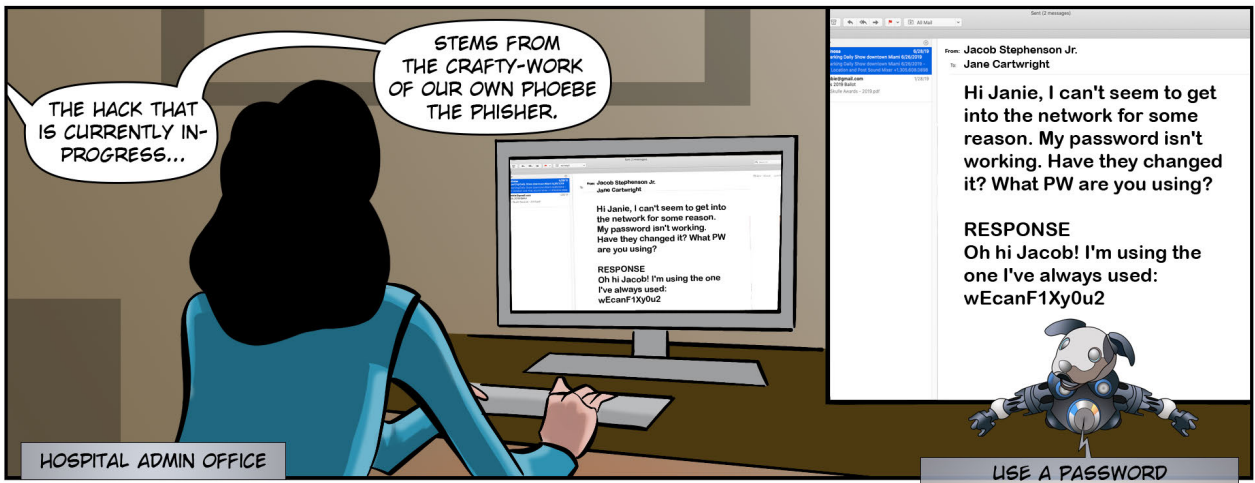
THE WHITE HATS ARE BOUND TO CATCH UP SOONER OR LATER.

ONCE NEWS GETS OUT, LOTS OF FACILITIES WILL BE LOOKING TO BEEF UP THEIR CYBER SECURITY.

LET'S MILK THIS HAUL FOR ALL IT'S GOT!



DARK WEB EVIL EMPIRE, LET'S GET TO WORK!



THE HACK THAT IS CURRENTLY IN-PROGRESS...

STEMS FROM THE CRAFTY-WORK OF OUR OWN PHOEBE THE PHISHER.

From: Jacob Stephenson Jr.
To: Jane Cartwright

Hi Janie, I can't seem to get into the network for some reason. My password isn't working. Have they changed it? What PW are you using?

RESPONSE
Oh hi Jacob! I'm using the one I've always used:
wEcanF1Xy0u2

From: Jacob Stephenson Jr.
To: Jane Cartwright

Hi Janie, I can't seem to get into the network for some reason. My password isn't working. Have they changed it? What PW are you using?

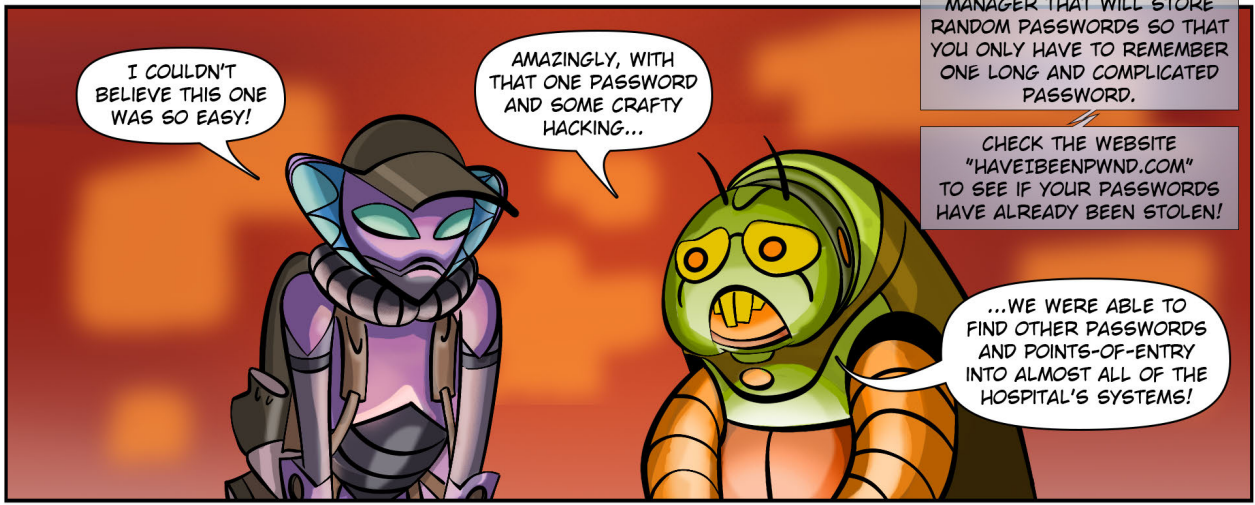
RESPONSE
Oh hi Jacob! I'm using the one I've always used:
wEcanF1Xy0u2



HOSPITAL ADMIN OFFICE

USE A PASSWORD MANAGER THAT WILL STORE RANDOM PASSWORDS SO THAT YOU ONLY HAVE TO REMEMBER ONE LONG AND COMPLICATED PASSWORD.

CHECK THE WEBSITE "HAVEIBEENPWND.COM" TO SEE IF YOUR PASSWORDS HAVE ALREADY BEEN STOLEN!



I COULDN'T BELIEVE THIS ONE WAS SO EASY!

AMAZINGLY, WITH THAT ONE PASSWORD AND SOME CRAFTY HACKING...

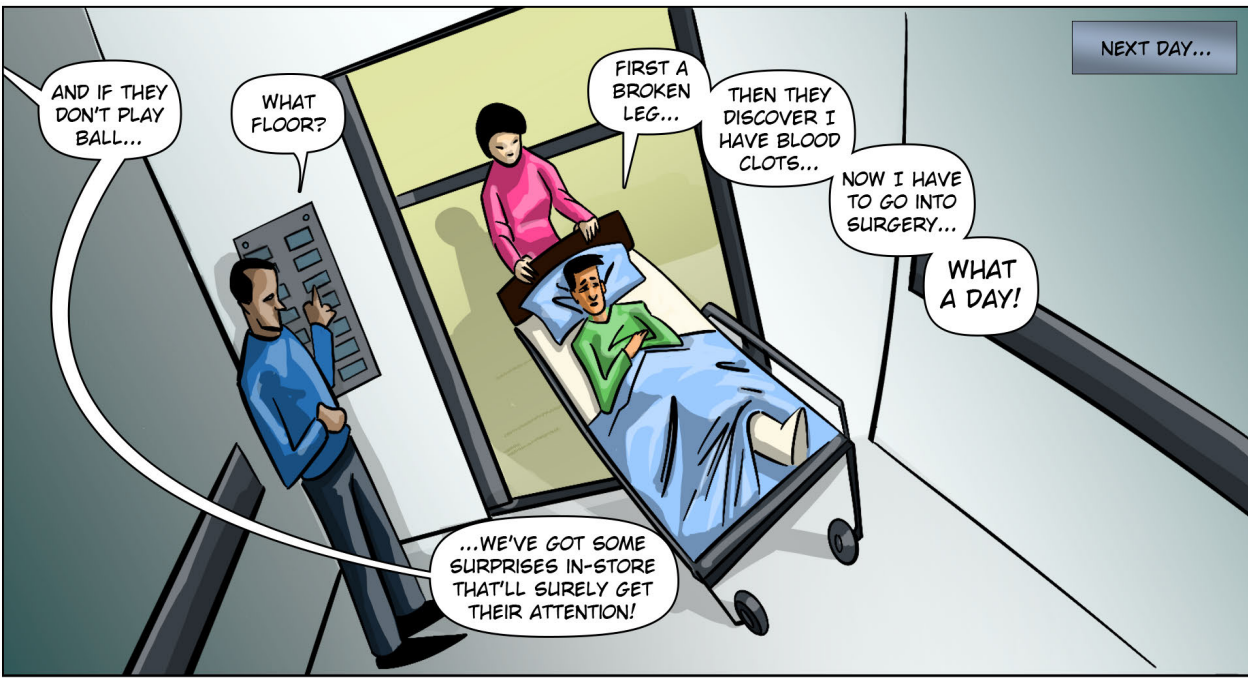
...WE WERE ABLE TO FIND OTHER PASSWORDS AND POINTS-OF-ENTRY INTO ALMOST ALL OF THE HOSPITAL'S SYSTEMS!



OH NO! WHAT IS THIS?

Your data has been locked and is being stored safely.
You have 24 hours to pay US\$80,000.00 in Bitcoin crypto-currency.
After 24 hours, you must pay US\$250,000.00.
After 48 hours, your data will be destroyed.
Click [here](#) for Bitcoin instructions.

NEXT DAY...



AND IF THEY DON'T PLAY BALL...

WHAT FLOOR?

FIRST A BROKEN LEG...

THEN THEY DISCOVER I HAVE BLOOD CLOTS...

NOW I HAVE TO GO INTO SURGERY...

WHAT A DAY!

...WE'VE GOT SOME SURPRISES IN-STORE THAT'LL SURELY GET THEIR ATTENTION!



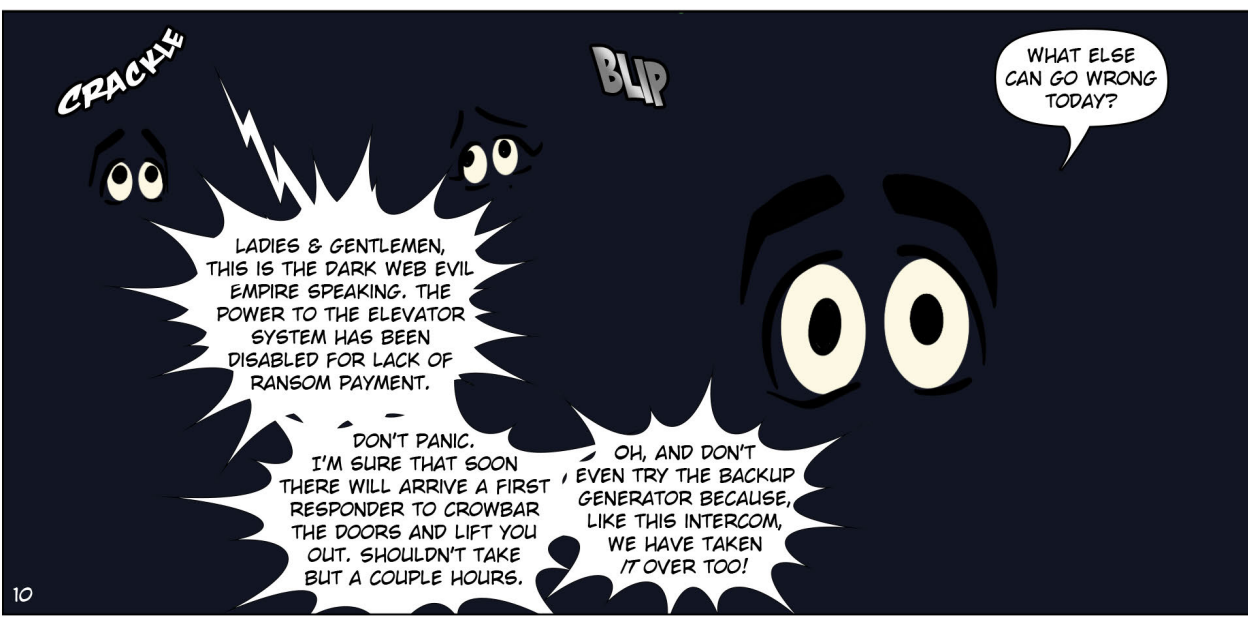
I'M REALLY SCARED ABOUT GOING INTO SURGERY.

DON'T WORRY MR. JONES, EVERYTHING WILL BE OKA...



WHAT THE?

BZZT BZZT CHINK



WHAT ELSE CAN GO WRONG TODAY?

LADIES & GENTLEMEN, THIS IS THE DARK WEB EVIL EMPIRE SPEAKING. THE POWER TO THE ELEVATOR SYSTEM HAS BEEN DISABLED FOR LACK OF RANSOM PAYMENT.

DON'T PANIC. I'M SURE THAT SOON THERE WILL ARRIVE A FIRST RESPONDER TO CROWBAR THE DOORS AND LIFT YOU OUT. SHOULDN'T TAKE BUT A COUPLE HOURS.

OH, AND DON'T EVEN TRY THE BACKUP GENERATOR BECAUSE, LIKE THIS INTERCOM, WE HAVE TAKEN IT OVER TOO!

PART TWO
MEET THE CYBER
HERO ADVENTURES'
REAL-LIFE HEROES!

YOU BETTER STOP
PICKING ON SUSAN IF
YOU KNOW WHAT'S
GOOD FOR YOU!

YOU'LL BE
BROUGHT UP ON
ASSAULT CHARGES
AND BE KICKED OUT
OF SCHOOL!

FROM A YOUNG AGE, JUSTINA JASCO
DEFENDED THE DEFENSELESS.

TWELVE YEARS LATER...

SHE SET OUT TO LEARN ALL SHE COULD ABOUT
THE JUDICIAL SYSTEM AND RECEIVED HER JURIS
DOCTOR DEGREE SUMMA CUM LAUDE.

OUT OF LAW SCHOOL,
JUSTINA BECAME A
PUBLIC DEFENDER...

DEFENDING THE RIGHTS
OF THE ACCUSED.

AFTER A RANSOMWARE ATTACK CRIPPLED
THE PUBLIC DEFENDER'S OFFICES...

...SHE GREW INTERESTED IN
CYBER CRIME AND DECIDED TO
JOIN THE STATE ATTORNEY'S
OFFICE AS A PROSECTOR.

AFTER WORKING TIRELESSLY WITH
LAW ENFORCEMENT TO PUT CYBER
CRIMINALS BEHIND BARS...

FOR THE FIRST TIME EVER
JUSTINA WAS BEGINNING
TO LOSE HOPE.

HELLO, THIS
IS DR. G...

ACQUITTED

RING!
RING!

