CYBER AWARENESS

THE AMERICAN CLUB

Foreword And Acknowledgements

For all the extraordinary convenience it lends to the conduct of life in the twenty-first century, modern information technology, in its burgeoning forms of intimate connectivity, has a dark side.

All of us are aware of the more egregious elements of that dark side. Indeed some of us, despite the best of intentions, may have fallen prey to those devious denizens of the internet who seek to defraud us or, indeed, cause much greater damage to our affairs for whatever motives impel them to do so.

The need for cyber awareness in the operation of ships has become an increasingly urgent focus of the industry over recent years. This focus has necessarily responded to the growing technological complexity of ships and the electronic systems used to operate them. Rising complexity often – but not always – implies the expansion of possibilities for things to go wrong, particularly if the human interface with the systems in question is not equal to the task of maintaining their integrity.

So, despite the movement towards greater technological autonomy in the management of ships, both ashore and afloat, the human element remains a key factor in ensuring the reliability of IT systems and their protection from external manipulation and corruption.

As mentioned in the preface, the importance of cyber security has been recognized by the requirement, from January 1, 2021, of ISM Code certification to take account of cyber risk management. Many of the practical dimensions to this will relate to the cyber awareness of crews, and their use of IT capabilities for communication and other purposes during their period of attachment to the ship.

In this context, it is hoped that *Cyber Awareness* will prove useful to Members and their seafaring employees in highlighting, in an accessible and memorable form, some of the key best practices to ensure a ship's safety and security in regard to the risks created by the modern cyber environment and the onboard vulnerabilities associated with it.

Many thanks are due to Dr. William Moore, Ms. Danielle Centeno and the Shipowners Claims Bureau, Inc.'s IT team for driving this latest initiative of the American Club with their characteristic enthusiasm and energy. Thanks are also due to Mr. John Steventon whose artistic talent is matched only by his ability to capture in images complex ideas made understandable by their ingenious representation in pictorial form.

Joseph E.M. Hughes
Chairman & CEO
Shipowners Claims Bureau, Inc.
Managers of the American Club

THE AMERICAN CLUB 1917

Preface

The primary audience of *Cyber Awareness* is the seafarer. There are common and basic best practices to maintain cyber security for seafarers' personal devices as well as shipboard systems alike. Many of these common best practices apply at home as well as aboard ship.

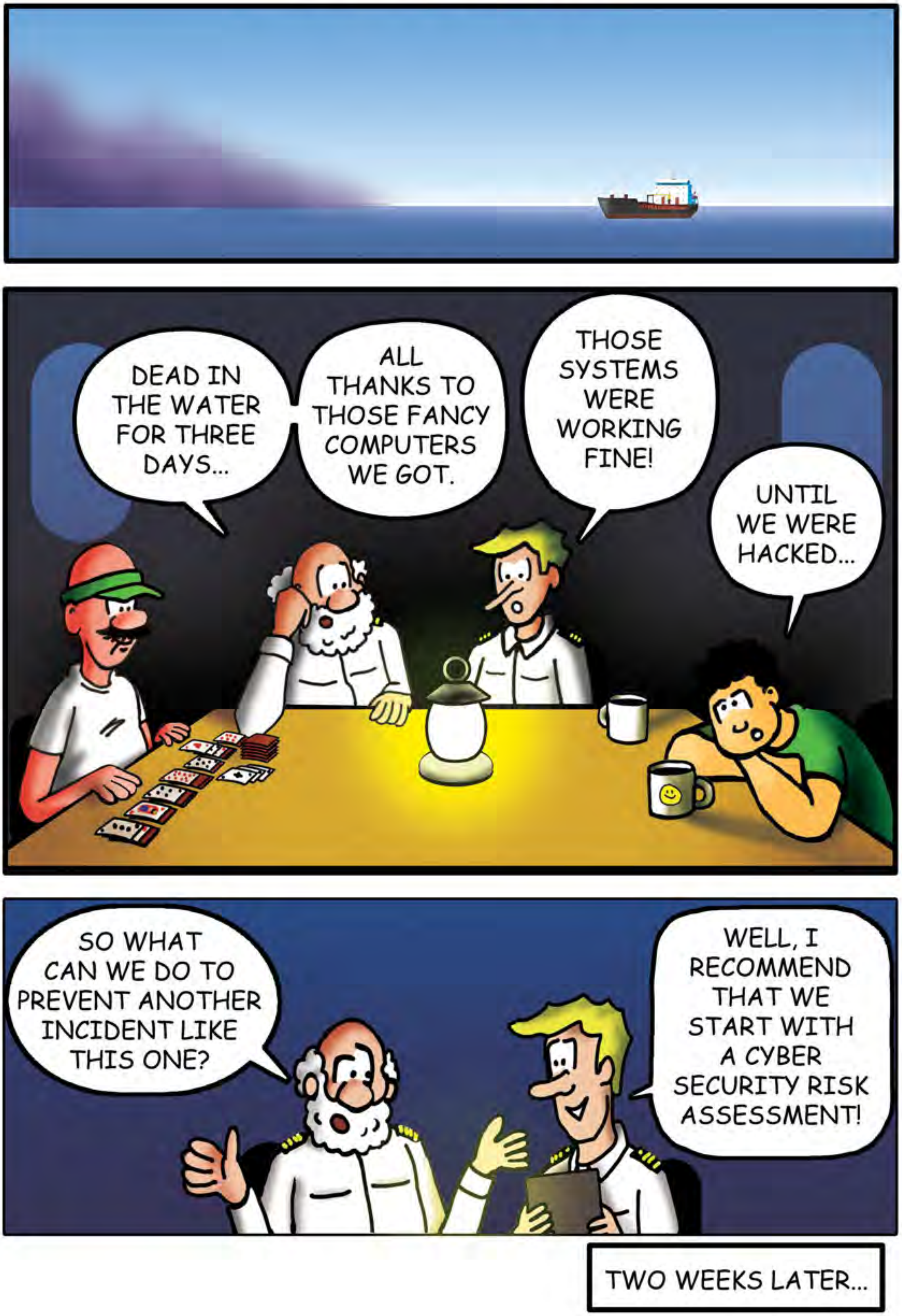
The necessity for seafarers to establish a level of cyber risk awareness and diligence is imperative to both their personal and professional lives. While the 2017 IMO resolution only "encourages" cyber risk management (CRM) compliance, it is important to understand that cybersecurity is essential to every business and critical to the safety, integrity and reliability of maritime assets and operations. In practice this means that the company should risk assess their IT systems environment –including systems used to operate the vessel – and issue procedures to manage all cyber security risks including those impacting the ships' seafarers.

Communication and socialization with the outside world, particularly with friends and family is commonplace for the modern seafarer. From a human element perspective, their cyber wellness is a critical component of their over all health and personal wellness. However, it is important to understand that with that privilege also comes the responsibility to protect oneself and ensure the ship's safety and security are not compromised. These common objectives are achieved by employing good personal cyber security practices. It is our hope that seafarers find *Cyber Awareness* a useful reminder of the simple practices of protecting themselves and the ship's safety and security.

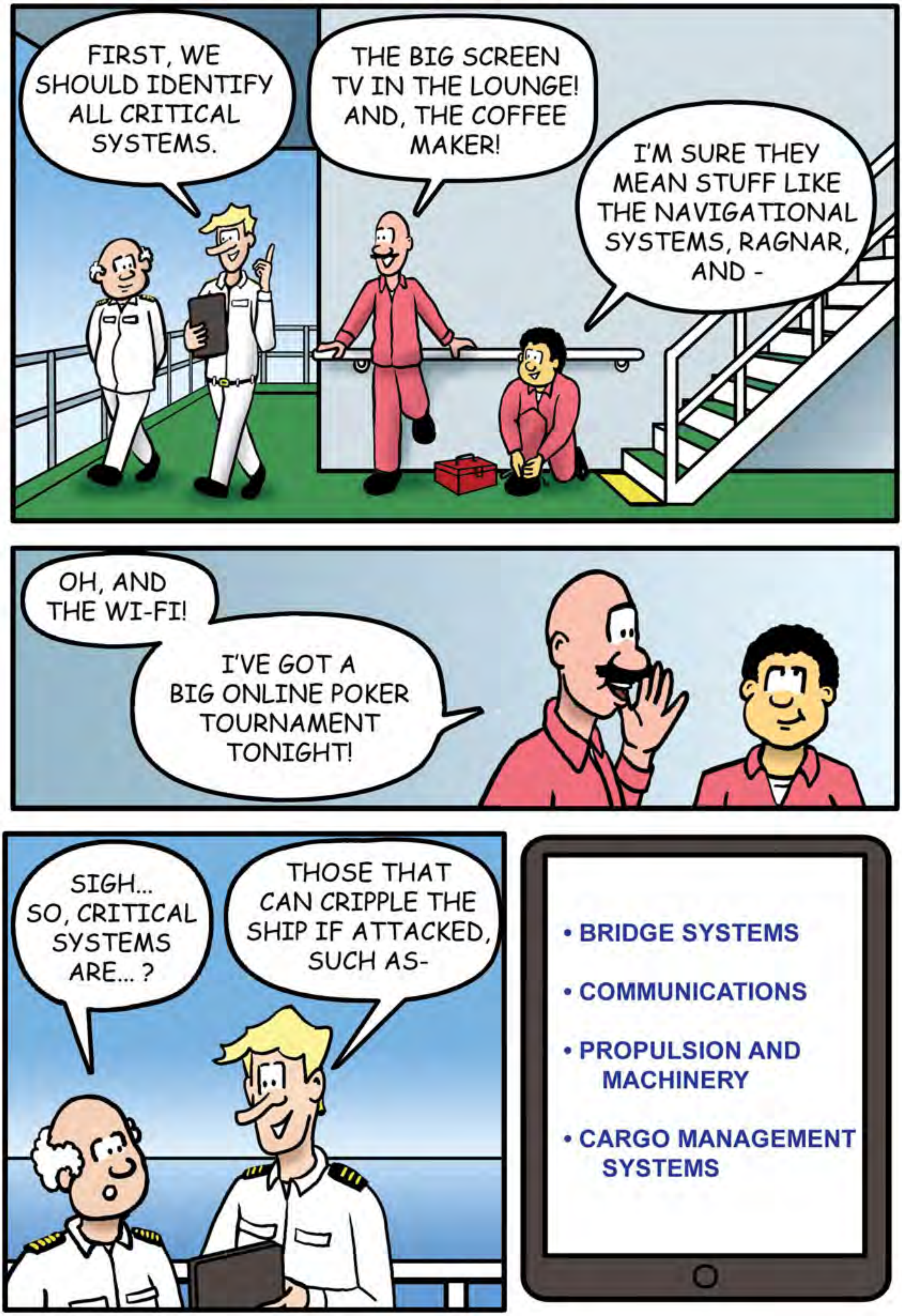
William H. Moore, Dr. Eng.
Senior Vice President
Shipowners Claims Bureau, Inc., Managers
American Steamship Owners Mutual Protection & Indemnity Association, Inc.