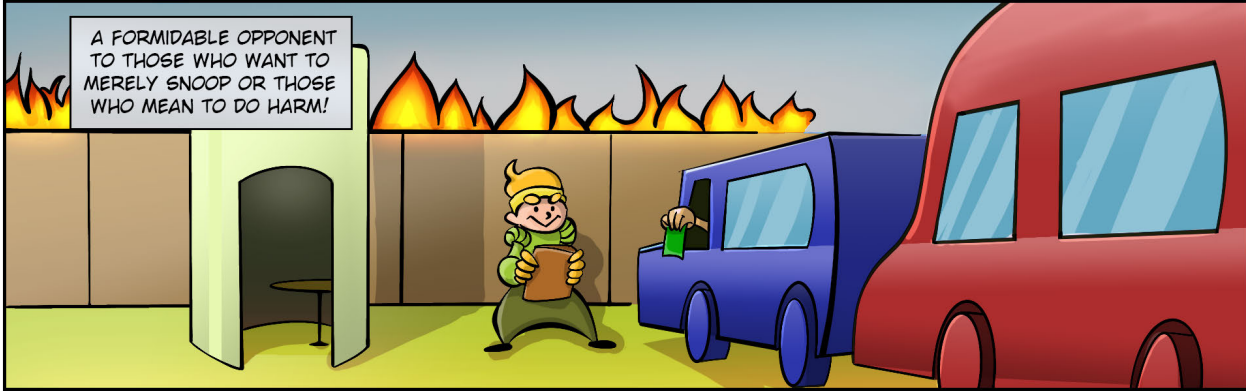
THAT IS, UNTIL THE CYBER HERO
ADVENTURE TEAM CALLED!

FINN THE FIREWALL
LOVES RULES...
HE LIVES BY THEM!

A FIREWALL IS ONE OF
THE MOST CHALLENGING
OBSTACLES THAT BLACK HAT
HACKERS HAVE TO BYPASS...



A FORMIDABLE OPPONENT
TO THOSE WHO WANT TO
MERELY SNOOP OR THOSE
WHO MEAN TO DO HARM!



FINN WORKS IN
CONJUNCTION WITH
OTHER TEAMMATES TO
FORM A SECURE DATA
PERIMETER...

SO THE SDP HAS
BECOME MUCH MORE
DIFFICULT TO DEFEND.

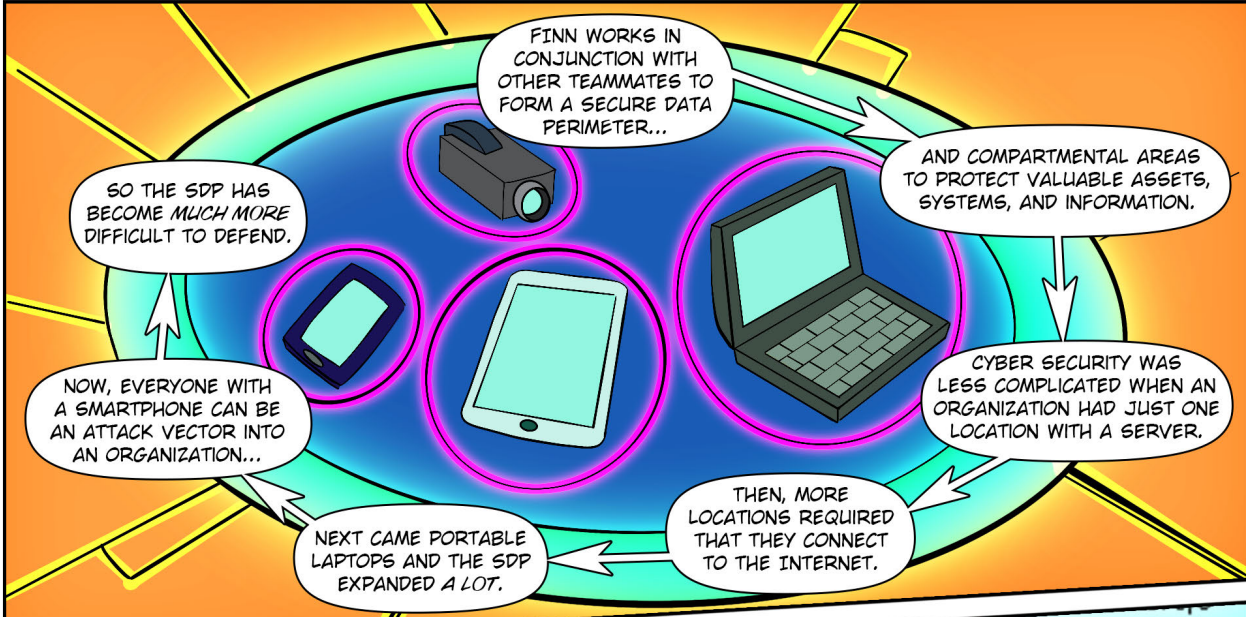
AND COMPARTMENTAL AREAS
TO PROTECT VALUABLE ASSETS,
SYSTEMS, AND INFORMATION.

NOW, EVERYONE WITH
A SMARTPHONE CAN BE
AN ATTACK VECTOR INTO
AN ORGANIZATION...

CYBER SECURITY WAS
LESS COMPLICATED WHEN AN
ORGANIZATION HAD JUST ONE
LOCATION WITH A SERVER.

NEXT CAME PORTABLE
LAPTOPS AND THE SDP
EXPANDED A LOT.

THEN, MORE
LOCATIONS REQUIRED
THAT THEY CONNECT
TO THE INTERNET.

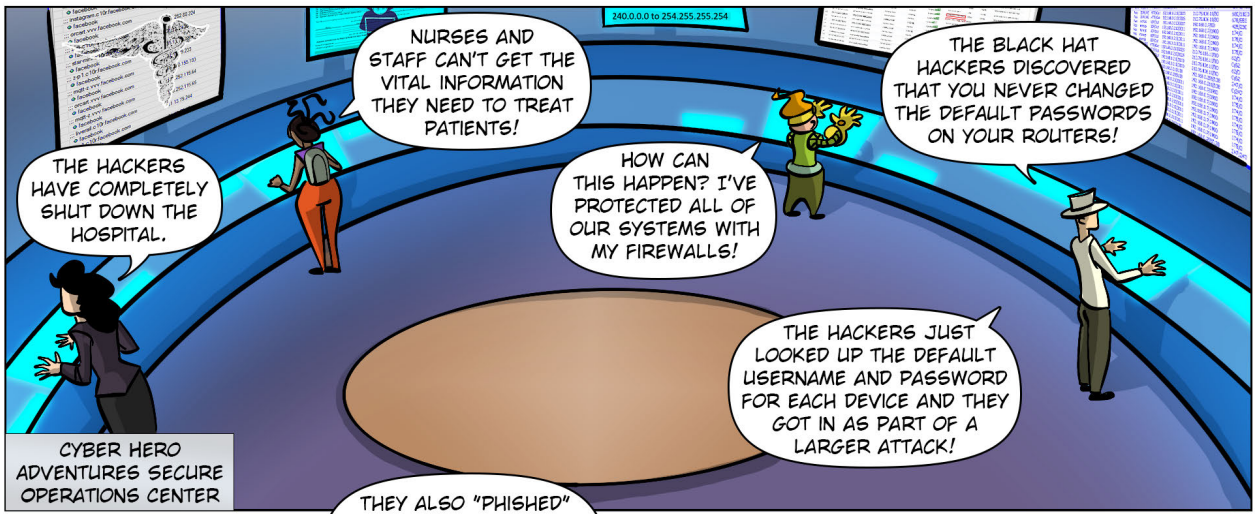


HIS ONLY WEAKNESS
IS STALE, OLD RULES.

IN A CONSTANTLY
CHANGING CYBER
LANDSCAPE, FINN MUST
ENSURE THAT HIS RULES
ARE ALWAYS UP-TO-DATE.

92	Pass	mmsgs	UDP/Out	192.168.0.210/3011	192.168.0.210/3011	174/0
92	Pass	IEXPLORE	HTTP/Out	192.168.0.210/3029	192.168.0.210/3029	276/10
30	Pass	svchost	UDP/Out	192.168.0.210/138	192.168.0.210/138	0/247
30	Pass	svchost	UDP/Out	192.168.0.255/138	192.168.0.255/138	174/0
33	Pass	mmsgs	UDP/Out	192.168.0.210/3011	192.168.0.7/1900	175/0
33	Pass	mmsgs	UDP/Out	192.168.0.210/3011	192.168.0.7/1900	174/0
33	Pass	mmsgs	UDP/Out	192.168.0.210/3011	192.168.0.7/1900	175/0
33	Pass	mmsgs	UDP/Out	192.168.0.210/3011	192.168.0.7/1900	174/0
33	Pass	mmsgs	UDP/Out	192.168.0.210/3011	192.168.0.7/1900	175/0
33	Pass	mmsgs	UDP/Out	192.168.0.210/3011	192.168.0.7/1900	174/0
33	Pass	mmsgs	UDP/Out	192.168.0.210/3011	192.168.0.7/1900	175/0
33	Pass	mmsgs	UDP/Out	192.168.0.210/3011	192.168.0.7/1900	174/0
30	Pass	svchost	UDP/Out	192.168.0.210/138	192.168.0.255/138	276/10

AND ONE STEP AHEAD
OF HIS ADVERSARIES!



THE HACKERS HAVE COMPLETELY SHUT DOWN THE HOSPITAL.

NURSES AND STAFF CAN'T GET THE VITAL INFORMATION THEY NEED TO TREAT PATIENTS!

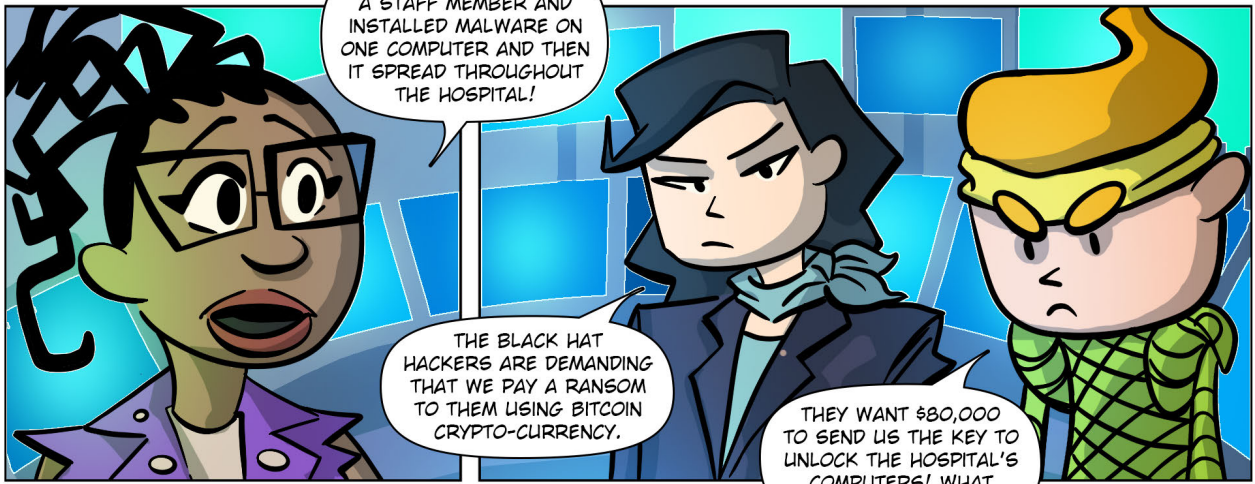
HOW CAN THIS HAPPEN? I'VE PROTECTED ALL OF OUR SYSTEMS WITH MY FIREWALLS!

THE BLACK HAT HACKERS DISCOVERED THAT YOU NEVER CHANGED THE DEFAULT PASSWORDS ON YOUR ROUTERS!

THE HACKERS JUST LOOKED UP THE DEFAULT USERNAME AND PASSWORD FOR EACH DEVICE AND THEY GOT IN AS PART OF A LARGER ATTACK!

CYBER HERO ADVENTURES SECURE OPERATIONS CENTER

THEY ALSO "PHISHED" A STAFF MEMBER AND INSTALLED MALWARE ON ONE COMPUTER AND THEN IT SPREAD THROUGHOUT THE HOSPITAL!



THE BLACK HAT HACKERS ARE DEMANDING THAT WE PAY A RANSOM TO THEM USING BITCOIN CRYPTO-CURRENCY.

THEY WANT \$80,000 TO SEND US THE KEY TO UNLOCK THE HOSPITAL'S COMPUTERS! WHAT SHOULD WE DO?



WE HAVE 3 CHOICES:
1. USE OUR BACKUP DATA AND HOPE THAT THE BACKUP WAS NOT AFFECTED IN THE ATTACK.
2. SWITCH FROM COMPUTERS TO PAPER GOING FORWARD...

YOU'RE JOKING RIGHT?

OR THREE...

TO REGAIN ACCESS TO OUR COMPUTERS...

PAY THE RANSOM AND HOPE THAT THE CRIMINALS ACTUALLY SEND US THE CORRECT KEY!

WE HAVE TO CONTAIN THE THREAT AND FIND OUT WHAT OTHER SYSTEMS HAVE BEEN AFFECTED... FAST!

IT'S GOING TO TAKE A LOT OF TIME TO RECOVER.

AND TO AVOID FUTURE ATTACKS...



THE F.B.I. RECOMMENDS THAT WE NOT PAY THE RANSOM...

BECAUSE THE CRIMINALS JUST GET MORE MONEY TO CONTINUE THEIR ATTACKS.

WELL, REGARDLESS OF WHAT WE DECIDE...

IN ADDITION TO CAUSING HARM TO OUR PATIENTS...

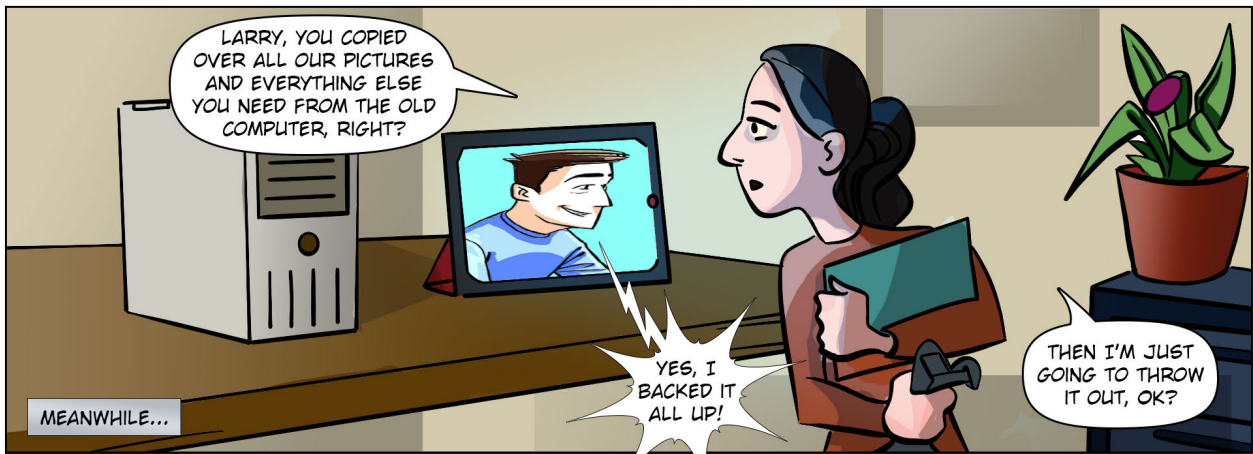
THIS IS GOING TO COST A LOT OF MONEY!

WE'LL NEED TO BRING IN CYBER SECURITY EXPERTS AND ADDITIONAL LEGAL HELP.

WITH STATE-OF-THE-ART EQUIPMENT!

WE NEED TO REPLACE OUR OUT-DATED LEGACY SYSTEMS...

KEEP READING TO LEARN HOW TO SAFELY DISPOSE OF OLD COMPUTERS!

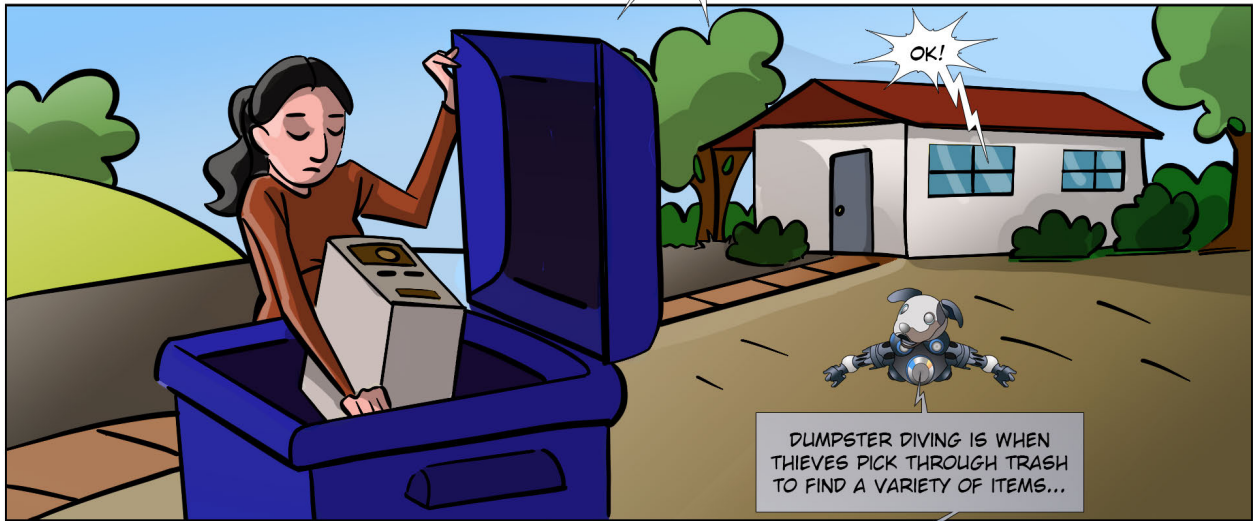


LARRY, YOU COPIED OVER ALL OUR PICTURES AND EVERYTHING ELSE YOU NEED FROM THE OLD COMPUTER, RIGHT?

MEANWHILE...

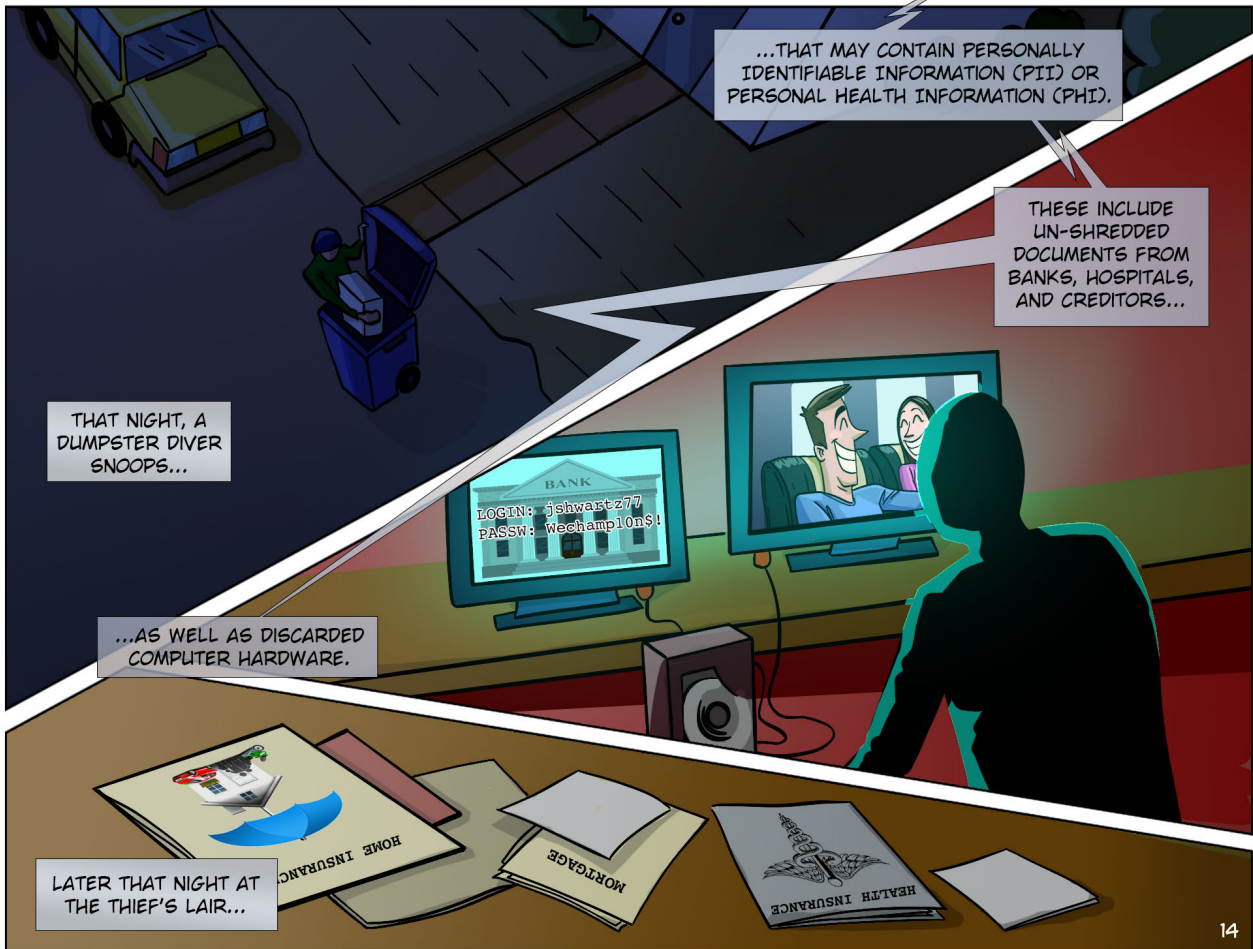
YES, I BACKED IT ALL UP!

THEN I'M JUST GOING TO THROW IT OUT, OK?



OK!

DUMPSTER DIVING IS WHEN THIEVES PICK THROUGH TRASH TO FIND A VARIETY OF ITEMS...



...THAT MAY CONTAIN PERSONALLY IDENTIFIABLE INFORMATION (PII) OR PERSONAL HEALTH INFORMATION (PHI).

THESE INCLUDE UN-SHREDDED DOCUMENTS FROM BANKS, HOSPITALS, AND CREDITORS...

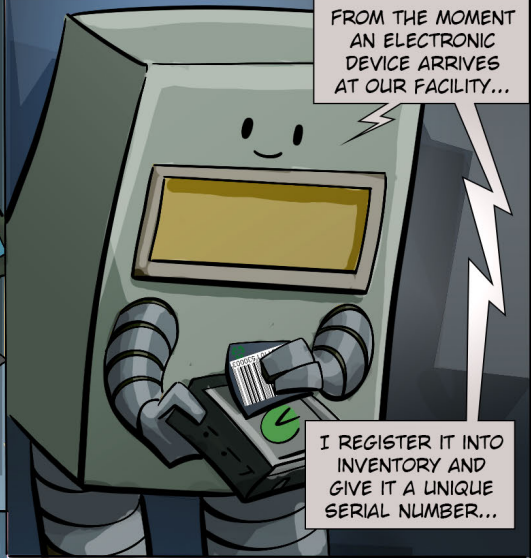
THAT NIGHT, A DUMPSTER DIVER SNOOPS...

...AS WELL AS DISCARDED COMPUTER HARDWARE.

LATER THAT NIGHT AT THE THIEF'S LAIR...

AS THE NUMBER OF OUTDATED ELECTRONIC DEVICES SOARS, WE MUST PAY CLOSER ATTENTION TO HOW WE DISPOSE-OF AND RECYCLE THESE DEVICES, WHICH CONTAIN SO MUCH PERSONAL HEALTH INFORMATION (PHI)!

FROM THE MOMENT AN ELECTRONIC DEVICE ARRIVES AT OUR FACILITY...



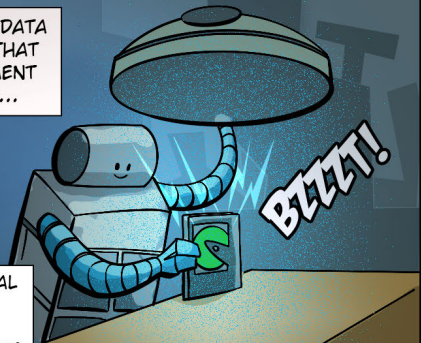
WE HAVE TO MAKE SURE THAT WE ACCOMPLISH OUR MISSION TO PERMANENTLY DESTROY ALL THE DATA ON THESE DEVICES, SO NONE OF IT ENDS UP IN THE WRONG HANDS!

I REGISTER IT INTO INVENTORY AND GIVE IT A UNIQUE SERIAL NUMBER...

[HTTPS://ERIDIRECT.COM](https://eridirect.com)

...WHICH ALLOWS US TO TRACK IT EVERY STEP OF THE WAY, USING OUR ONLINE TRACKER, TO ITS FINAL DISPOSITION...

WE EMPLOY A STRICT DATA SECURITY PROCESS THAT MEETS THE DEPARTMENT OF DEFENSE (DOD)...



AND THE NATIONAL INSTITUTE OF STANDARDS & TECHNOLOGY (NIST) STANDARDS.

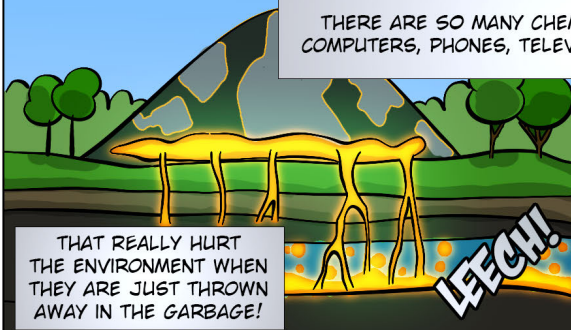
WE ARE ALSO AAA-CERTIFIED BY NAID, WHICH MONITORS THE STRICTEST STANDARDS OF EFFECTIVE AND RESPONSIBLE DATA DESTRUCTION IN THE WORLD TODAY.

THIS ENSURES THAT DATA IS NEVER COMPROMISED AND IS COMPLETELY DESTROYED VIA SOFTWARE, DEGAUSSING, OR SHREDDING.

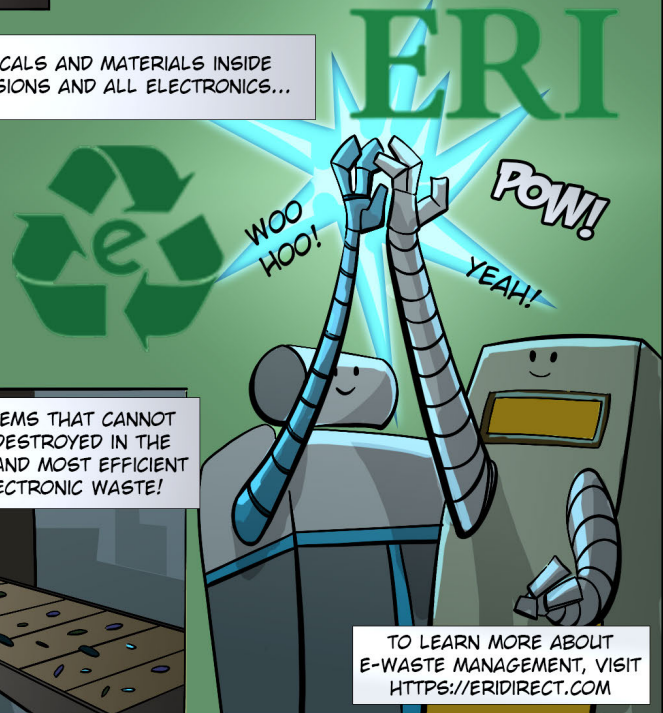


...WHETHER THE DEVICE IS RECONDITIONED, SHREDDED, OR HARVESTED FOR PARTS.

THERE ARE SO MANY CHEMICALS AND MATERIALS INSIDE COMPUTERS, PHONES, TELEVISIONS AND ALL ELECTRONICS...



THAT REALLY HURT THE ENVIRONMENT WHEN THEY ARE JUST THROWN AWAY IN THE GARBAGE!