Ms. Danielle Centeno
Assistant Vice President
Shipowners Claims Bureau, Inc., Managers
American Steamship Owners Mutual Protection & Indemnity Association, Inc.

CYBER AWARENESS

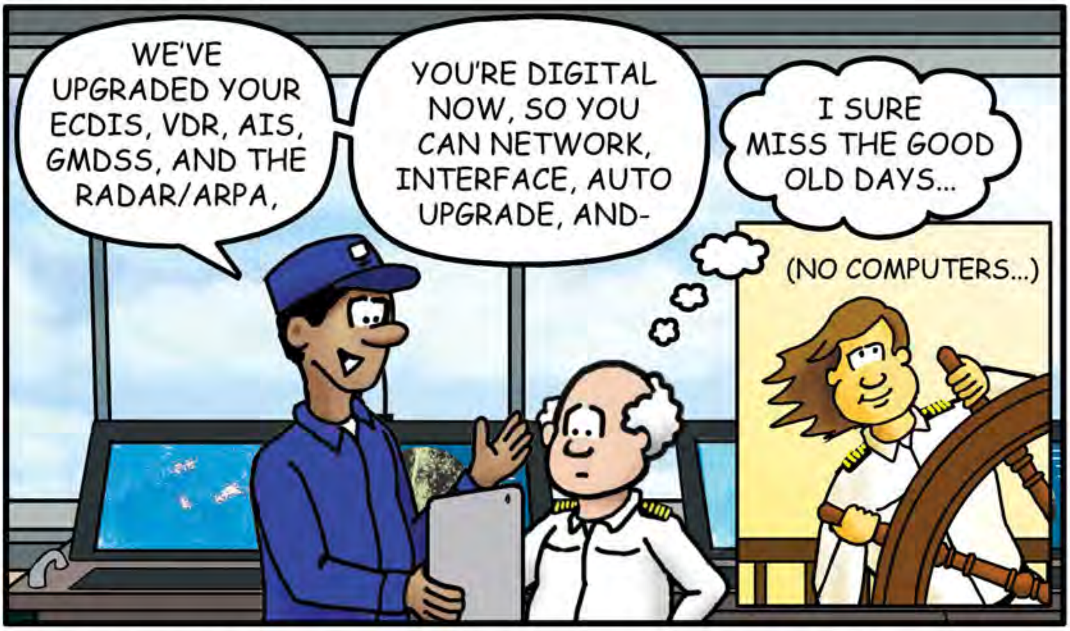

DEAD IN THE WATER FOR THREE DAYS...
ALL THANKS TO THOSE FANCY COMPUTERS WE GOT.
THOSE SYSTEMS WERE WORKING FINE!
UNTIL WE WERE HACKED...
SO WHAT CAN WE DO TO PREVENT ANOTHER INCIDENT LIKE THIS ONE?
WELL, I RECOMMEND THAT WE START WITH A CYBER SECURITY RISK ASSESSMENT!
TWO WEEKS LATER...

CYBER SECURITY RISK ASSESSMENT

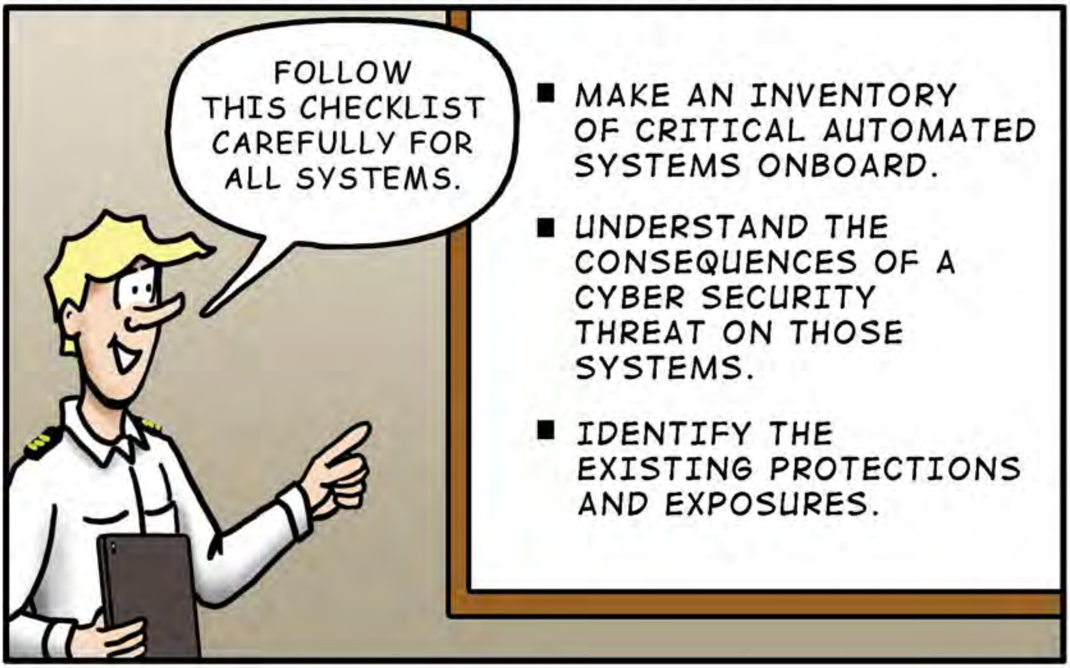

FIRST, WE SHOULD IDENTIFY ALL CRITICAL SYSTEMS.
THE BIG SCREEN TV IN THE LOUNGE! AND, THE COFFEE MAKER!
I'M SURE THEY MEAN STUFF LIKE THE NAVIGATIONAL SYSTEMS, RAGNAR, AND -
OH, AND THE WI-FI!
I'VE GOT A BIG ONLINE POKER TOURNAMENT TONIGHT!
SIGH... SO, CRITICAL SYSTEMS ARE... ?
THOSE THAT CAN CRIPPLE THE SHIP IF ATTACKED, SUCH AS-
• BRIDGE SYSTEMS
• COMMUNICATIONS
• PROPULSION AND MACHINERY
• CARGO MANAGEMENT SYSTEMS

IDENTIFYING CRITICAL SYSTEMS

BRIDGE SYSTEMS


WE'VE UPGRADED YOUR ECDIS, VDR, AIS, GMDSS, AND THE RADAR/ARPA,
YOU'RE DIGITAL NOW, SO YOU CAN NETWORK, INTERFACE, AUTO UPGRADE, AND-
I SURE MISS THE GOOD OLD DAYS...
(NO COMPUTERS...)

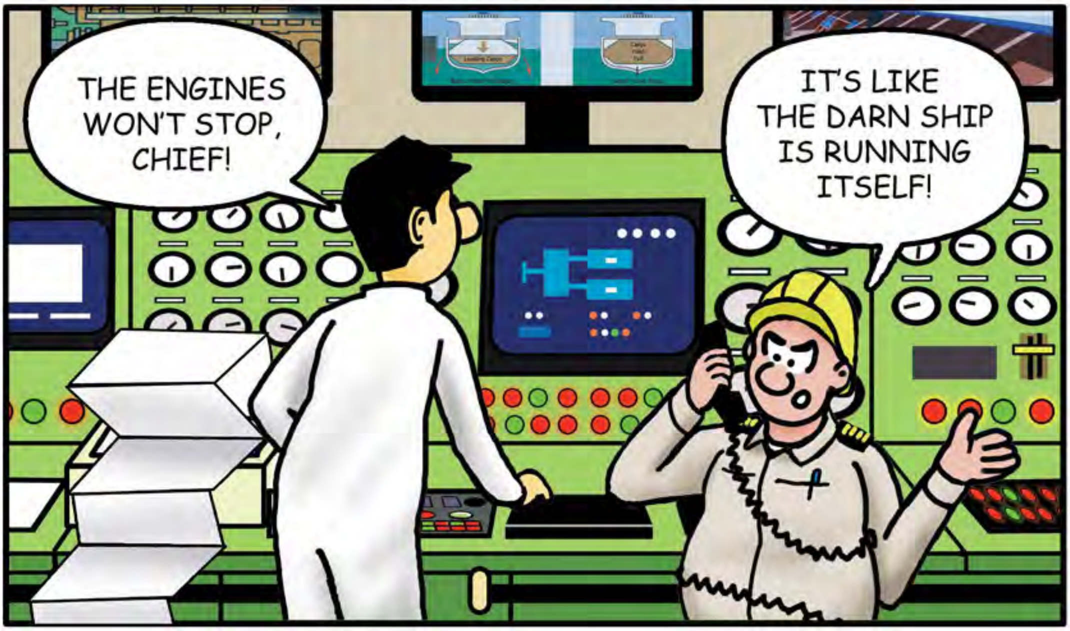
THE BRIDGE HAS MANY SYSTEMS, SOME OF WHICH MAY BE VULNERABLE TO AN OUTSIDE INTERFERENCE.



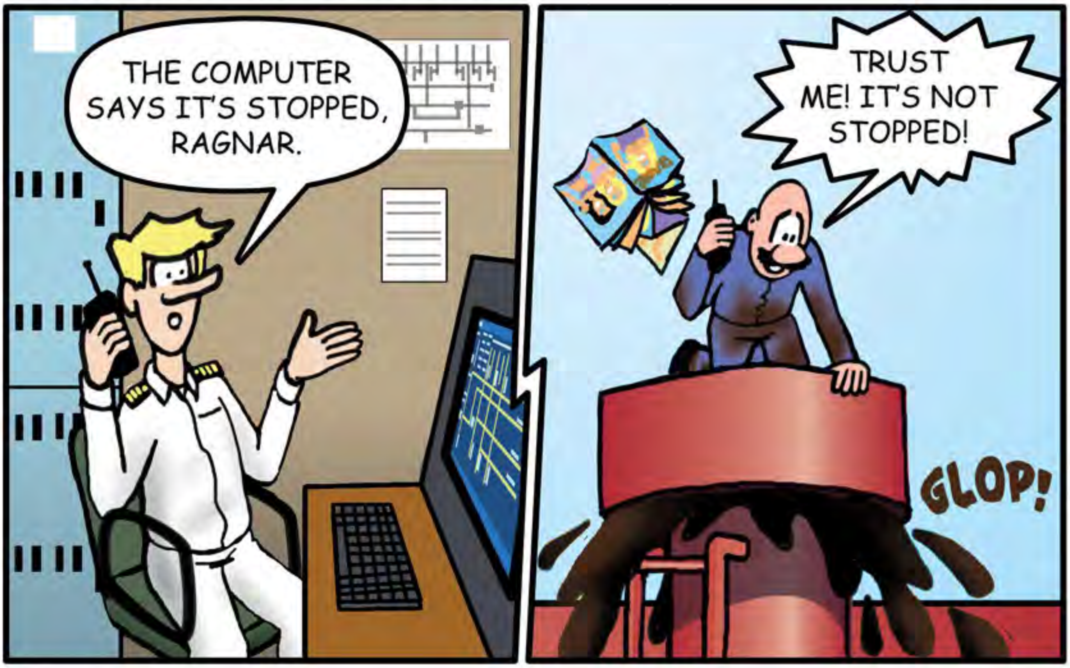
- MAKE AN INVENTORY OF CRITICAL AUTOMATED SYSTEMS ONBOARD.
- UNDERSTAND THE CONSEQUENCES OF A CYBER SECURITY THREAT ON THOSE SYSTEMS.
- IDENTIFY THE EXISTING PROTECTIONS AND EXPOSURES.

IDENTIFYING CRITICAL SYSTEMS

PROPULSION AND MACHINERY SYSTEMS

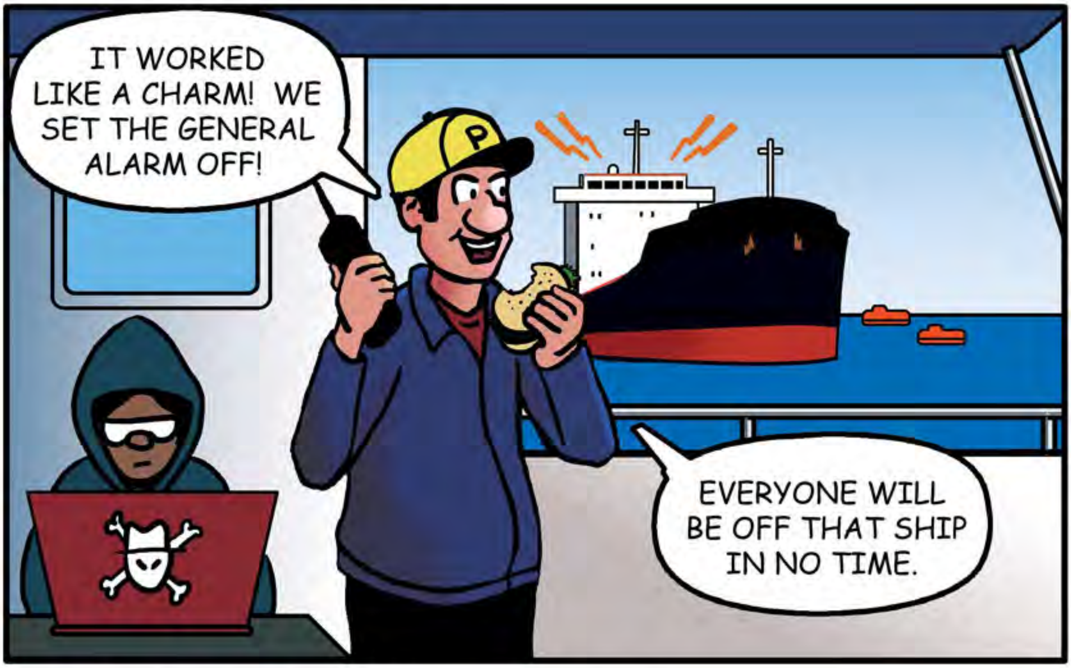

THE ENGINES WON'T STOP, CHIEF!
IT'S LIKE THE DARN SHIP IS RUNNING ITSELF!

CARGO MANAGEMENT SYSTEMS

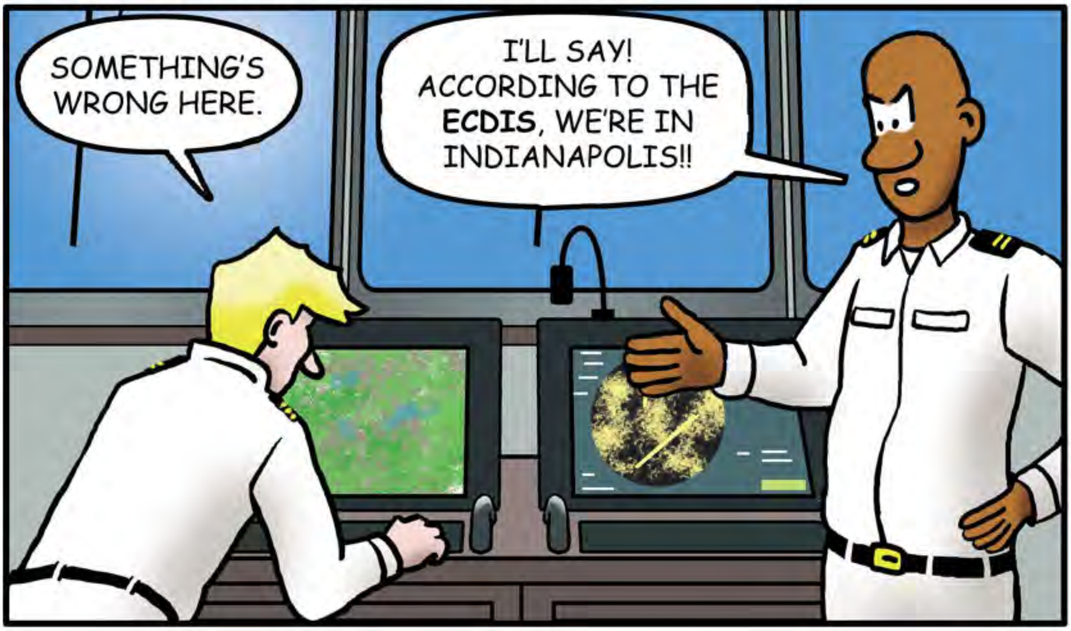

THE COMPUTER SAYS IT'S STOPPED, RAGNAR.
TRUST ME! IT'S NOT STOPPED!
GLOP!

IDENTIFYING CRITICAL SYSTEMS

COMMUNICATION SYSTEMS


IT WORKED LIKE A CHARM! WE SET THE GENERAL ALARM OFF!
P
EVERYONE WILL BE OFF THAT SHIP IN NO TIME.

AND DID WE MENTION BRIDGE SYSTEMS?



ONCE CRITICAL SYSTEMS ARE IDENTIFIED, WE NEED TO LOOK AT POSSIBLE THREATS TO THOSE SYSTEMS,

IDENTIFYING THREATS

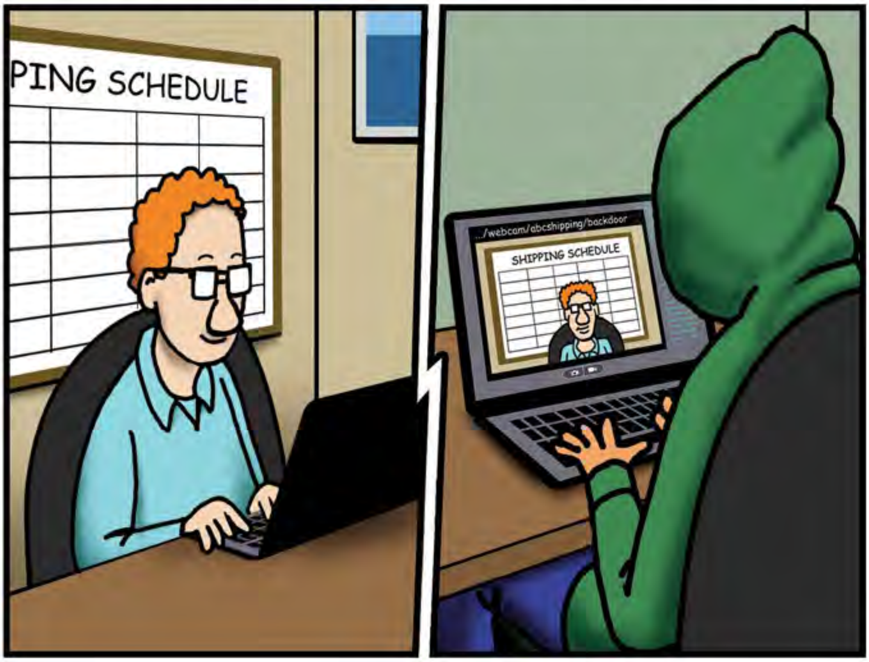
THERE ARE INTERNAL THREATS, USUALLY CAUSED BY HUMAN ERROR, CARELESSNESS, OR LACK OF AWARENESS.

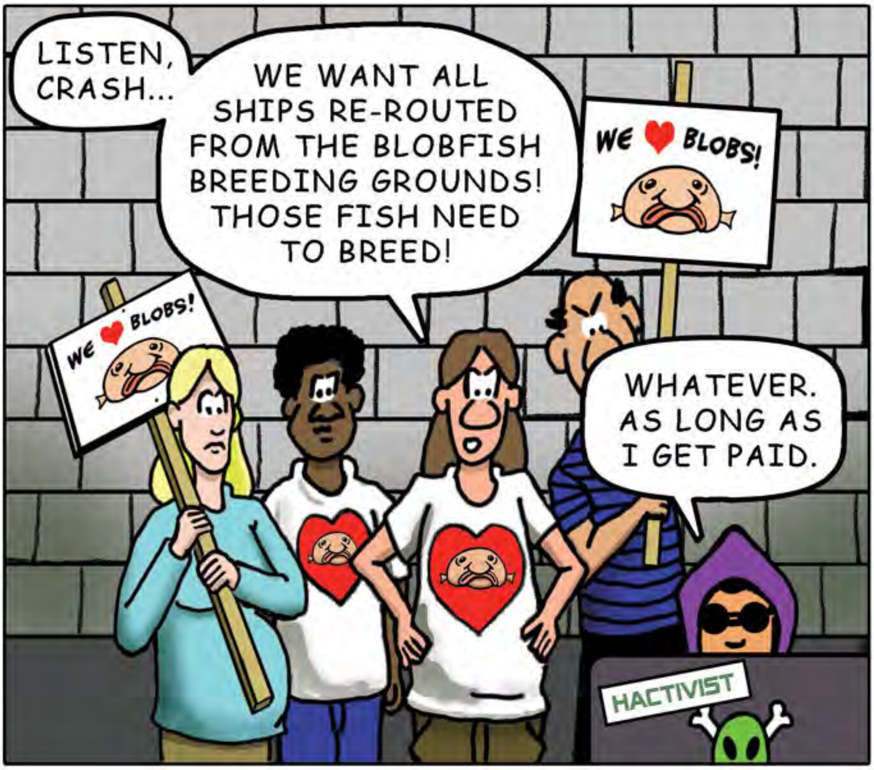
INTERNET CAFE

AND MANY EXTERNAL THREATS, SUCH AS THOSE FROM ACTIVISTS, CRIMINALS, AND OPPORTUNISTS.