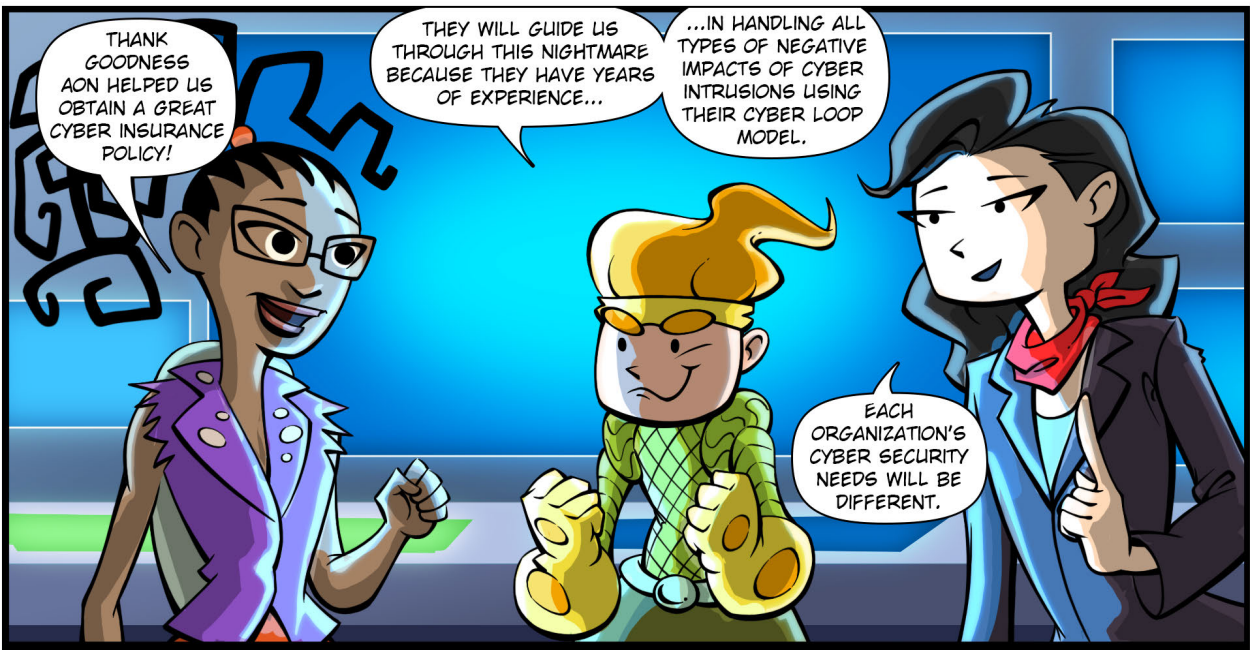


AT OUR FACILITY, ITEMS THAT CANNOT BE RE-USED ARE DESTROYED IN THE WORLD'S LARGEST AND MOST EFFICIENT SHREDDER OF ELECTRONIC WASTE!



THEN SORTED INTO RAW COMMODITIES, 100% OF WHICH ARE RECYCLED SO NOTHING ENDS UP IN A LANDFILL!

TO LEARN MORE ABOUT E-WASTE MANAGEMENT, VISIT [HTTPS://ERIDIRECT.COM](https://eridirect.com)



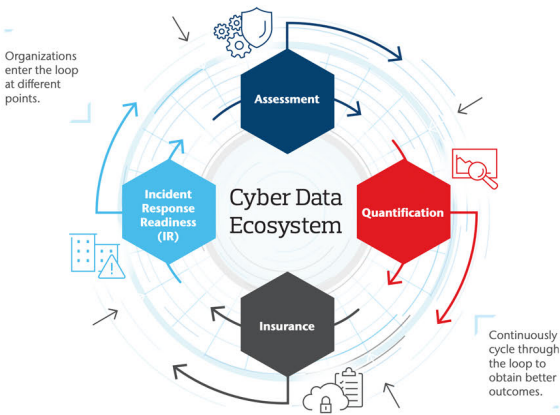
THANK GOODNESS AON HELPED US OBTAIN A GREAT CYBER INSURANCE POLICY!

THEY WILL GUIDE US THROUGH THIS NIGHTMARE BECAUSE THEY HAVE YEARS OF EXPERIENCE...

...IN HANDLING ALL TYPES OF NEGATIVE IMPACTS OF CYBER INTRUSIONS USING THEIR CYBER LOOP MODEL.

EACH ORGANIZATION'S CYBER SECURITY NEEDS WILL BE DIFFERENT.

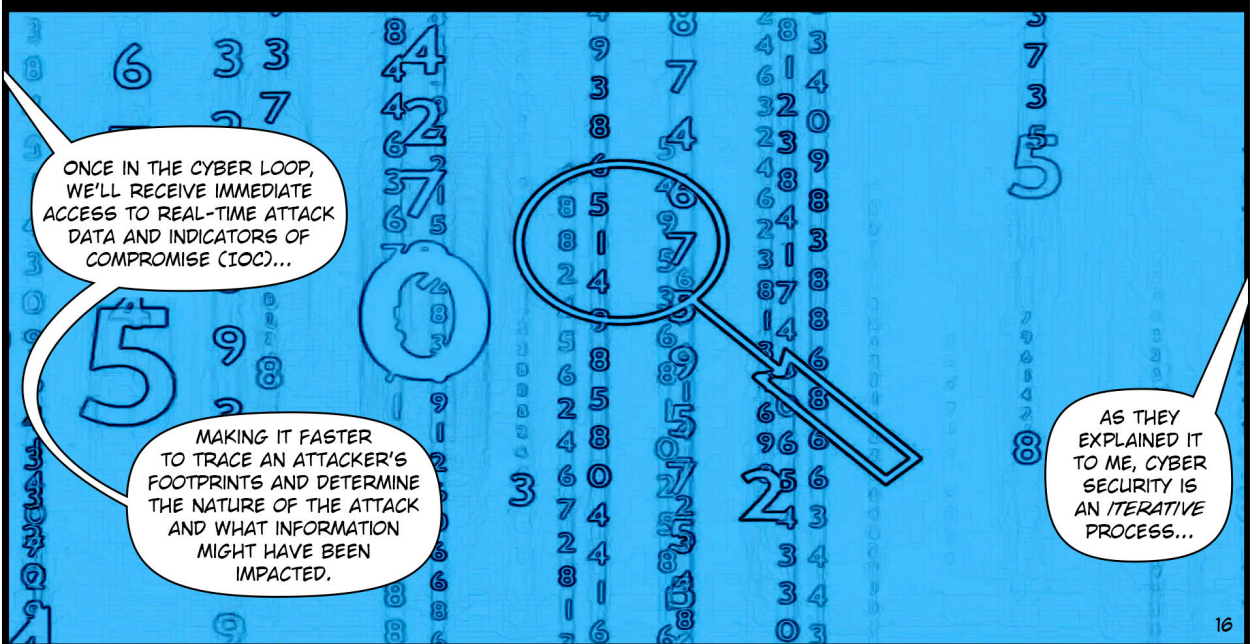
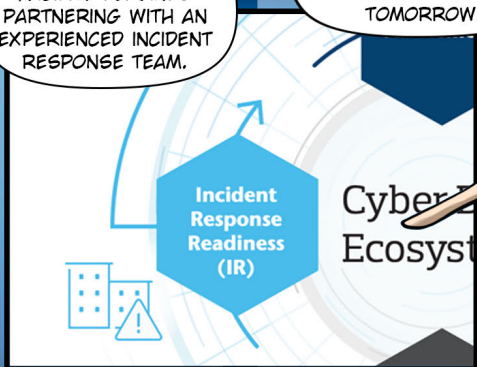
The Cyber Loop



[HTTPS://WWW.AON.COM/CYBER-SOLUTIONS](https://www.aon.com/cyber-solutions)

THIS SIGNIFICANT BREACH OF A MEDICAL FACILITY DEMANDS PARTNERING WITH AN EXPERIENCED INCIDENT RESPONSE TEAM.

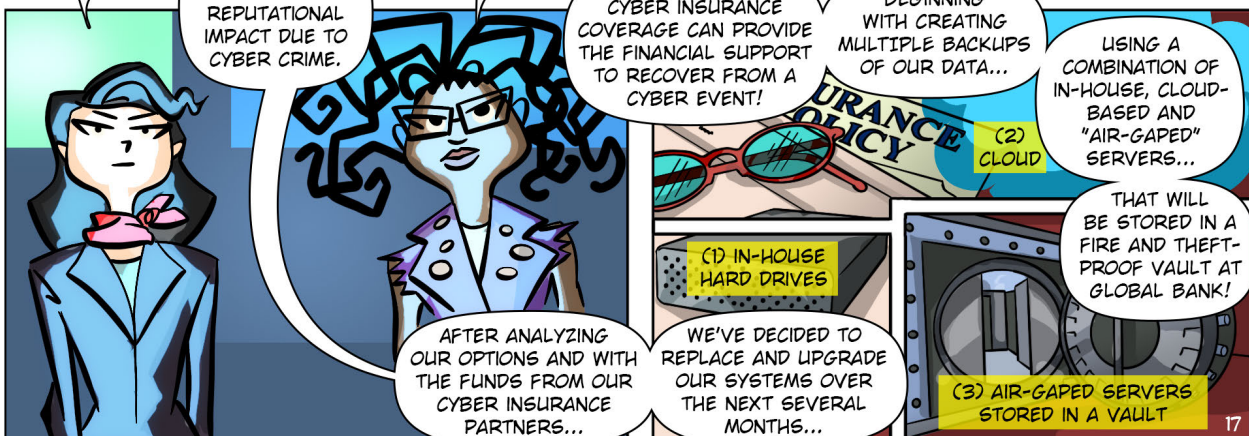
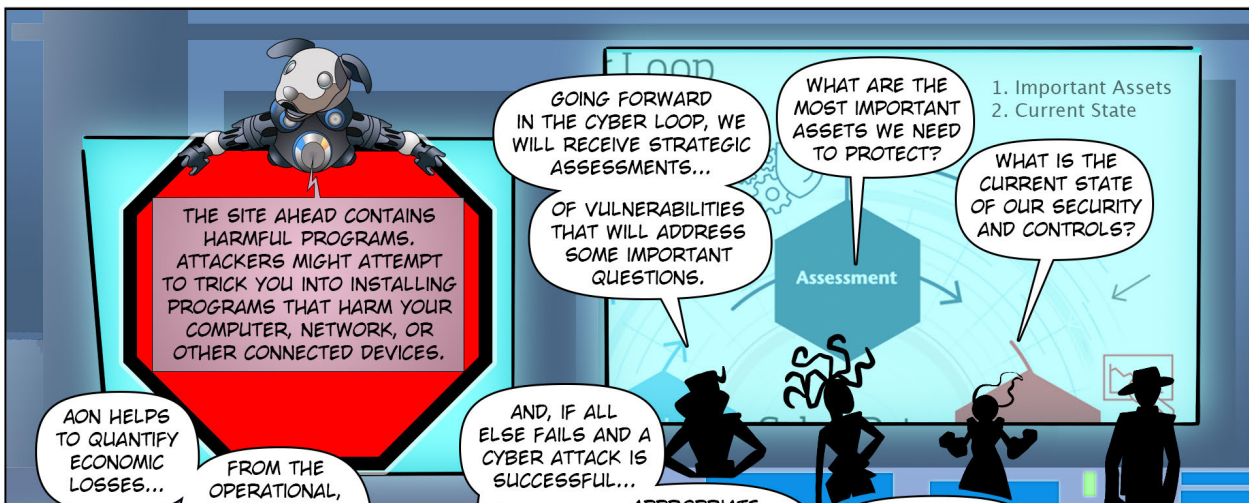
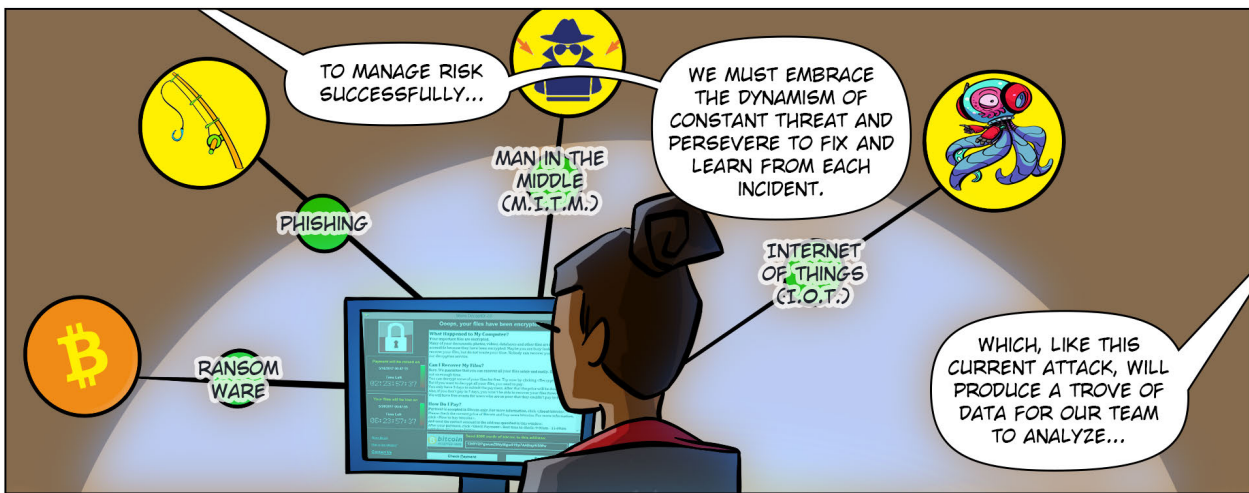
I'VE ALREADY CONTACTED THEM AND AN ENTIRE AON TEAM WILL BE AT OUR OFFICES TOMORROW!

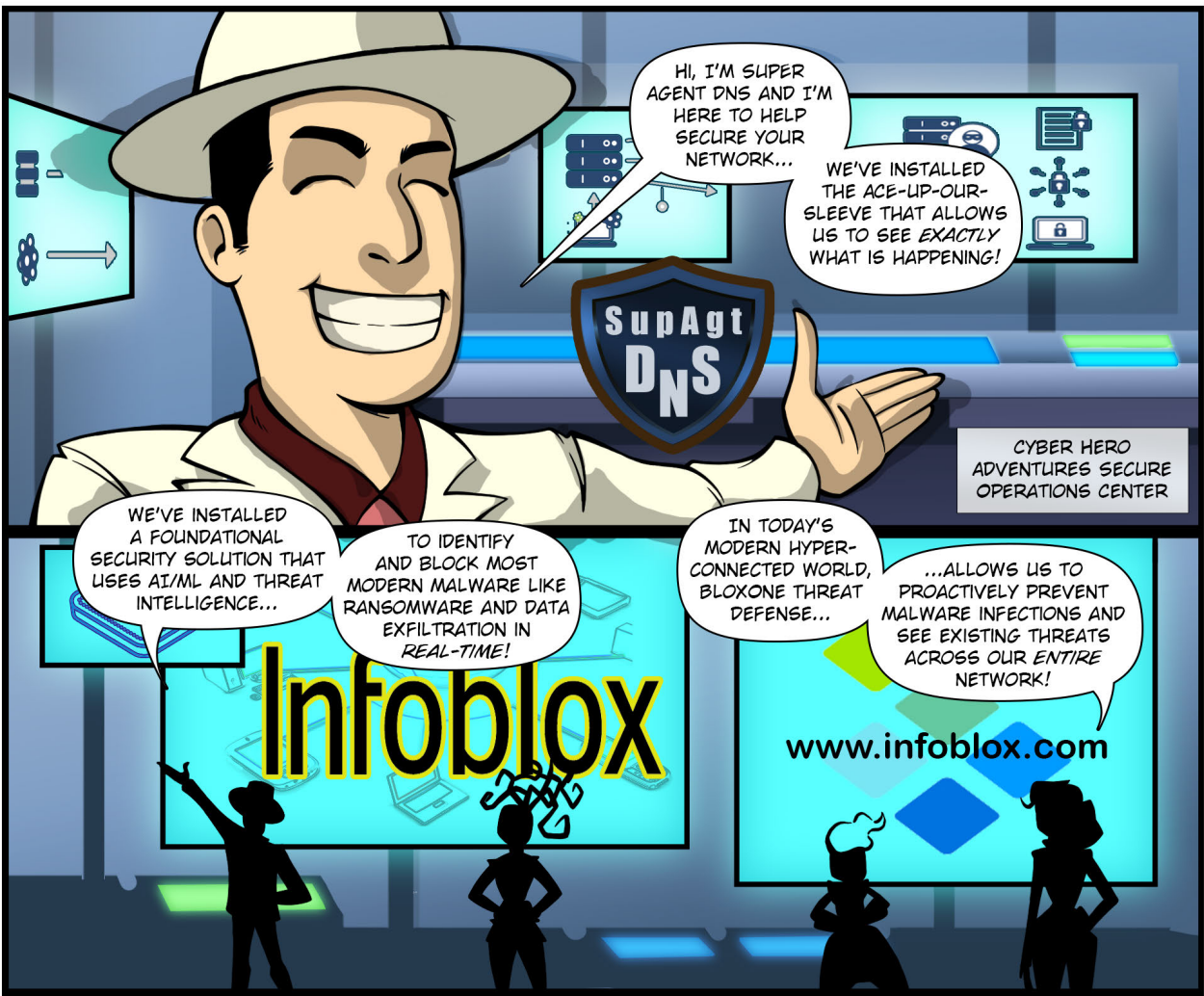


ONCE IN THE CYBER LOOP, WE'LL RECEIVE IMMEDIATE ACCESS TO REAL-TIME ATTACK DATA AND INDICATORS OF COMPROMISE (IOC)...

MAKING IT FASTER TO TRACE AN ATTACKER'S FOOTPRINTS AND DETERMINE THE NATURE OF THE ATTACK AND WHAT INFORMATION MIGHT HAVE BEEN IMPACTED.

AS THEY EXPLAINED IT TO ME, CYBER SECURITY IS AN ITERATIVE PROCESS...





HI, I'M SUPER AGENT DNS AND I'M HERE TO HELP SECURE YOUR NETWORK...

WE'VE INSTALLED THE ACE-UP-OUR-SLEEVE THAT ALLOWS US TO SEE EXACTLY WHAT IS HAPPENING!

CYBER HERO ADVENTURES SECURE OPERATIONS CENTER

WE'VE INSTALLED A FOUNDATIONAL SECURITY SOLUTION THAT USES AI/ML AND THREAT INTELLIGENCE...

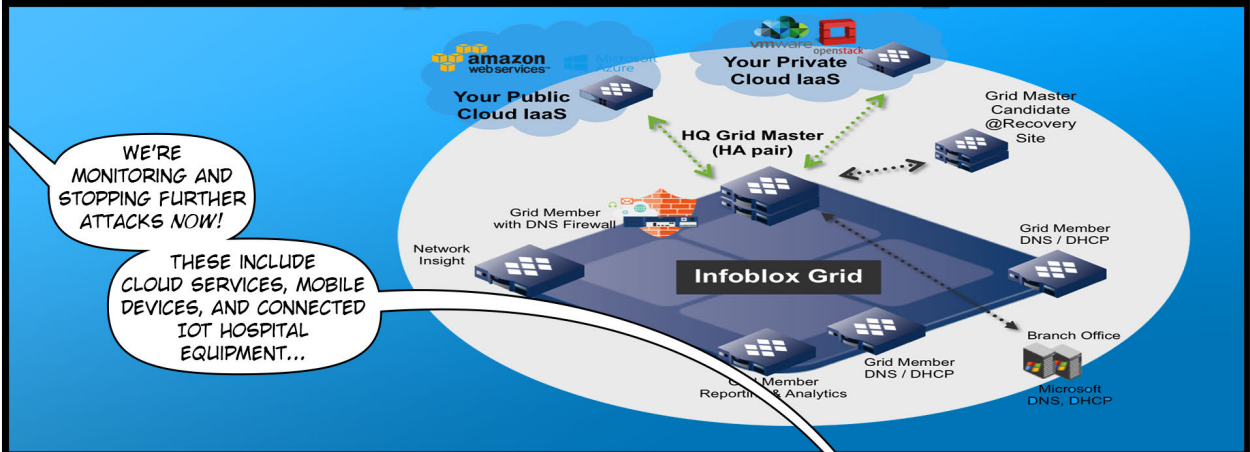
TO IDENTIFY AND BLOCK MOST MODERN MALWARE LIKE RANSOMWARE AND DATA EXFILTRATION IN REAL-TIME!

IN TODAY'S MODERN HYPER-CONNECTED WORLD, BLOXONE THREAT DEFENSE...

...ALLOWS US TO PROACTIVELY PREVENT MALWARE INFECTIONS AND SEE EXISTING THREATS ACROSS OUR ENTIRE NETWORK!

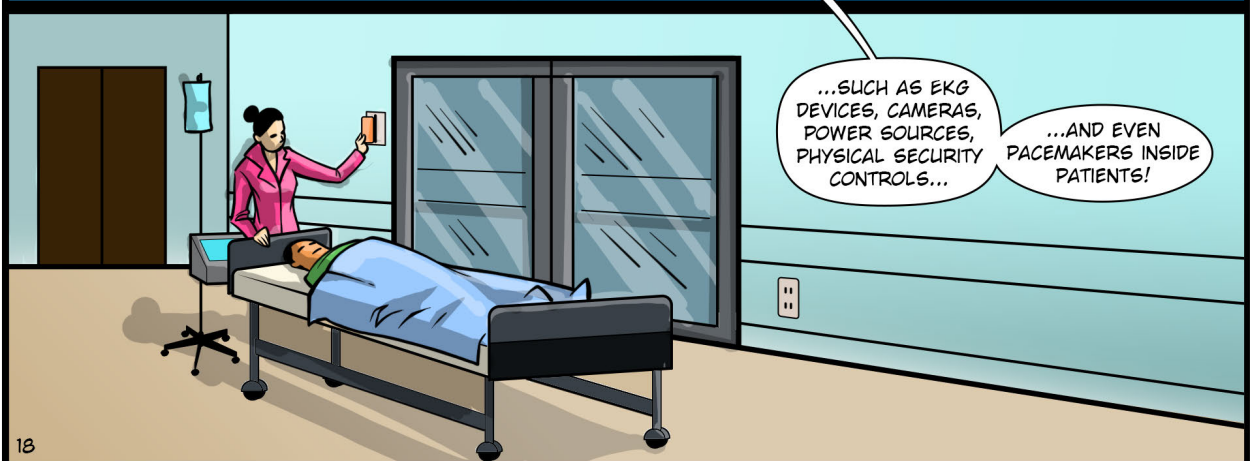
Infoblox

www.infoblox.com



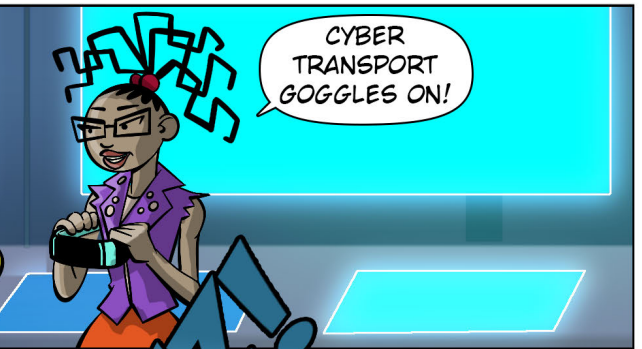
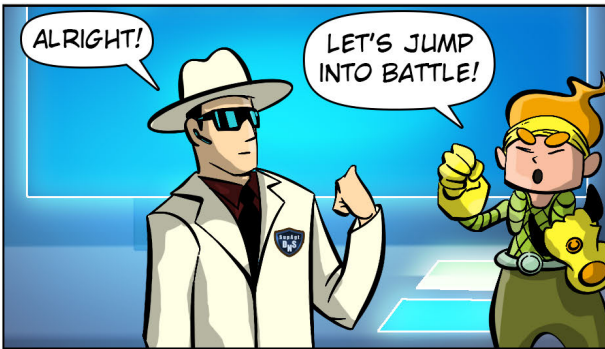
WE'RE MONITORING AND STOPPING FURTHER ATTACKS NOW!

THESE INCLUDE CLOUD SERVICES, MOBILE DEVICES, AND CONNECTED IOT HOSPITAL EQUIPMENT...



...SUCH AS EKG DEVICES, CAMERAS, POWER SOURCES, PHYSICAL SECURITY CONTROLS...

...AND EVEN PACEMAKERS INSIDE PATIENTS!



LET'S IDENTIFY THE USER OF THE DEVICE THROUGH THE ACCOUNT...

...AND WE COULD IDENTIFY EVERYTHING ABOUT THE COMPROMISED DEVICE...

THEN WE'LL LOOK AT THE DEVICES THAT THOSE ACCOUNTS ACCESSED BEFORE AND AFTER ACCESSING THE INFECTED MACHINE.

WHERE IN THE NETWORK IT IS, AND WHERE IT PHYSICALLY IS LOCATED.

...WHAT IT IS (PC, MAC, PHONE, TABLET, IOT ETC), WHO OWNS IT (BASED ON THE ACCOUNT)...

WannaCry Attack Trend

CRITICAL
INFORMATIONAL
MAJOR
WARNING

Jul 31 Sun Aug 2 Tue Aug 4 Thu Aug 6

L2 Domains

Domain	Hits
email.cnndaily.com	22014
e.cnndaily.com	21284
europa.cnndaily.com	21224
bjmeset.ahtcna.com	20904
www.nikey.cn	20858
cnndaily.com	20690
	20474

[HTTPS://WWW.INFOBLOX.COM](https://www.infoblox.com)

File name	Type
...	Configuration details
...	Message to the user with instructions on how to pay
...	Message to the user: "Most of your files are encrypted..."
taskmgr.exe	Application for displaying the messages in t1.wry and t2.wry
tasksch.exe	WannaCry encryption application

WE WILL EXAMINE EACH MACHINE FOR ANOMALOUS BEHAVIOR CAUSED BY KNOWN OR UNKNOWN MALWARE.



WOOHOOO! MS. TARA BYTE RUNNING AT THE SPEED OF LIGHT!

THE USE OF MULTIPLE NETWORK NODES CAN SEVERELY COMPLICATE TRACING BACK IP ADDRESSES, BECAUSE THEY BOUNCE THE DATA OFF MANY NODES IN AN EFFORT TO COVER ITS TRACKS.

MALWARE TYPICALLY TALKS TO A COMMAND-AND-CONTROL SERVER LIVING OUTSIDE YOUR NETWORK.

AUTHORITIES CAN ISSUE SUBPOENAS FOR RECORDS FROM ISPS, TO GET THE IP ADDRESSES AND PHYSICAL ADDRESSES OF SUSPECTS.

ALRIGHT FINN,
I'M JUST OUTSIDE
THE FIREWALL. HOW
DO I GET IN?

WELL,
THERE'S A CAN
OF GEL IN YOUR
BACKPACK...

JUST SOAK
YOURSELF IN IT
AND RUN THROUGH
THE FIRE!

WHAT?
!!!

JUST
KIDDING!

SOME OF THE
DATA YOU RECOVERED
FROM OTHER NODES
ARE PROVING HELPFUL
IN GETTING YOU IN.

HANG
ON...

THERE!
YOU'RE
IN!

THANKS FINN!
YOU WANT THIS
GEL FOR YOUR
HAIR?

HA
HA!

MEANWHILE...

THIS
IS THE POLICE.

OPEN THE
DOOR.

WE HAVE A
WARRANT.

THEN THE
AUTHORITIES CAN
OBTAIN A WARRANT
TO SEIZE ALL COMPUTERS
FROM A HOME OR
WORK PLACE.

THE LOGS OF
THAT MACHINE ARE
FORENSICALLY ANALYZED
FOR STOLEN CONTENT,
HACKING TOOLS...

...AND TO
DETERMINE WHICH
MACHINES IT'S
TALKING TO.

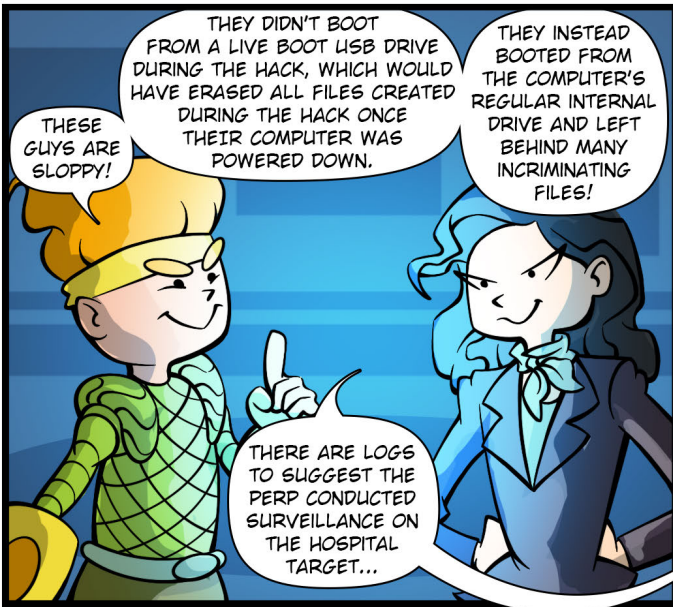
BUT WHAT
SAY WE TAKE
A LITTLE PEAK
NOW?

AGENT DNS,
THE DE-CLOAK
DEVICE IS IN-PLACE.
LET ME KNOW WHEN
YOU GET A MATCH!

WE GOT ONE!
WORKED LIKE
A CHARM!

dR900LS¶Hn5*2

CYBER HEROES S.O.C.S.
COMMAND CENTER

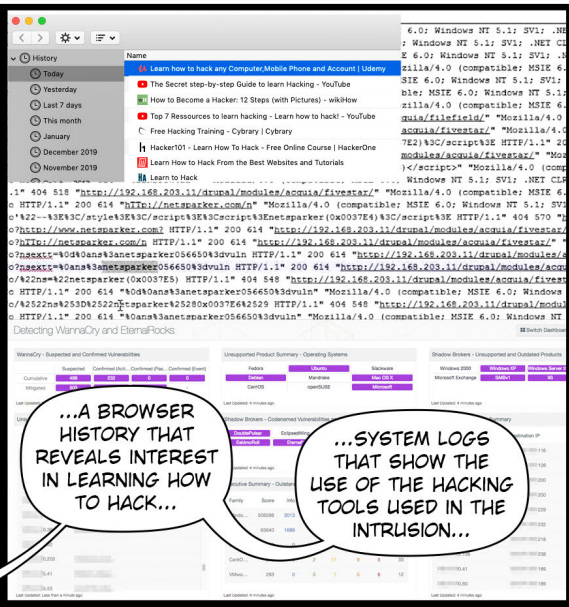


THESE GUYS ARE SLOPPY!