THREAT ACTORS

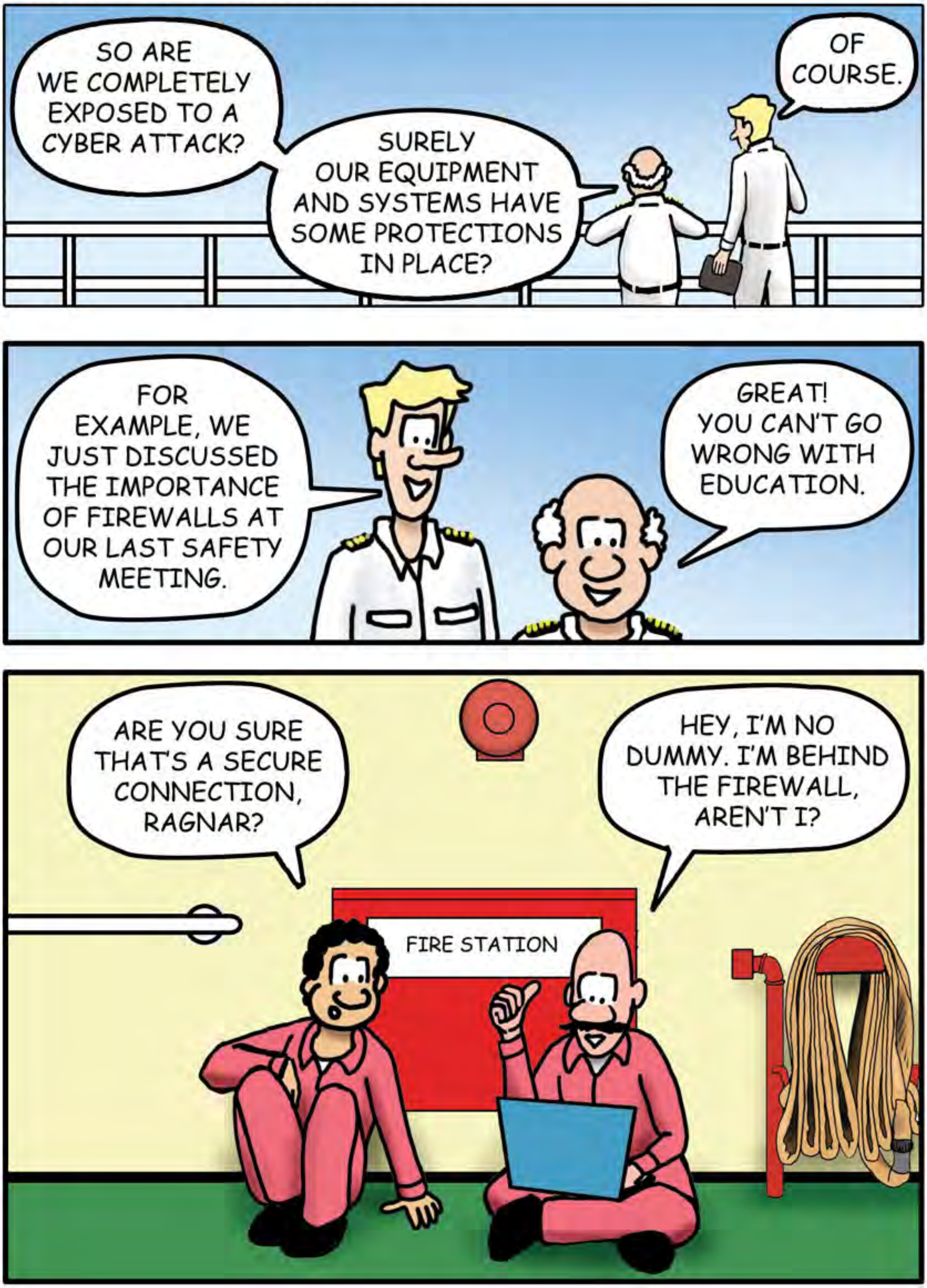
THESE GROUPS HAVE THE SKILLS AND RESOURCES TO THREATEN THE SECURITY AND SAFETY OF SHIPS.



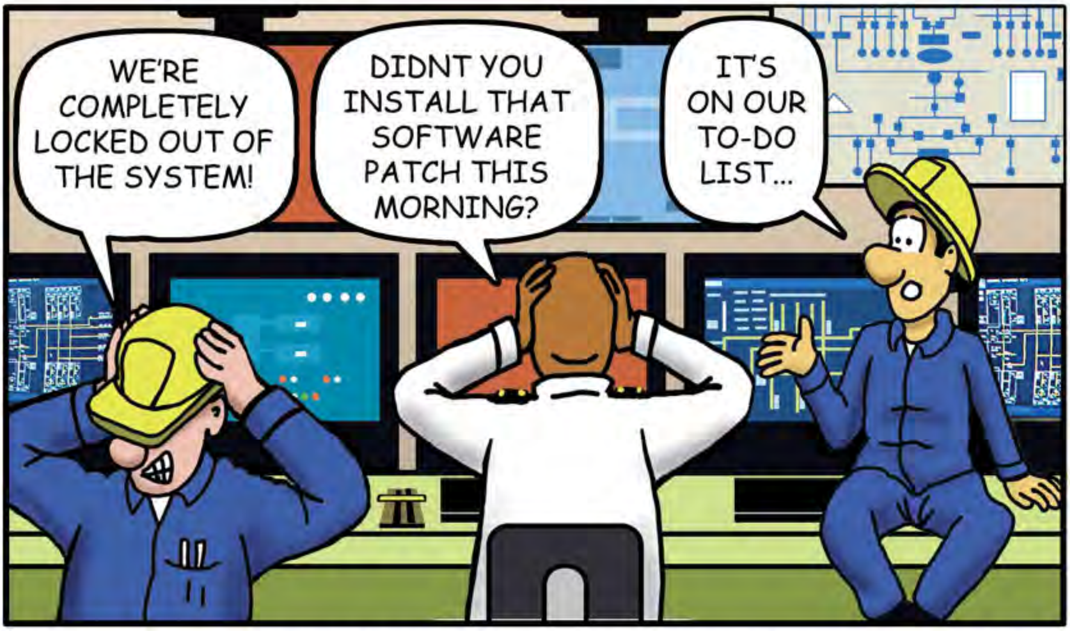

LISTEN, CRASH...
WE WANT ALL SHIPS RE-ROUTED FROM THE BLOBFISH BREEDING GROUNDS! THOSE FISH NEED TO BREED!
WE ♥ BLOBS!
WE ♥ BLOBS!
WHATEVER. AS LONG AS I GET PAID.
HACTIVIST

IDENTIFYING VULNERABILITIES

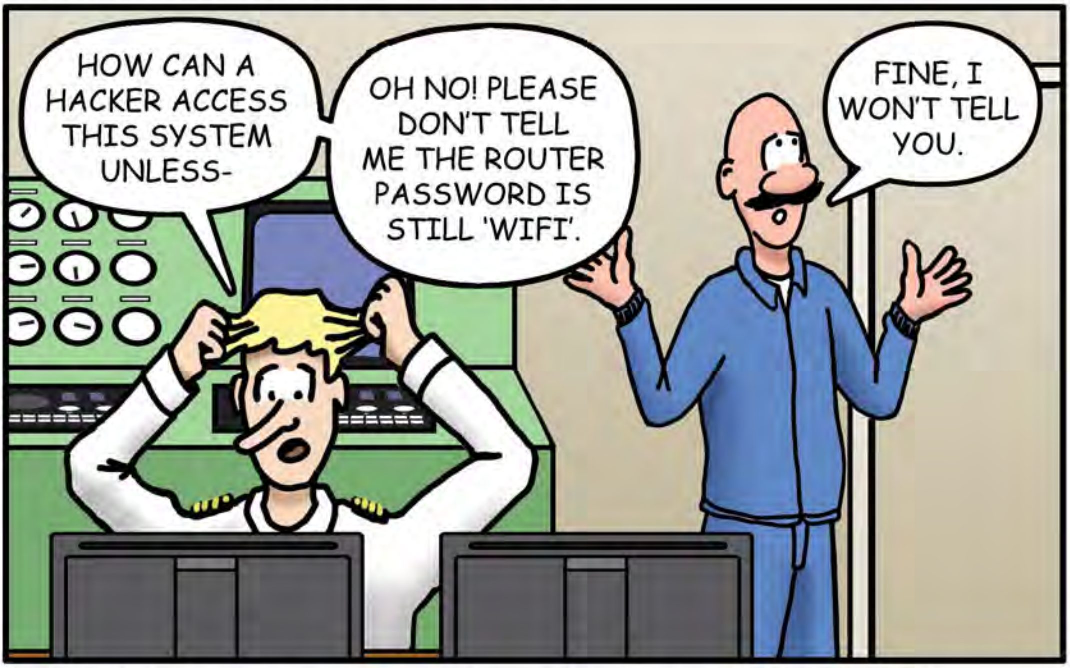
IDENTIFY CONTROLS THAT ARE ALREADY IN PLACE, AND ANY SPECIFIC VULNERABILITIES.