THEY DIDN'T BOOT FROM A LIVE BOOT USB DRIVE DURING THE HACK, WHICH WOULD HAVE ERASED ALL FILES CREATED DURING THE HACK ONCE THEIR COMPUTER WAS POWERED DOWN.

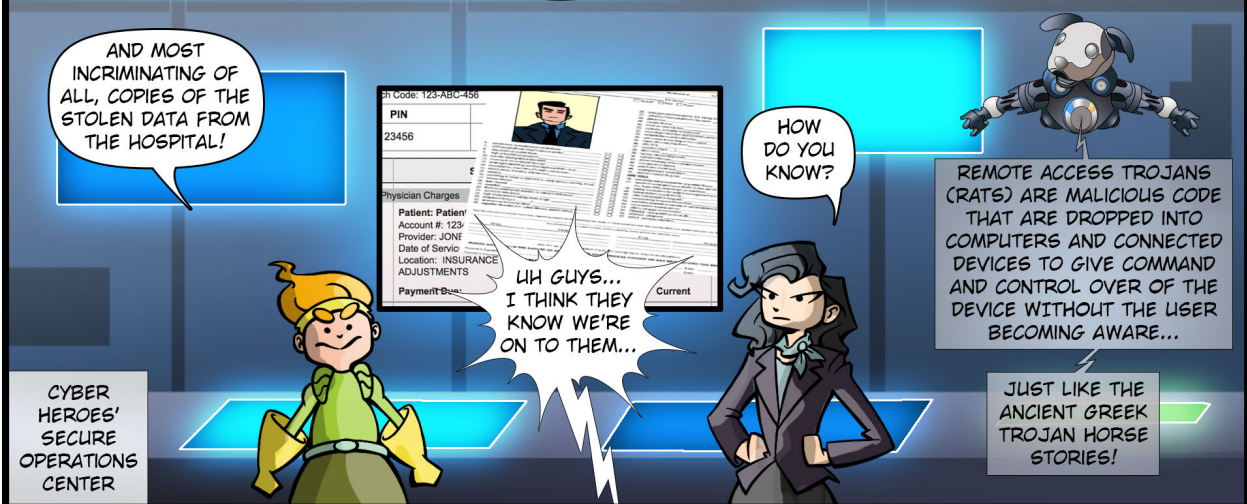
THEY INSTEAD BOOTED FROM THE COMPUTER'S REGULAR INTERNAL DRIVE AND LEFT BEHIND MANY INCRIMINATING FILES!

THERE ARE LOGS TO SUGGEST THE PERP CONDUCTED SURVEILLANCE ON THE HOSPITAL TARGET...

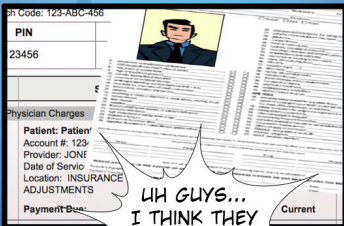


...A BROWSER HISTORY THAT REVEALS INTEREST IN LEARNING HOW TO HACK...

...SYSTEM LOGS THAT SHOW THE USE OF THE HACKING TOOLS USED IN THE INTRUSION...



AND MOST INCRIMINATING OF ALL, COPIES OF THE STOLEN DATA FROM THE HOSPITAL!



HOW DO YOU KNOW?

UH GUYS... I THINK THEY KNOW WE'RE ON TO THEM...

REMOTE ACCESS TROJANS (RATS) ARE MALICIOUS CODE THAT ARE DROPPED INTO COMPUTERS AND CONNECTED DEVICES TO GIVE COMMAND AND CONTROL OVER OF THE DEVICE WITHOUT THE USER BECOMING AWARE...

JUST LIKE THE ANCIENT GREEK TROJAN HORSE STORIES!



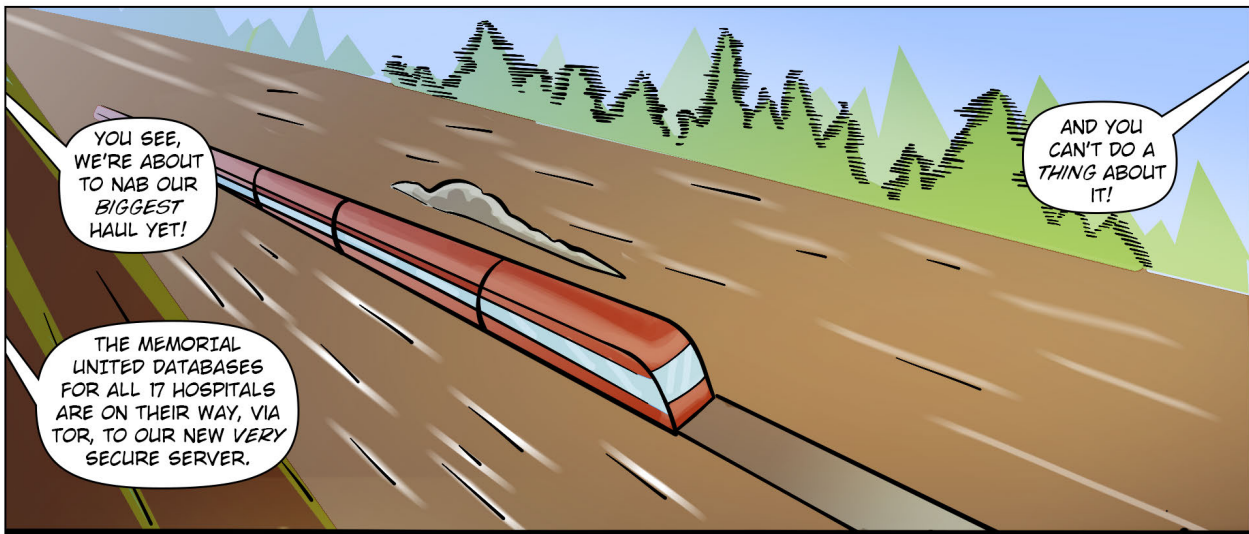
BECAUSE WE'RE MAKING EYE CONTACT!

YOU DIDN'T THINK WE HAD SYSTEMS IN-PLACE TO SNIFF OUT RATS, DID YOU?

WELL, YOU'RE TOO LATE WHITE HAT!

YOU WHITE HAT DO-GOODERS HAVE ONCE AGAIN PROVEN THAT YOU'RE NO MATCH FOR US BLACK HATS!

THEY LOVE TO UNDERESTIMATE THEIR SMARTER COLLEAGUES!



YOU SEE, WE'RE ABOUT TO NAB OUR BIGGEST HAUL YET!

AND YOU CAN'T DO A THING ABOUT IT!

THE MEMORIAL UNITED DATABASES FOR ALL 17 HOSPITALS ARE ON THEIR WAY, VIA TOR, TO OUR NEW VERY SECURE SERVER.



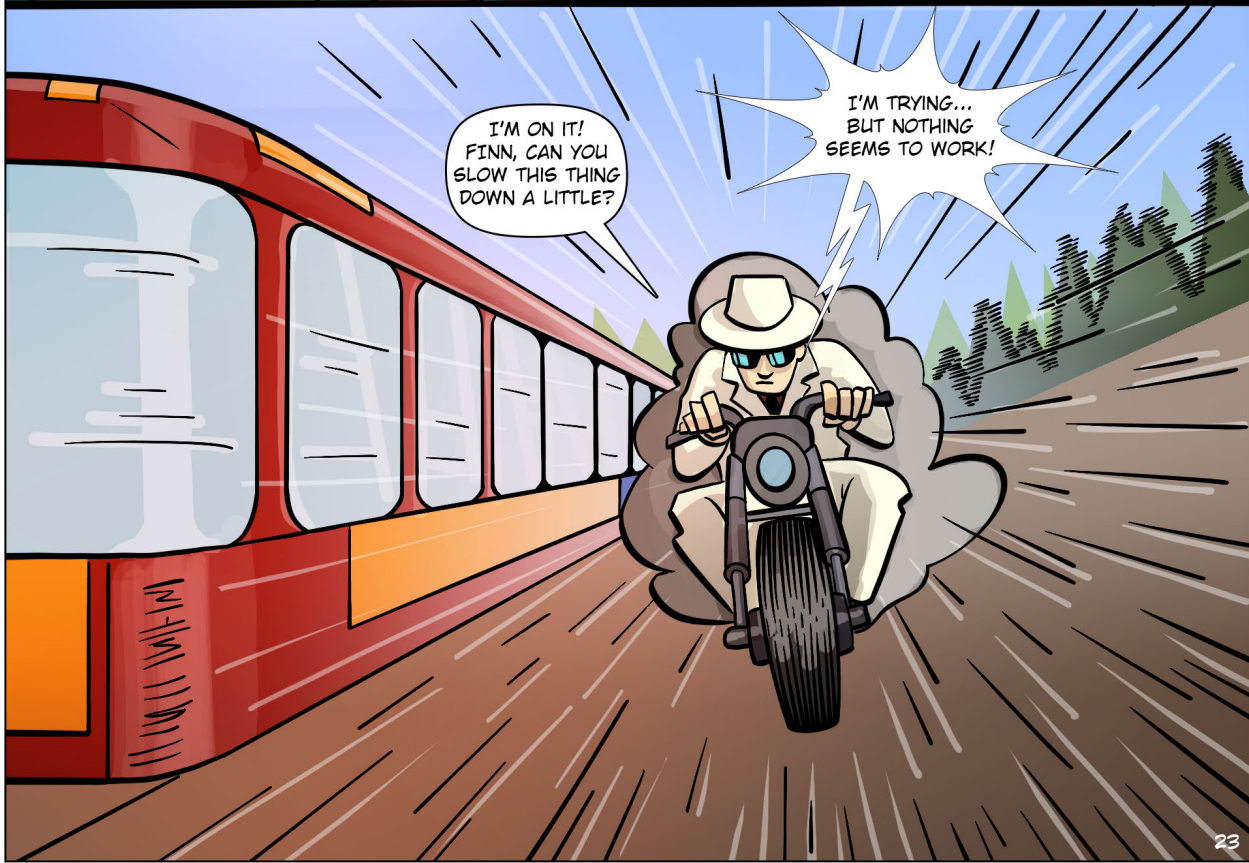
BECAUSE IN 30 SECONDS, YOU'LL BE GONE, NEITHER TO EVER BE FOUND AGAIN...

BUT WE'RE GOING TO DIFFERENT PLACES!



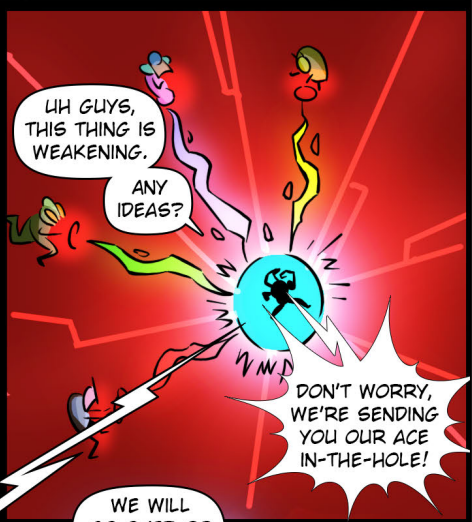
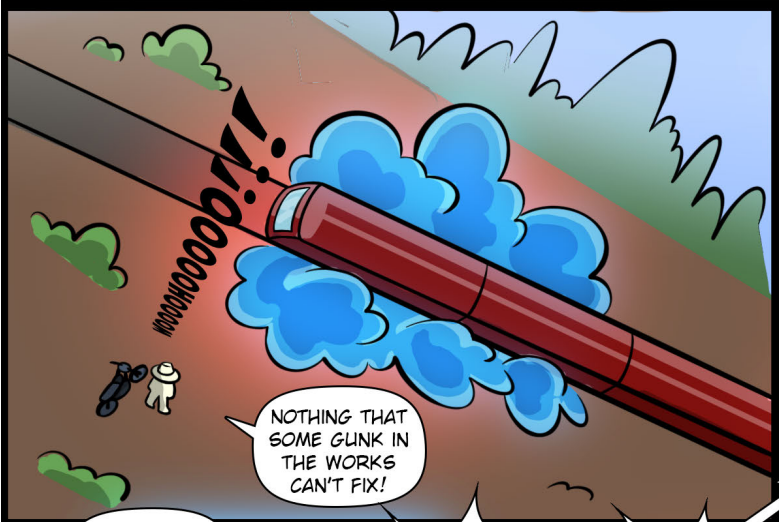
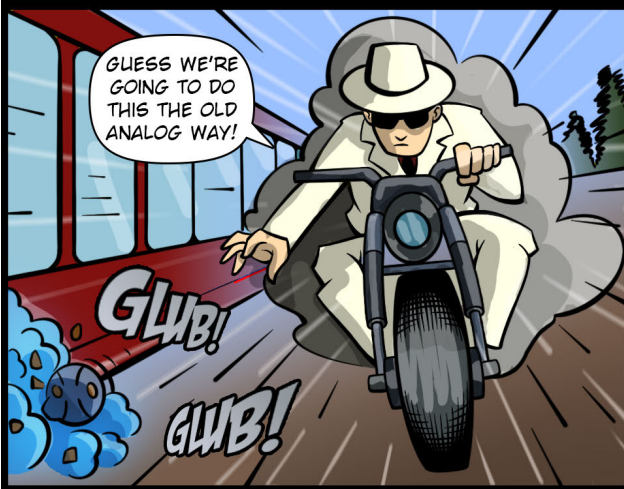
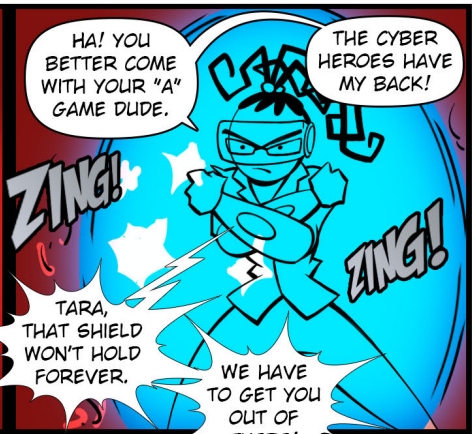
THANKS FOR CONFESSING INTO THE MIC.

YOU GET ALL THAT EVERYONE? STOP THAT DATA DUMP!



I'M ON IT! FINN, CAN YOU SLOW THIS THING DOWN A LITTLE?

I'M TRYING... BUT NOTHING SEEMS TO WORK!





SHE IS ALWAYS READY TO INFORM USING HER METICULOUSLY RESEARCHED POWER PRESENTATION SLIDES THAT PROJECT FROM A LENS IN HER COSTUME. SHE SUBDUES HER ADVERSARIES WITH SLIDES SO DENSE WITH DATA THAT THEY ARE OVERCOME BY INSTANT SLUMBER!

THE PRESENTER IS A SKILLED WHITE-HAT EX-HACKER, WHO NOW SPENDS HER TIME PROMOTING CYBERSECURITY EDUCATION AND FACILITATING PARTNERSHIPS BETWEEN GOVERNMENT, ACADEMIA, AND THE PRIVATE SECTOR FOCUSED ON SUPPORTING PEOPLE'S ABILITY TO ADDRESS CURRENT AND FUTURE CYBERSECURITY ISSUES AND WORKFORCE CHALLENGES THROUGH STANDARDS AND BEST PRACTICES. EVEN HER JOB DESCRIPTION PUTS YOU TO SLEEP!

THE PRESENTER

NOW MEET THE GOOD PEOPLE!



THE CYBERHEROES

DEFENDERS OF THE
DIGITAL UNIVERSE!



JACK THE FIREWALL LOVES RULES. HE LIVES BY RULES. HE DENIES AND ALLOWS ENTRY BY RULES. HE DOES HIS JOB QUIETLY AND UNDER THE RADAR. MOST OF THE TIME, YOU DON'T EVEN KNOW HE IS THERE. HE'S ONE OF THE MOST CHALLENGING OBSTACLES THAT HACKERS HAVE TO BYPASS. A FORMIDABLE OPPONENT TO THOSE WHO WANT TO MERELY SNOOP OR THOSE WHO MEAN TO DO HARM!

HE WORKS IN PARALLEL WITH OTHER FIREWALLS AND TEAMMATES TO FORM DATA DMZ'S AND COMPARTMENTAL AREAS TO PROTECT VALUABLE ASSETS, SYSTEMS, AND INFORMATION. HIS ONLY WEAKNESS? STALE, OLD RULES. IN A CONSTANTLY-CHANGING CYBER LANDSCAPE, JACK MUST ENSURE THAT HIS RULES ARE ALWAYS UP-TO-DATE AND ONE STEP AHEAD OF HIS ADVERSARIES!

JACK THE FIREWALL



WHILE ON TOUR OF THE FACILITY, LARRY AND SUPER AGENT K MEET TARA BIGHT, WHO WORKS AT THE INSTITUTE. THEY ARE INSTANTLY IMPRESSED WITH HER PASSION, KNOWLEDGE AND SKILLS AS A PROGRAMMER.

TARA CAME FROM HUMBLE BEGINNINGS. AGAINST ALL ODDS, AND WITH THE HELP OF EXPERT MENTORS IN THE TECHNOLOGY AND CYBERSECURITY FIELDS, SHE PROVED TO BE A LIGHTNING-FAST CODER.

SHE HAS DEDICATED HER CAREER TO OPENING UP THE WORLD OF CODING TO CHILDREN AND TO IMBUE A LOVE OF TECHNOLOGY IN THEM. TARA IS THE "PIED PIPER" OF PROGRAMMERS. HER MAIN MOTIVATION IS TO SHATTER THE GLASS CEILING FOR DIVERSITY IN TECHNOLOGY.

TO DEFEAT A HACKER, YOU NEED A BETTER HACKER!

AND THE CYBERHEROES HAVE TWO OF THE VERY BEST!

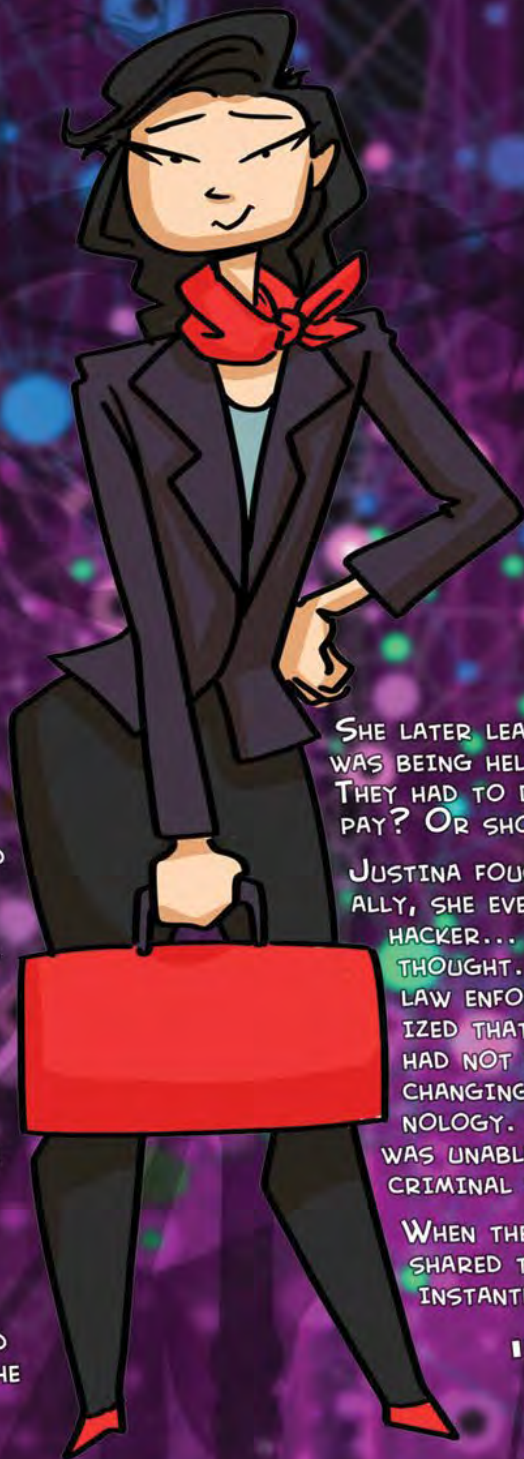
TARA BIGHT & THE SUPERCODER



LARRY JONES (A.K.A. CYBER HERO) KNEW THAT HE NEEDED HELP TO LEARN ABOUT TECHNOLOGY AND HACKING. THE MOST IMPORTANT THING THAT HE NEEDED TO UNDERSTAND WAS: WHY DO HACKERS DO WHAT THEY DO? AFTER LISTENING AND LEARNING ABOUT HACKING AND CYBER SECURITY FROM THE AMAZING PEOPLE IN LAW ENFORCEMENT, SUCH AS THE FBI, CYBER SECURITY EXPERTS, THE DEPARTMENT OF DEFENSE, THE DEPARTMENT OF HOMELAND SECURITY AND ACADEMIA, LARRY BEGAN TO UNDERSTAND THAT ALMOST ALL OF THE HACKERS WERE ACTUALLY TRYING TO HELP (WHITE HATS) BY PROGRAMMING AND HER DESTINY WAS DEFENDING THE WORLD AGAINST CYBER CRIMINALS (BLACK HATS).

THERE WERE ALSO MANY GREAT PEOPLE WHO WERE THREAT RESEARCHERS WHO DISCOVERED VULNERABILITIES IN COMPUTERS AND CONNECTED DEVICES TO HELP PROTECT US ALL (GREY HATS). LARRY KEPT HEARING THE NAME OF ONE PERSON WHO WAS CONSISTENTLY MENTIONED AS BEING THE BEST HACKER IN THE UNIVERSE: QUEEN JIO. FROM THE MOMENT THAT SHE WAS BORN, HER PARENTS KNEW THAT SHE WAS DESTINED TO BECOME A POWERFUL LEADER AND ROLE MODEL AND TO SHED SUNLIGHT ON A DARK WORLD, SO THEY NAMED HER JIO (AN ANCIENT TERM FOR "SUN"). HER FIRST WORDS WERE: WHO, WHAT, WHERE, WHEN AND MOST IMPORTANTLY...HOW? SHE QUICKLY DISCOVERED COMPUTERS AND SEALED TO SPREAD SUNSHINE ON A DIVERSE AND INCLUSIVE WORLD.

QUEEN JIO™



JUSTINA IS A FIRST-GENERATION AMERICAN OF MEXICAN HERITAGE. FROM A YOUNG AGE, SHE DEFENDED THE DEFENSELESS. SINCE THEN, SHE ALWAYS KNEW SHE WOULD BE A LAWYER.

SHE SET OUT TO LEARN ALL SHE COULD ABOUT THE JUDICIAL SYSTEM. MANY YEARS LATER SHE BECAME A PUBLIC DEFENDER, DEFENDING THE RIGHTS OF THE ACCUSED. ONE DAY, SOMETHING SHOCKING HAPPENED TO JUSTINA AND HER COLLEAGUES, WHEN SHE CLICKED ON AN EMAIL AND ALL THE COMPUTERS IN THE OFFICE FROZE.

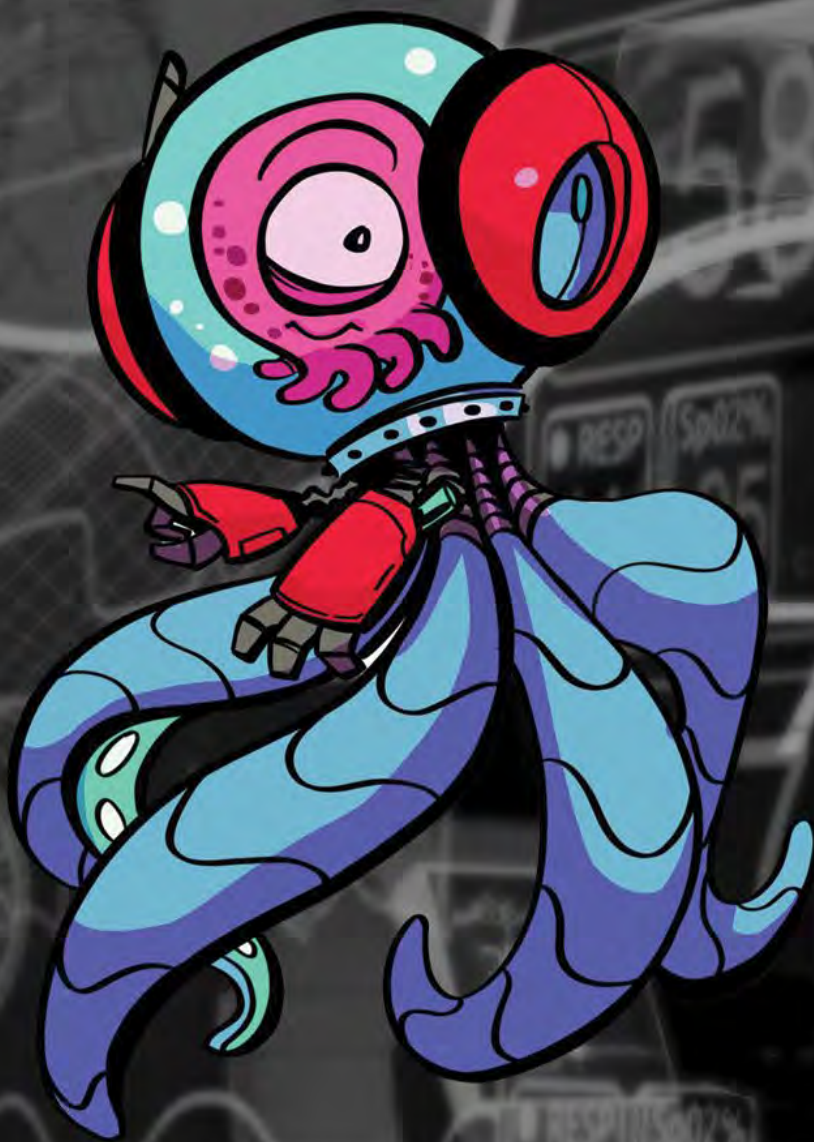
SHE LATER LEARNED HER OFFICE WAS BEING HELD FOR RANSOM. THEY HAD TO DECIDE: SHOULD THEY PAY? OR SHOULD THEY FIGHT?

JUSTINA FOUGHT. HARD. EVENTUALLY, SHE EVEN IDENTIFIED THE HACKER... OR SO SHE THOUGHT. WORKING WITH LAW ENFORCEMENT, SHE REALIZED THAT THE LEGAL SYSTEM HAD NOT KEPT PACE WITH THE CHANGING WORLD OF TECHNOLOGY. IN TIME, JUSTINA WAS UNABLE TO BRING THE CRIMINAL TO JUSTICE.

WHEN THE CYBER HEROES SHARED THEIR STORIES, SHE INSTANTLY TOLD THEM:

"I'M IN!"

JUSTINA JASCO & THE DEFENDER



THE INTERNET OF THINGS (IOT) IS A NETWORK OF PHYSICAL DEVICES THAT INCLUDES VEHICLES, HOME APPLIANCES, HEART MONITORING IMPLANTS, STREET LIGHTS, BIOCHIP TRANSPONDERS, CAMERAS STREAMING LIVE FEEDS, AND OTHER ELECTRONIC DEVICES EMBEDDED WITH SOFTWARE, SENSORS, AND ACTUATORS. EACH THING IS UNIQUELY IDENTIFIABLE BUT IS ABLE TO OPERATE WITHIN THE EXISTING INTERNET INFRASTRUCTURE.

PRETTY MUCH ANY OBJECT CAN BE TURNED INTO AN IOT DEVICE IF IT CAN BE CONNECTED TO THE INTERNET AND CONTROLLED THAT WAY. THE TERM 'IOT' IS USED FOR DEVICES THAT WOULDN'T GENERALLY BE EXPECTED TO HAVE AN INTERNET CONNECTION, AND THAT CAN COMMUNICATE WITH THE NETWORK INDEPENDENTLY OF HUMAN ACTION. THEREFORE, PCs AND SMARTPHONES AREN'T CONSIDERED IOT DEVICES.