SO ARE WE COMPLETELY EXPOSED TO A CYBER ATTACK?
SURELY OUR EQUIPMENT AND SYSTEMS HAVE SOME PROTECTIONS IN PLACE?
OF COURSE.
FOR EXAMPLE, WE JUST DISCUSSED THE IMPORTANCE OF FIREWALLS AT OUR LAST SAFETY MEETING.
GREAT! YOU CAN'T GO WRONG WITH EDUCATION.
ARE YOU SURE THAT'S A SECURE CONNECTION, RAGNAR?
HEY, I'M NO DUMMY. I'M BEHIND THE FIREWALL, AREN'T I?
FIRE STATION

COMMON CYBER VULNERABILITIES CAN INCLUDE OLD OPERATING SYSTEMS, MISSING OR OUTDATED ANTIVIRUS SOFTWARE, AND UNPATCHED IT SYSTEMS.


WE'RE COMPLETELY LOCKED OUT OF THE SYSTEM!
DIDNT YOU INSTALL THAT SOFTWARE PATCH THIS MORNING?
IT'S ON OUR TO-DO LIST...

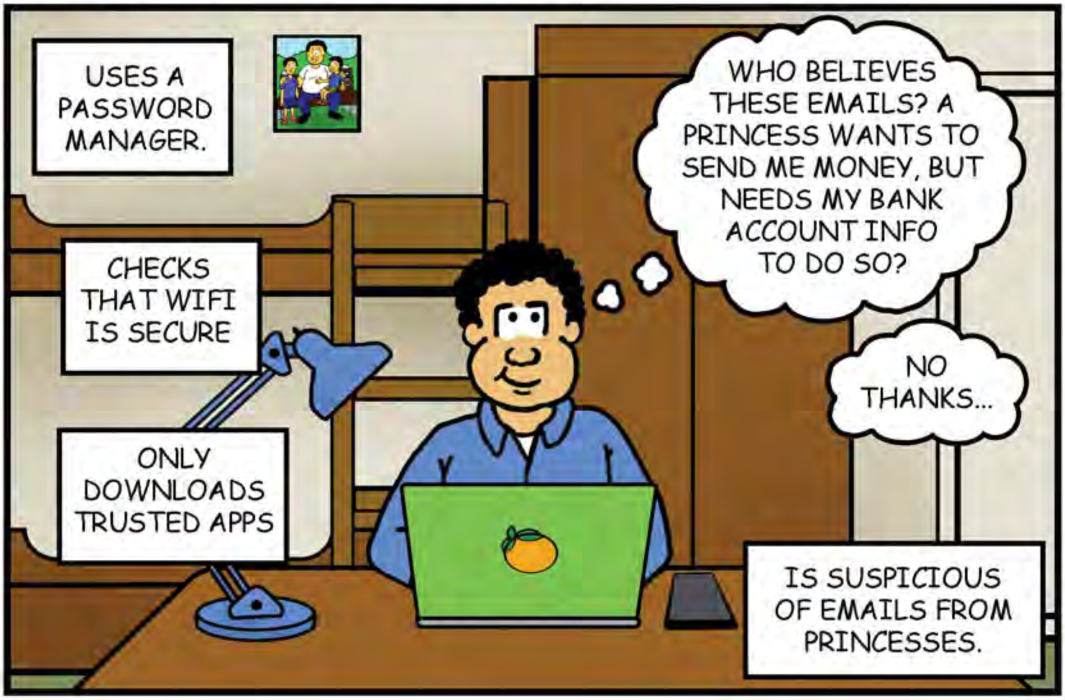
COMMON MISTAKES CAN INVOLVE STOCK PASSWORDS NOT BEING CHANGED OR LEFT OUT IN THE OPEN.


HOW CAN A HACKER ACCESS THIS SYSTEM UNLESS-
OH NO! PLEASE DON'T TELL ME THE ROUTER PASSWORD IS STILL 'WIFI'.
FINE, I WON'T TELL YOU.

REVIEWING BEST PRACTICES WITH ALL CREW MEMBERS CAN PREVENT MANY FUTURE PROBLEMS.

ELECTRONIC COMMUNICATIONS: BEST PRACTICES

DO BE CAUTIOUS, LIKE GEORGE.

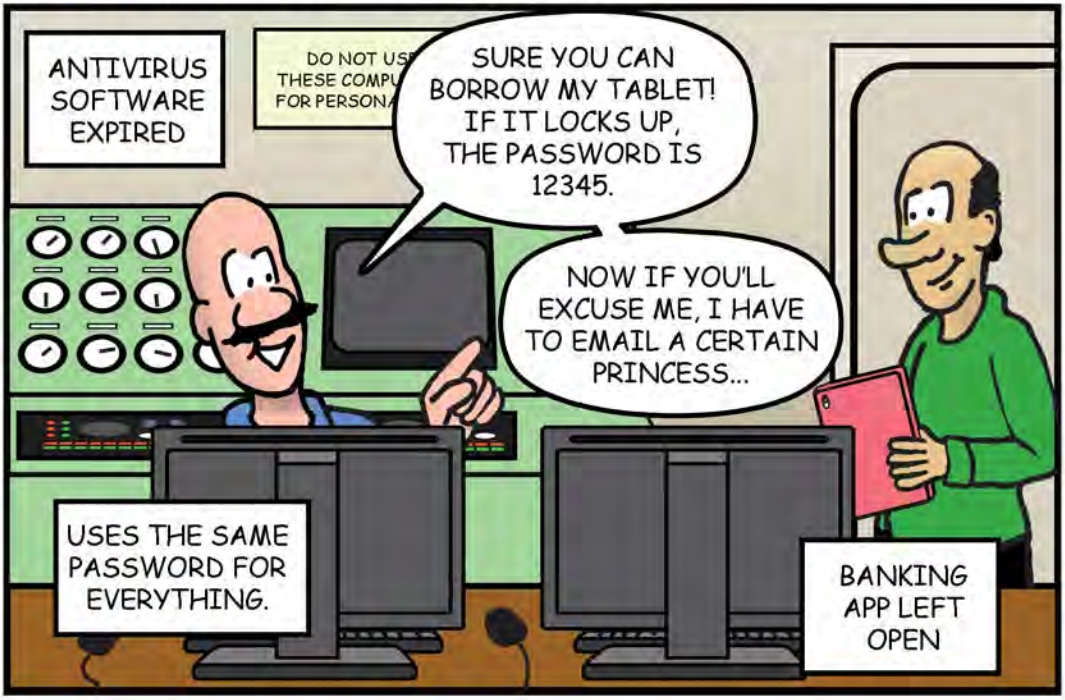

USES A PASSWORD MANAGER.
CHECKS THAT WIFI IS SECURE
ONLY DOWNLOADS TRUSTED APPS
WHO BELIEVES THESE EMAILS? A PRINCESS WANTS TO SEND ME MONEY, BUT NEEDS MY BANK ACCOUNT INFO TO DO SO?
NO THANKS...
IS SUSPICIOUS OF EMAILS FROM PRINCESSES.

USE LENGTHY PASSWORDS. PASSWORDS SHOULD HAVE 14 OR MORE CHARACTERS CONTAINING AT LEAST ONE NUMBER, ONE UPPERCASE LETTER, AND ONE SYMBOL (E.G. $, @, ?, #)

ONLY PERSONAL DEVICES AND USB DRIVES FROM A TRUSTED SUPPLIER SHOULD BE USED ONBOARD.

INSTALL, REGISTER AND RENEW ANTIVIRUS, ANTISPYWARE AND FIREWALL PACKAGES ON PERSONAL DEVICES.

DON'T BE CARELESS LIKE RAGNAR.


ANTIVIRUS SOFTWARE EXPIRED
DO NOT US THESE COMPU FOR PERSONA
SURE YOU CAN BORROW MY TABLET! IF IT LOCKS UP, THE PASSWORD IS 12345.
NOW IF YOU'LL EXCUSE ME, I HAVE TO EMAIL A CERTAIN PRINCESS...
USES THE SAME PASSWORD FOR EVERYTHING.
BANKING APP LEFT OPEN

BE SUSPICIOUS OF EXTERNAL DOWNLOADS AND EMAILS. VERIFY THE AUTHENTICITY OF UNEXPECTED EMAILS, ESPECIALLY THOSE WITH ATTACHMENTS AND LINKS.

BOTH PERSONAL AND SHIPBOARD DEVICES SHOULD NEVER BE LEFT UNLOCKED WHILE UNATTENDED.

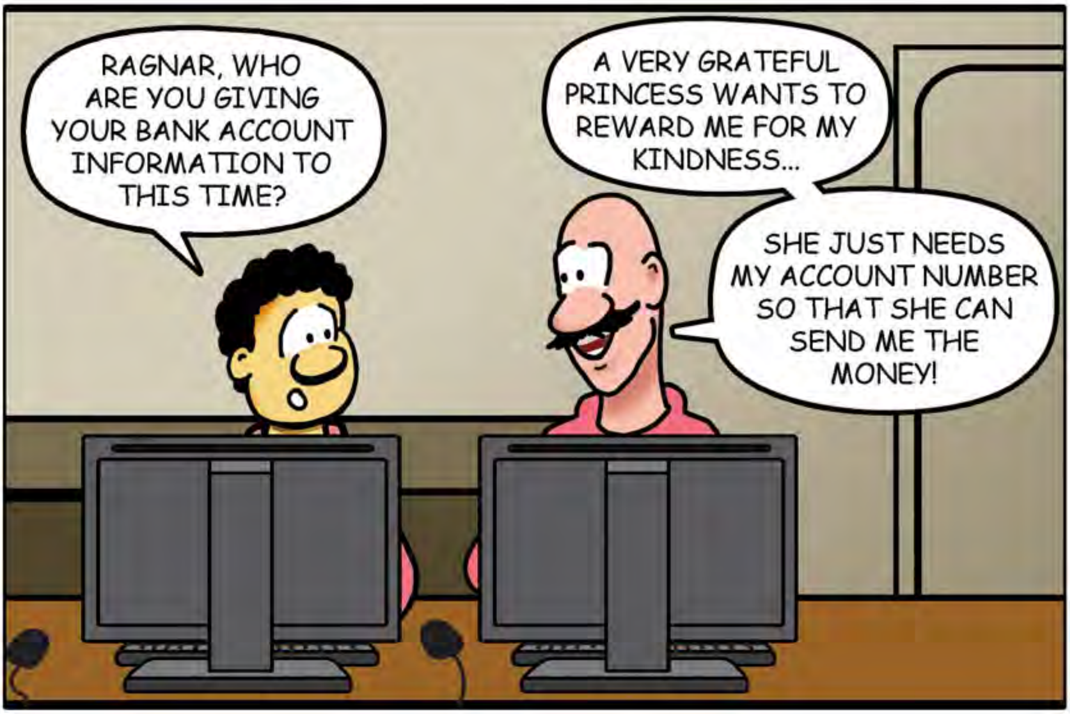
ONLY USE YOUR COMPANY'S PRIVATE WI-FI NETWORK, WHICH SHOULD BE ENCRYPTED, SECURED, AND HIDDEN.

CYBER WELLNESS CONSIDERATIONS

CYBER WELLNESS PERTAINS TO THE POSITIVE WELLBEING, RESPONSIBLE BEHAVIOR, AND GOOD CHOICES OF INTERNET USERS.

CLICK WISELY!
BULLYING?
ILLEGAL?
SPAM?

BE CAREFUL WHO YOU MEET AND TRUST ONLINE! A FRAUDSTER COULD USE YOUR BANK ACCOUNT INFORMATION, CREDIT CARDS, OR SOCIAL SECURITY NUMBER TO STEAL FROM YOU!


RAGNAR, WHO ARE YOU GIVING YOUR BANK ACCOUNT INFORMATION TO THIS TIME?
A VERY GRATEFUL PRINCESS WANTS TO REWARD ME FOR MY KINDNESS...
SHE JUST NEEDS MY ACCOUNT NUMBER SO THAT SHE CAN SEND ME THE MONEY!

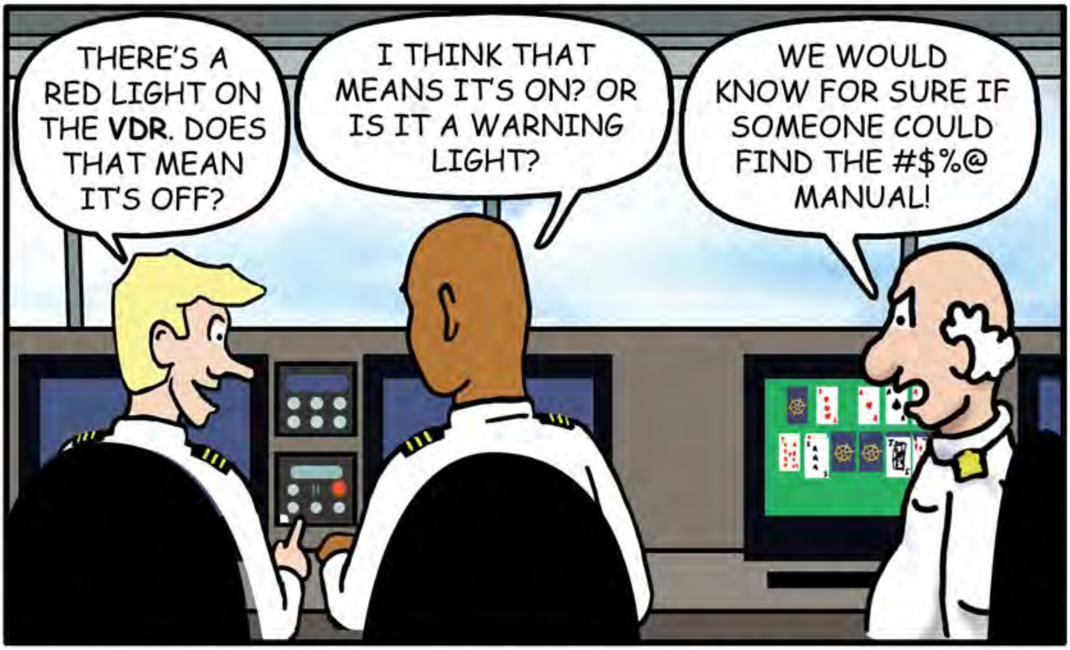
THERE ARE PERSONAL RISK FACTORS ASSOCIATED WITH CYBER CONNECTIVITY, INCLUDING INAPPROPRIATE OR OVERUSE OF MOBILE DEVICES...

I CAN'T STOP NOW! I'M AT MY HIGHEST SCORE EVER!
BLEEP! BLEEP! BLEEP!
I NEED TO SLEEP!

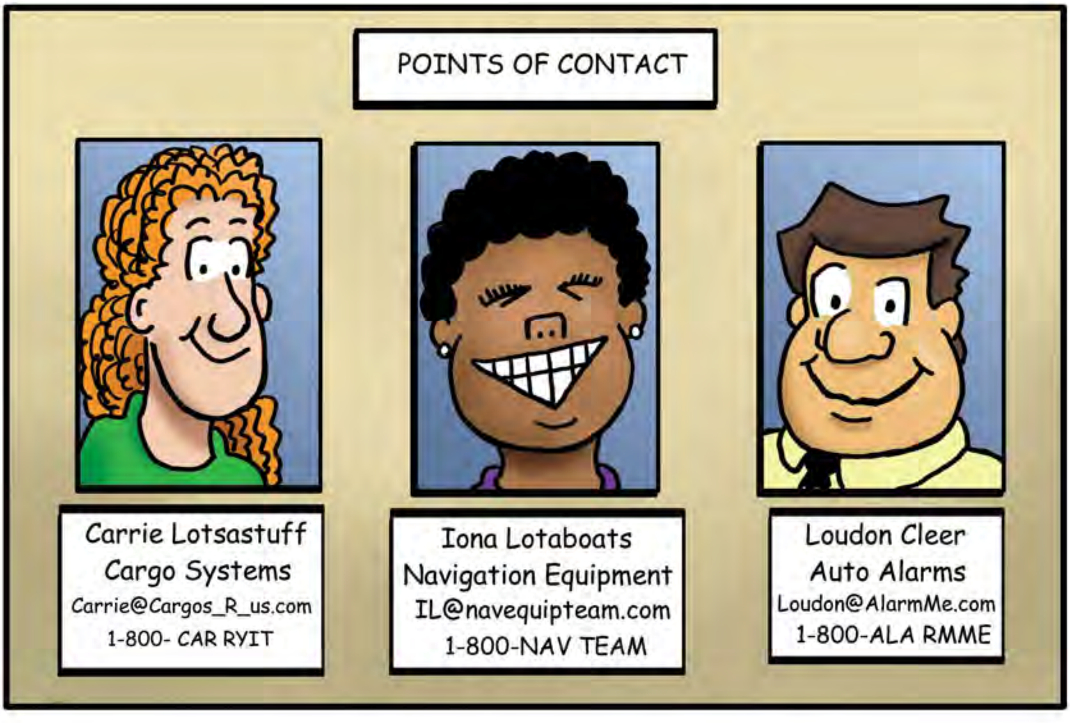
KEEP POSTING AND BEHAVIOR ON SOCIAL MEDIA POSITIVE AND PROFESSIONAL, ESPECIALLY ON THE JOB!

SO I POSTED SOME PICS OF THE CREW HAVING A WILD PARTY? WHO CARES?
IT HAD NOTHING TO DO WITH THAT ACCIDENT THE NEXT MORNING!
APPARENTLY THE INSURANCE COMPANY CARES!! A LOT!!

CYBER SECURITY PROCEDURES DETAILING THE PROPER USE OF SYSTEMS AND THEIR MAINTENANCE ROUTINES SHOULD BE KEPT UP TO DATE AND READILY AVAILABLE.

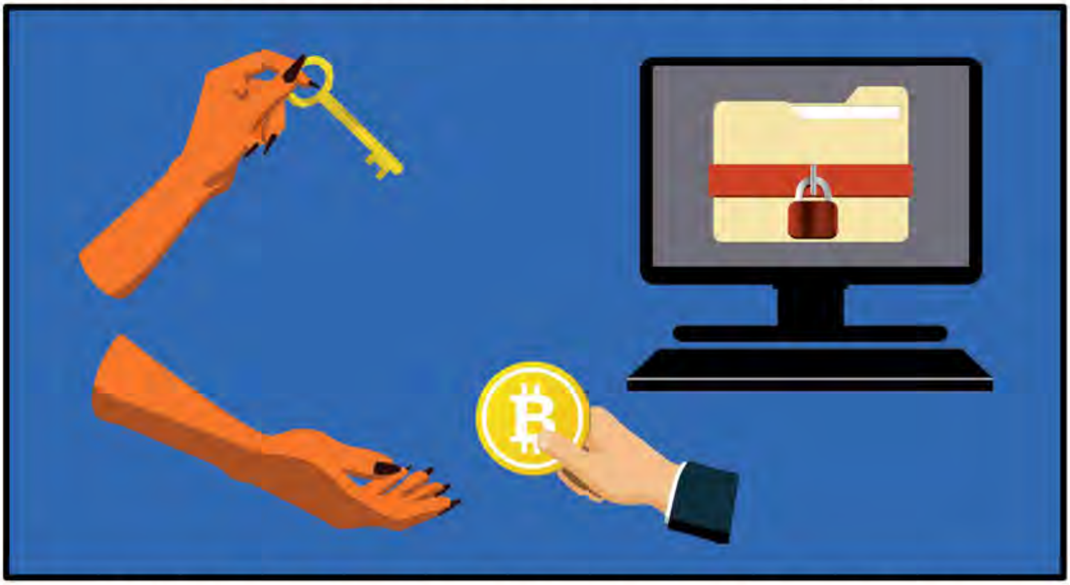

THERE'S A RED LIGHT ON THE **VDR**. DOES THAT MEAN IT'S OFF?
I THINK THAT MEANS IT'S ON? OR IS IT A WARNING LIGHT?
WE WOULD KNOW FOR SURE IF SOMEONE COULD FIND THE #$%@ MANUAL!

PROCEDURES SHOULD ALSO IDENTIFY CYBER SECURITY POINTS OF CONTACT WITHIN YOUR ORGANIZATION, AND AT EACH SERVICE PROVIDER'S OFFICE.