IOT THE INTERNET OF THINGS



LARRY IS A "REGULAR GUY" WHO IS AN EXPERT AT MARKETING COMMUNICATIONS AND CORPORATE TRAINING. HE RAN A SUCCESSFUL COMPANY THAT WAS SUBSEQUENTLY SOLD TO GLOBALCOMM. EVERYTHING WAS GOING GREAT UNTIL ONE DAY HE RECEIVED A FATEFUL CALL. UNBEKNOWNST TO HIM, ONE OF LARRY'S EXECUTIVES PHONED GLOBALCOMM PRETENDING TO BE A WHISTLE-BLOWER AND SPREAD A RUMOR THAT THERE WAS RAMPANT FRAUD THROUGHOUT LARRY'S COMPANY AND THAT ALL CLIENTS SHOULD STOP ALL COMMUNICATIONS!

LARRY LOST MILLIONS OF DOLLARS AND HIS HOME. HE WAS FORCED TO FIRE ONE HUNDRED EMPLOYEES. ONLY YEARS LATER, LIKE PEELING THE LAYERS OF AN ONION, LARRY BEGAN TO UNDERSTAND THAT HE WAS BEING

VICTIMIZED BY A SERIES OF INSIDER CYBER ATTACKS THAT FUNNELED HIS BUSINESS INTO A SHADOW COMPANY CONTROLLED BY SEVERAL FORMER EXECUTIVES. THEY SPOOFED HIS WEBSITE, RE-DIRECTED CALLS TO THE SHADOW COMPANY AND DESTROYED HIS REPUTATION.

UNABLE TO PROVE HIS CASE AND RECEIVE JUSTICE DUE TO THE DIFFICULTY OF IDENTIFYING THE PLOT AND THE HACKER, LARRY DECIDED TO PIVOT FROM BEING A VICTIM TO BECOMING AN ADVOCATE. HE LEARNED EVERYTHING HE COULD ABOUT CYBER SECURITY. LIKE DOROTHY IN THE WIZARD OF OZ, LARRY MEETS WONDERFUL CYBERHEROES ALONG THE WAY, WHO ARE MISSION-DRIVEN CHARACTERS JOINING HIM ON HIS QUEST TO RAISE AWARENESS OF CYBERCRIME AND TO DEFEND THE DIGITAL UNIVERSE!

LARRY JONES vs THE CYBERHERO!

MEET THE CYBER VILLAINS OF THE DARK WEB!



AND BEWARE... THEY LURK IN YOUR
COMPUTER, NETWORK, SMARTPHONE, CAR,
WEBCAM, THERMOSTAT, BABY MONITOR...
EVEN YOUR VACUUM CLEANER! THEY LIVE IN A
PLACE WHERE EVEN GOOGLE WON'T TREAD...

THE DARK WEB!



INTERPOL
case #
F-34937H-75U



WANNACRY IS AN INSIDIOUS FORM OF RANSOMWARE CRYPTOWORM THAT ATTACKED THE **MICROSOFT WINDOWS** OPERATING SYSTEMS OF INDIVIDUALS AND BUSINESSES AROUND THE WORLD BY ENCRYPTING THE USER'S DATA (LOCKING THEM OUT OF THEIR COMPUTER) AND DEMANDING **RANSOM** IN DIFFICULT-TO-TRACE DIGITAL CURRENCIES SUCH AS **BITCOIN** TO UNLOCK IT, MAKING APPREHENDING AND PROSECUTING THE PERPETRATORS DIFFICULT. THE ATTACK WAS UNPRECEDENTED IN SCALE, INFECTING MORE THAN **230,000** COMPUTERS IN OVER **150** COUNTRIES.

RANSOMWARE ATTACKS ARE TYPICALLY CARRIED OUT USING A **TROJAN HORSE** DISGUISED AS A LEGITIMATE FILE. THE USER IS DUPED INTO DOWNLOADING OR OPENING IT IN AN EMAIL ATTACHMENT. HOWEVER, THE **WANNACRY** WORM WAS ABLE TO TRAVEL AUTOMATICALLY BETWEEN COMPUTERS WITHOUT ANY USER INTERACTION.

THE CRIMINALS BEHIND **WANNACRY** ARE STILL OUT IN THE WORLD, DEVELOPING NEW TRICKS, CODING NEW MALWARE, PLANNING THEIR

NEXT BIG ATTACK!

WILBUR WANNACRY



IVAN STEALS YOUR NAME, DATE OF BIRTH, SOCIAL SECURITY NUMBER, DRIVER'S LICENSE NUMBER, BANK ACCOUNT AND CREDIT CARD NUMBERS, PIN NUMBERS, ELECTRONIC SIGNATURES, FINGERPRINTS, AND PASSWORDS... ALL IN AN EFFORT TO BECOME YOU!

AT LEAST FOR THE PURPOSES OF STEALING YOUR MONEY AND APPLYING FOR LOANS CREDIT CARDS IN YOU'LL TYPICALLY A VARIETY OF

- RUMMAGING GARBAGE FOR PERSONAL DOCUMENTS AND PHONES.
- STEALING YOUR CREDIT CARDS, CARDS, PASSPORTS AND TOKENS.
- GUESSING COMMON QUESTIONS SUCH AS: "NAME?", "FIRST CAR", "FIRST PET'S"
- SKIMMING CREDIT CARDS USING HAND-HELD CARD READERS.

YOUR FIND AND NAME! IVAN AT ILLICIT ACTIVITIES: THROUGH YOUR UN-SHREDDED OR OLD HARD DRIVES

MAIL TO OBTAIN IDENTIFICATION AUTHENTICATION

KNOWLEDGE "MOTHER'S MAIDEN MODEL?" OR NAME?" INFORMATION FROM CARD READERS.

- HACKING DATABASES TO OBTAIN LARGE QUANTITIES.
- BRUTE-FORCE WORDS.
- BROWSING SITES FOR PER-BY USERS.
- DIVERTING IN ORDER TO OBTAIN CREDIT CARDS, BILLING STATEMENTS, OR NEW ACCOUNTS OPENED THIEVES IN THE

- USING 'CONTACTLESS' CREDIT CARD READERS TO ACQUIRE DATA WIRELESSLY.
- DISCREETLY WATCHING OR HEARING OTHERS PROVIDING VALUABLE PERSONAL INFORMATION (SHOULDER-SURFING).

- STEALING PERSONAL INFORMATION FROM COMPUTERS USING BREACHES IN BROWSER SECURITY-MALWARE SUCH AS TROJAN KEYSTROKE LOGGING PRO-

PUTER NETWORKS AND DATA-PERSONAL DATA, OFTEN IN

ATTACKING WEAK PASS-

SOCIAL NETWORKING SONAL DETAILS PUBLISHED

VICTIMS' EMAIL OR MAIL OBTAIN PERSONAL INFORMATIONALS SUCH AS CREDIT AND BANK/CREDIT CARD TO DELAY THE DISCOVERY OF AND CREDIT AGREEMENTS OPENED BY THE IDENTITY VICTIMS' NAMES.

IVAN THE IDENTITY THIEF



F.B.I.
case no.
A-645582
Phoebe Phillips
aka "The Phisher"

THE PHISHER

HUNTS ITS PREY BY PRETENDING TO BE LEGITIMATE COMMUNICATION FROM A TRUSTED COMPANY (OF WHICH OFTEN THE VICTIM IS A CUSTOMER) – OR – FROM THE HIJACKED IDENTITY OF A FRIEND, COLLEAGUE, OR FAMILY MEMBER.

USING ONE OF MANY RUSES (USUALLY INVOLVING SOME "PROBLEM" WITH THE ACCOUNT), THE PHISHER ENCOURAGES THE POTENTIAL VICTIM TO DIVULGE SENSITIVE INFORMATION, SUCH AS LOG-IN IDS, PASSWORDS, PINs, SOCIAL SECURITY NUMBERS, ETC.

THIS INFORMATION IS QUICKLY USED TO STEAL MONEY FROM ACCOUNTS AND TO APPLY FOR FRAUDULENT LOANS AND CREDIT CARDS. UNDOING THE DAMAGE CAUSED BY IDENTITY THEFT USUALLY TAKES MONTHS OF PHONE CALLS, WRITTEN COMMUNICATION, AND LOTS OF LEGAL AND FINANCIAL RED TAPE. KNOWING HOW TO SPOT THE SIGNS OF A PHISHING ATTACK (LOOKING AT THE SENDER'S ACTUAL EMAIL ADDRESS, FOR EXAMPLE) CAN BE THE DIFFERENCE BETWEEN AN ODYSSEY OF FRUSTRATION AND THE SIMPLE ACTION OF DELETING THE EMAIL AND BEING DONE WITH IT.

AS A GENERAL RULE, NO LEGITIMATE COMPANY WILL EVER ASK A CUSTOMER TO DIVULGE SENSITIVE INFORMATION VIA EMAIL. WHEN IN DOUBT, INSTEAD OF CLICKING THE LINK PROVIDED IN THE EMAIL, TYPE THE COMPANY'S URL DIRECTLY INTO YOUR BROWSER OR CALL A COMPANY REPRESENTATIVE USING

A KNOWN OR PUBLISHED PHONE NUMBER INSTEAD OF A PHONE NUMBER PROVIDED IN THE EMAIL.

PHOEBE THE PHISHER



HALF HUMAN, HALF INSECT, BORIS IS ABLE TO DETECT AND EXPLOIT VULNERABILITIES IN TECH DEVICES TO GAIN UNAUTHORIZED ACCESS PRIVILEGES, COMPROMISE DATA CONFIDENTIALITY AND INTEGRITY, AND WREAK HAVOC ON EVERYTHING HE TOUCHES.

BORIS HAS BEEN CREATING CHAOS FOR A LONG TIME. FOR EXAMPLE, IN 1996, A SOFTWARE BUG IN ITS GUIDANCE COMPUTER SOFTWARE FORCED THE EUROPEAN SPACE AGENCY TO DESTROY A \$1 BILLION ARIANE 5 PROTOTYPE ROCKET LESS THAN A MINUTE AFTER LAUNCH.

BORIS THE BUGGER



FRAUDSTER, SCAMMER, CONFIDENCE ARTIST, GRIFTER, HUSTLER, CHAMELEON. HE GOES BY MANY NAMES. THEY ALL ADD UP TO ONE THING: SONNY THE SOCIAL ENGINEER IS A MASTER MANIPULATOR OF HUMAN BEHAVIOR. HIS GAME IS TO TRICK YOU INTO BELIEVING WHATEVER HE WANTS IN ORDER TO STEAL YOUR MOST VALUABLE AND PERSONAL INFORMATION.

HIS WEAPONS ARE BASED ON EMOTIONAL INTELLIGENCE. HE DOES NOT HESITATE TO TAKE ADVANTAGE OF THE MOST EXCITING OR SAD MOMENTS. HE WIELDS FEAR LIKE A WHIP. HE PREYS ON ANY PERCEIVED WEAKNESS TO BRING DOWN HIS TARGETS AND ENRICH HIMSELF IN THE PROCESS.

SONNY

THE SOCIAL ENGINEER



THE **RAT** IS AN INSIDIOUS CREATURE WHO IS VERY CLEVER AND STEALTHY. PAY NO ATTENTION TO HIS HORSE-LIKE BODY OR HIS GNARLY RAT FACE... BUT TO THE LENGTH OF HIS TAIL. IT'S SINEWY AND ABLE TO INSERT ITSELF, WITHOUT DETECTION, INTO ANY DEVICE ON THE **I**NTERNET. MOST-COMMONLY IN

PARTNERSHIP WITH THE **P**HISHER, A SIMPLE CLICK ON A LINK IN AN OFFICIAL-LOOKING EMAIL LETS THE **RAT** AND HIS CREW INTO YOUR LIFE TO TURN IT UPSIDE-DOWN. ONCE INSIDE, HE COMPLETELY TAKES CONTROL OF YOUR ONLINE EXISTENCE, WHICH HE CAN THEN MANIPULATE, DESTROY, AND DELETE.

RANDALL R.A.T.



THIS SICKLY CREATURE SPREADS ITS DISEASE AND CONTAMINATES EVERYTHING IT TOUCHES. A COMPUTER VIRUS IS MALICIOUS SOFTWARE ("MALWARE") THAT REPLICATES ITSELF BY MODIFYING OTHER COMPUTER PROGRAMS AND INSERTING ITS OWN CODE.

VERNAN THE VIRUS TEAMS UP WITH SONNY THE SOCIAL ENGINEER, EMPLOYING A VARIETY OF MECHANISMS AND DECEPTIONS, COMPLEX ANTI-DETECTION STEALTH STRATEGIES TO EVADE ANTIVIRUS SOFTWARE, AND DETAILED KNOWLEDGE OF SECURITY VULNERABILITIES TO INFECT NEW HOSTS AND SPREAD THE DISASTROUS VIRUS. THEY ARE A DANGEROUS DUO INDEED!

CAUSING SYSTEM FAILURE, WASTING COMPUTER RESOURCES, CORRUPTING DATA, AND GREATLY INCREASING MAINTENANCE COSTS, VERNAN CAUSES BILLIONS OF DOLLARS' WORTH OF ECONOMIC DAMAGE EVERY YEAR. THE MOTIVES FOR THESE CRIMES VARY — FROM SEEKING PROFIT TO SENDING A POLITICAL MESSAGE, SABOTAGE OR REVENGE, OR SIMPLY FOR PERSONAL AMUSEMENT.

VERNAN THE VIRUS

Welcome to The Cyber Hero Network!



Join our mission to shine the light on the UNSUNG CYBER HEROES who toil in anonymity to keep us safe and Defend the Digital Universe!

Meet members of The Cyber Hero Network who participate in high-level, thought leadership Cyber Hero Adventures Shows, Micro Think Tanks and other B2B activities...

"Gary has put together a great show with some great talent from the cybersecurity space. From newbies to executives, everyone can stand to learn from Gary's fun and often funny (but serious) show highlighting the unsung heroes in cybersecurity".



Terry Dunlap

Principal Program Manager
at Microsoft

"What a pleasure professionally to work with Gary Berman and Cyber Heroes! I've participated in several sessions he's hosted and produced and am pleased with the high caliber of the discussion he stimulates and end product he creates. Gary invites (and gets) some pretty high-powered people".



Samuel Visner

Tech Fellow at MITRE

"Gary's show is highly relevant, informative and entertaining. His questions are always on point and his guests offer helpful insights to those of us in critical infrastructure. (You're a great host, Gary.)".



Michael Arceneaux

Chief Operating Officer,
AMWA / Managing Director,
WaterISAC

"Gary Berman is a marketing genius. With humor and aplomb he takes complex subjects and makes them accessible to everyone. He has been the pied piper for cyber security for several years now and his show is followed by thousands. I was honored to be featured myself and encouraged anyone who is invited to participate".



Tina Gravel

SVP Channels and
Alliances at
Appgate/Author/Influencer/



Gary Berman's
**CYBERHERO
ADVENTURES:
DEFENDERS OF THE
DIGITAL UNIVERSE**

www.cyberheronetwork.com