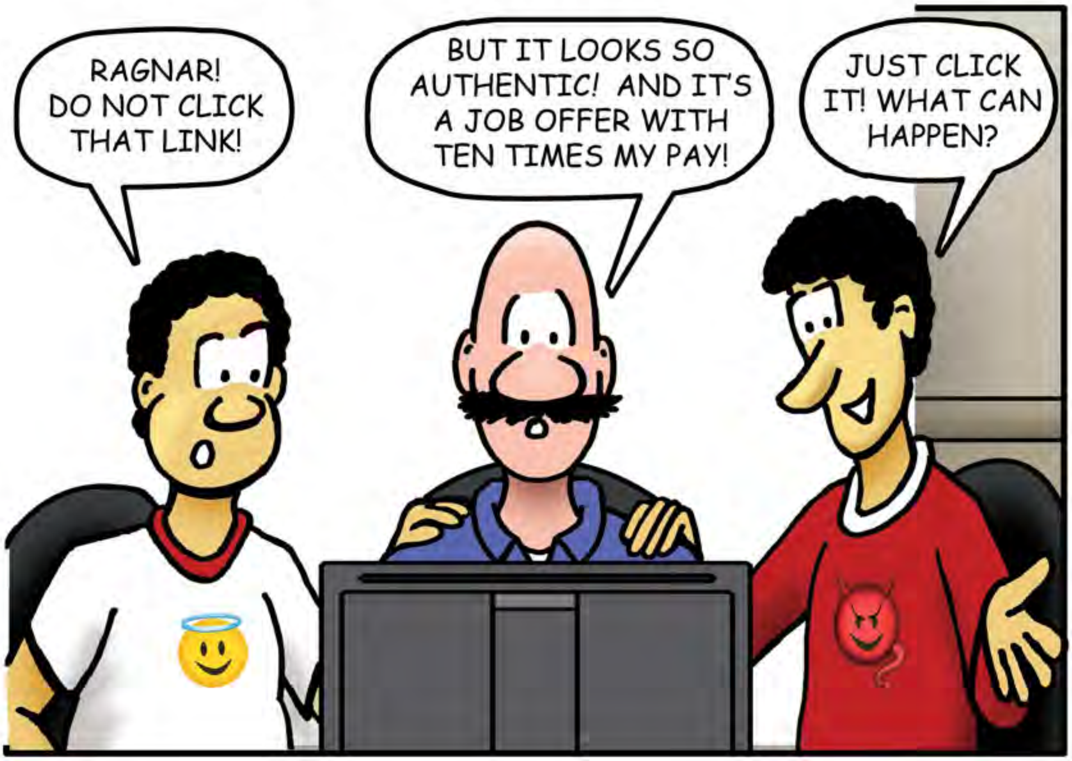

POINTS OF CONTACT
Carrie Lotsastuff Cargo Systems Carrie@Cargos_R_us.com 1-800- CAR RYIT
Iona Lotaboats Navigation Equipment IL@navequipteam.com 1-800-NAV TEAM
Loudon Cleer Auto Alarms Loudon@AlarmMe.com 1-800-ALA RMME

THE THREAT OF RANSOMWARE

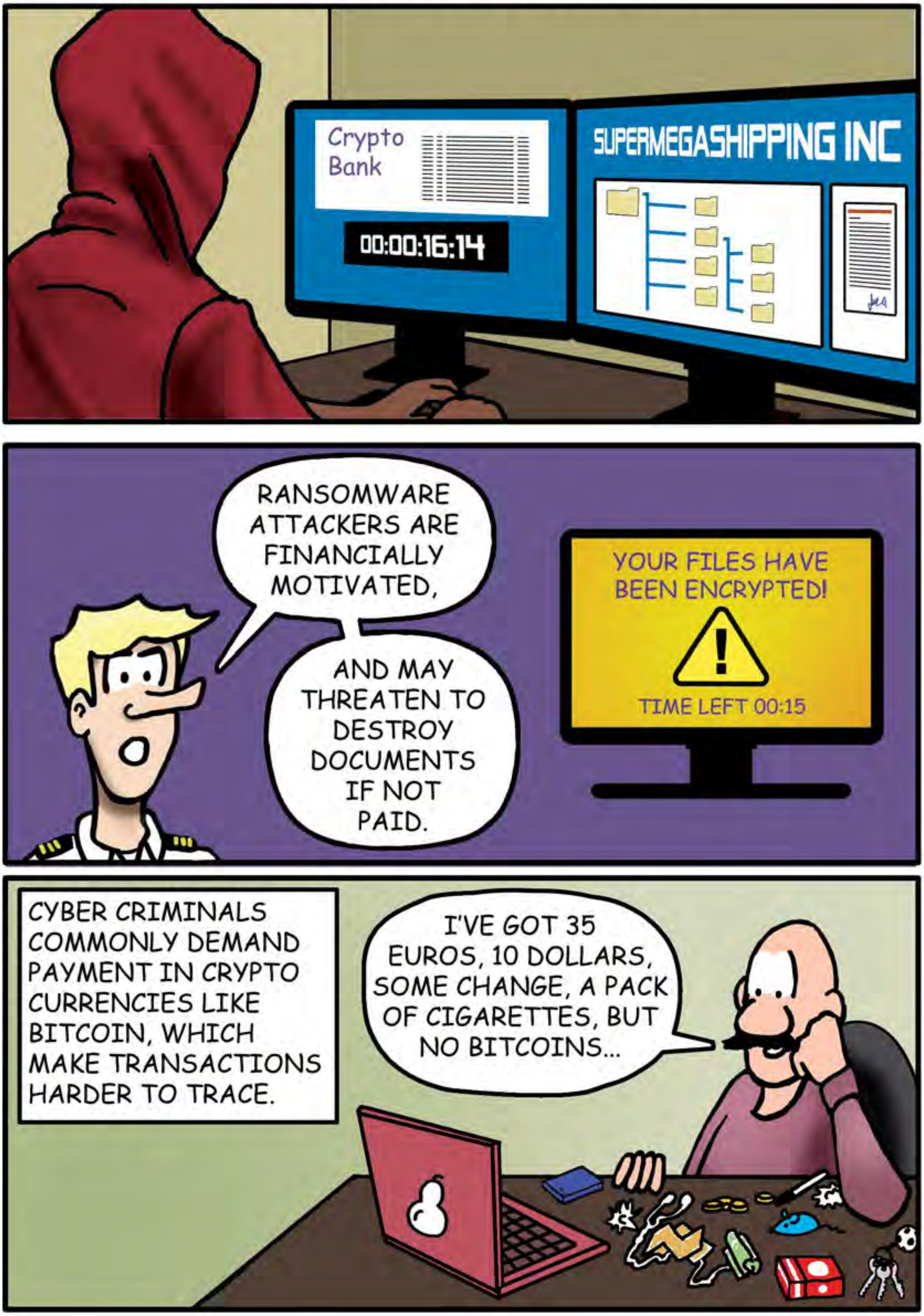
RANSOMWARE IS A TYPE OF MALICIOUS SOFTWARE DESIGNED TO ENCRYPT FILES OR LOCK YOU OUT OF YOUR COMPUTER ENTIRELY UNTIL A SUM OF MONEY IS PAID TO UNLOCK IT.



RANSOMWARE IS USUALLY INTRODUCED THROUGH A BOOBY-TRAPPED LINK OR ATTACHMENT IN AN EMAIL.

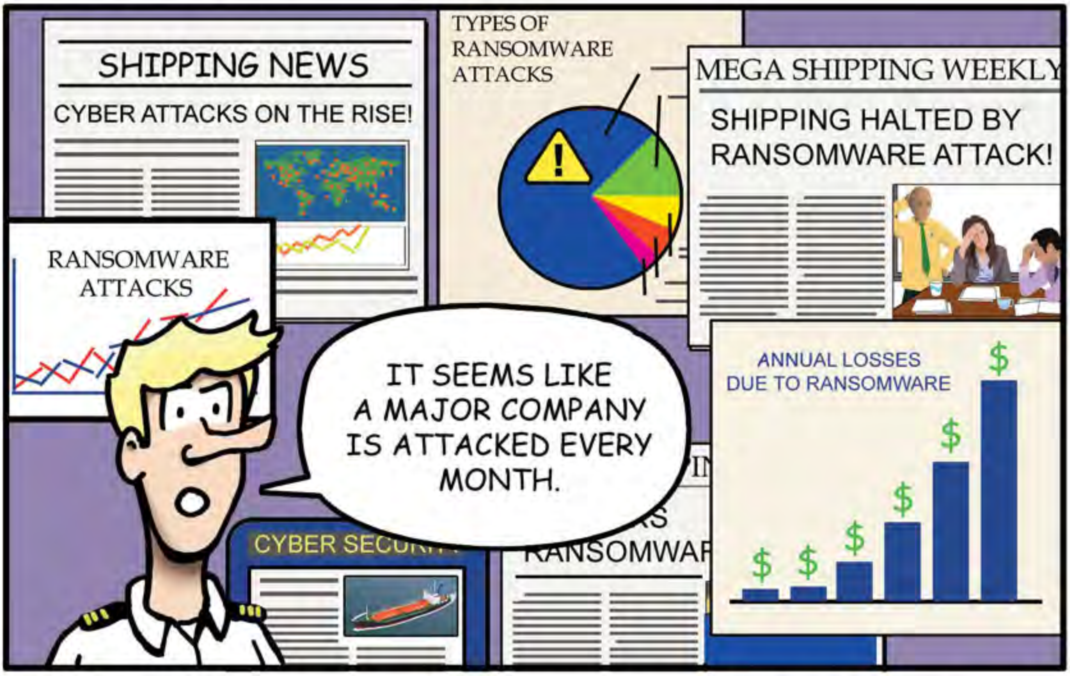

RAGNAR! DO NOT CLICK THAT LINK!
BUT IT LOOKS SO AUTHENTIC! AND IT'S A JOB OFFER WITH TEN TIMES MY PAY!
JUST CLICK IT! WHAT CAN HAPPEN?

RANSOMWARE IS A TERRIBLE ATTACK THAT CAN HAPPEN TO ANYONE FROM INDIVIDUALS TO LARGE COMPANIES.

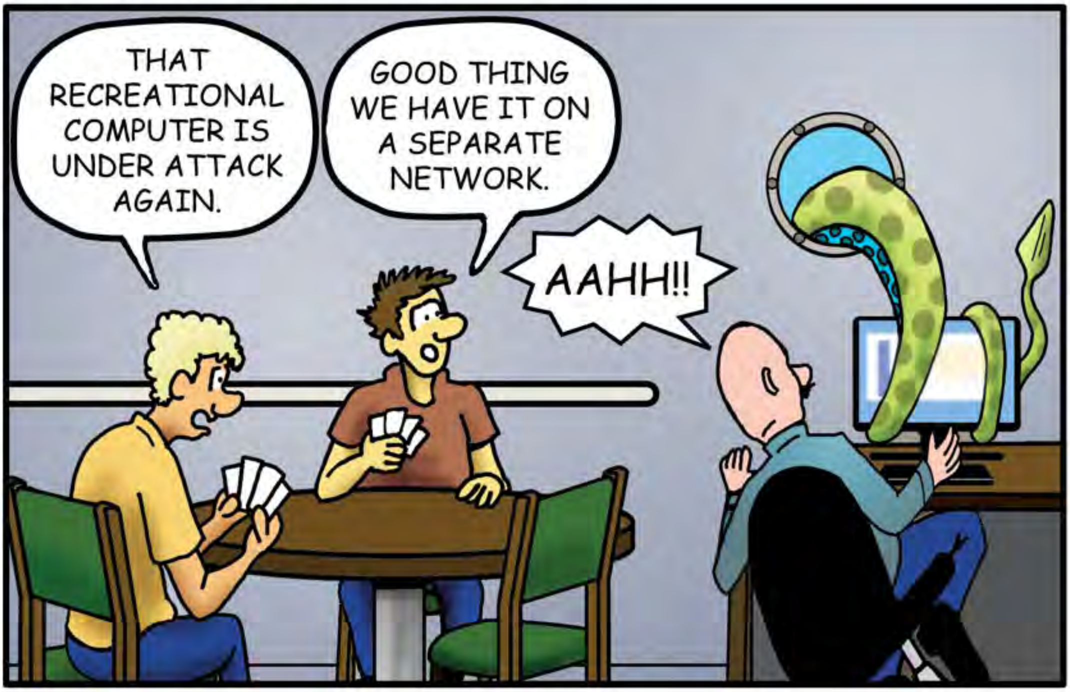

Crypto Bank
00:00:16:14
SUPERMEGASHIPPING INC
RANSOMWARE ATTACKERS ARE FINANCIALLY MOTIVATED,
AND MAY THREATEN TO DESTROY DOCUMENTS IF NOT PAID.
YOUR FILES HAVE BEEN ENCRYPTED!
TIME LEFT 00:15
CYBER CRIMINALS COMMONLY DEMAND PAYMENT IN CRYPTO CURRENCIES LIKE BITCOIN, WHICH MAKE TRANSACTIONS HARDER TO TRACE.
I'VE GOT 35 EUROS, 10 DOLLARS, SOME CHANGE, A PACK OF CIGARETTES, BUT NO BITCOINS...

RANSOMWARE OVERVIEW

RANSOMWARE IS POTENTIALLY THE MOST DAMAGING TYPE OF CYBER-ATTACK.

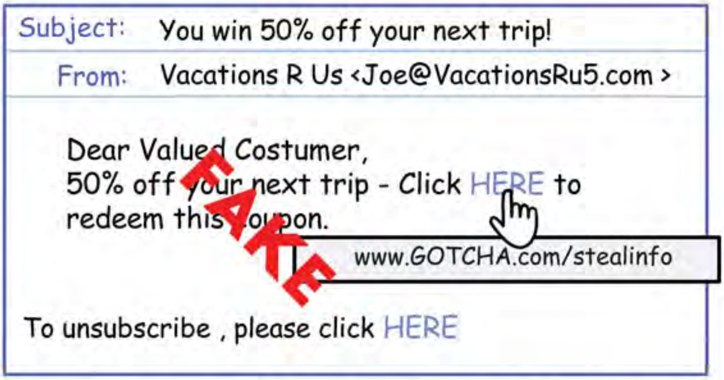

SHIPPING NEWS
CYBER ATTACKS ON THE RISE!
RANSOMWARE ATTACKS
TYPES OF RANSOMWARE ATTACKS
MEGA SHIPPING WEEKLY
SHIPPING HALTED BY RANSOMWARE ATTACK!
IT SEEMS LIKE A MAJOR COMPANY IS ATTACKED EVERY MONTH.
ANNUAL LOSSES DUE TO RANSOMWARE
$ $ $ $ $ $
CYBER SECU
RANSOMWAR

IF YOU EVEN SUSPECT A RANSOMWARE ATTACK, REPORT IT TO YOUR SUPERVISOR IMMEDIATELY! PREVENTION IS ULTIMATELY THE BEST DEFENSE.


THAT RECREATIONAL COMPUTER IS UNDER ATTACK AGAIN.
GOOD THING WE HAVE IT ON A SEPARATE NETWORK.
AAHH!!

RANSOMWARE : HOW TO DETECT IT

RANSOMWARE AND OTHER VIRUSES ARE USUALLY INTRODUCED THROUGH A BOOBY TRAPPED LINK OR ATTACHMENT, IN AN EMAIL THAT LOOKS CONVINCING.



Subject: You win 50% off your next trip!

From: Vacations R Us <Joe@VacationsRu5.com >

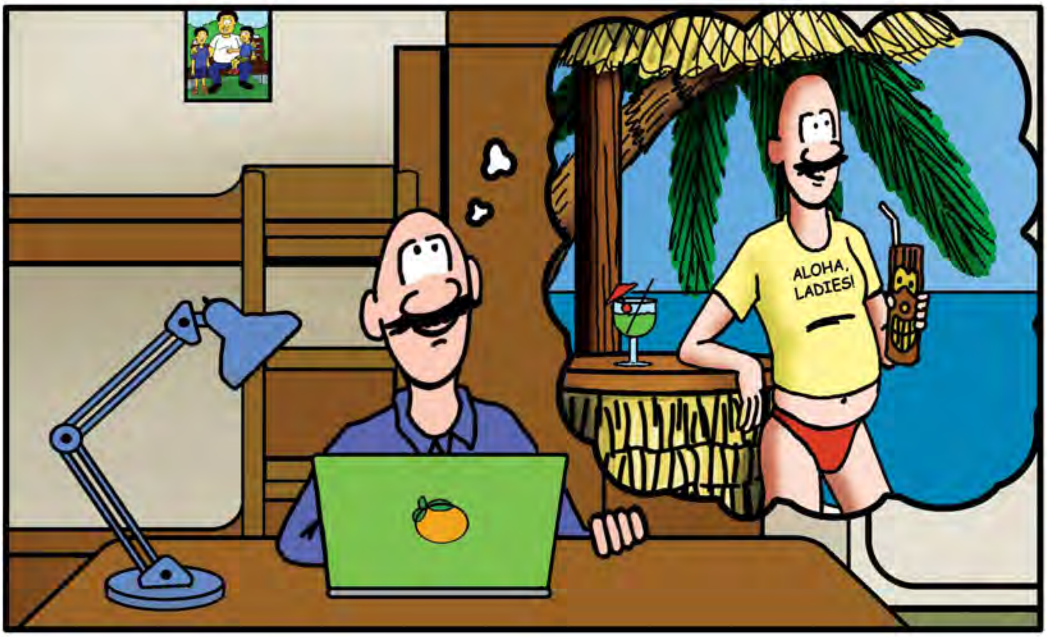
Dear Valued Costumer,
50% off your next trip - Click HERE to redeem this coupon.

www.GOTCHA.com/stealinfo

FAKE

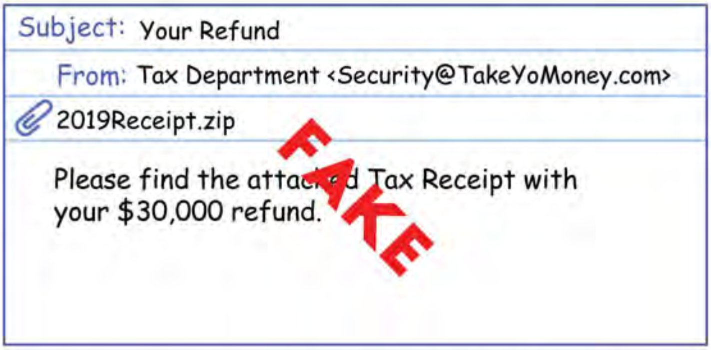
To unsubscribe , please click HERE

- EMAIL DOMAIN DOES NOT MATCH THE WEBSITE. LOOK FOR NUMBERS OR MISSPELLINGS SUCH AS @y0utube.com OR paypa1.com.
- LEGITIMATE COMPANIES WILL USE YOUR ACTUAL NAME.
- HOVER OVER LINKS WITHOUT CLICKING ON THEM TO REVEAL THE ACTUAL URL. IF IT DOES NOT MATCH THE CONTEXT OF THE EMAIL, DO NOT TRUST IT1



AND HOW TO DEFEND AGAINST IT.

BE ON THE LOOKOUT FOR HIGH-RISK ATTACHMENT FILE TYPES SUCH AS .exe, .scr, AND .zip WHICH REQUIRE A DOWNLOAD.


Subject: Your Refund

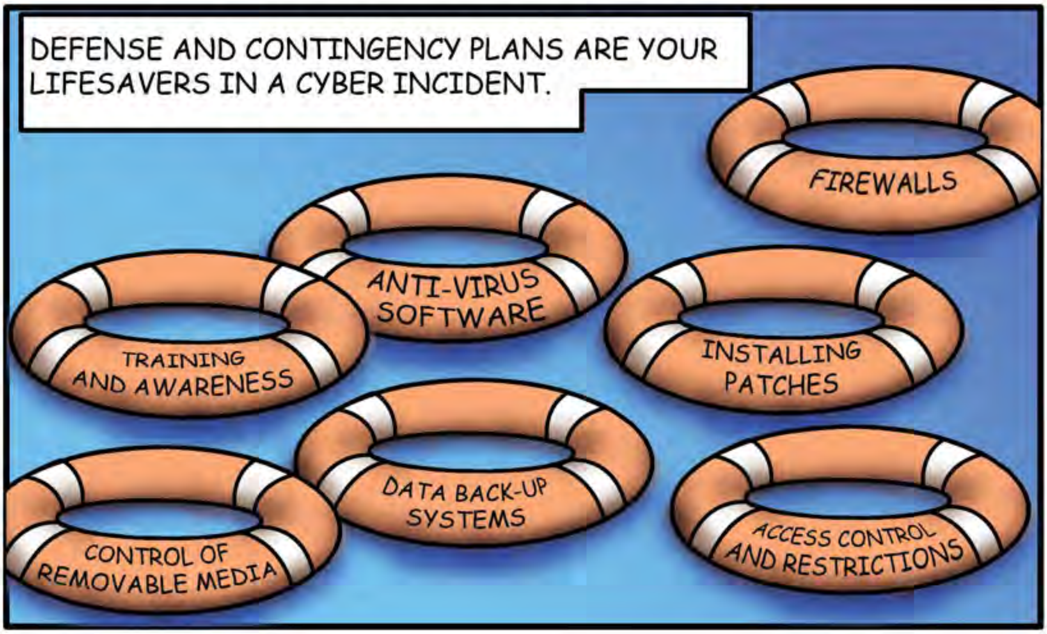
From: Tax Department <Security@TakeYoMoney.com>

2019Receipt.zip

Please find the attached Tax Receipt with your $30,000 refund.

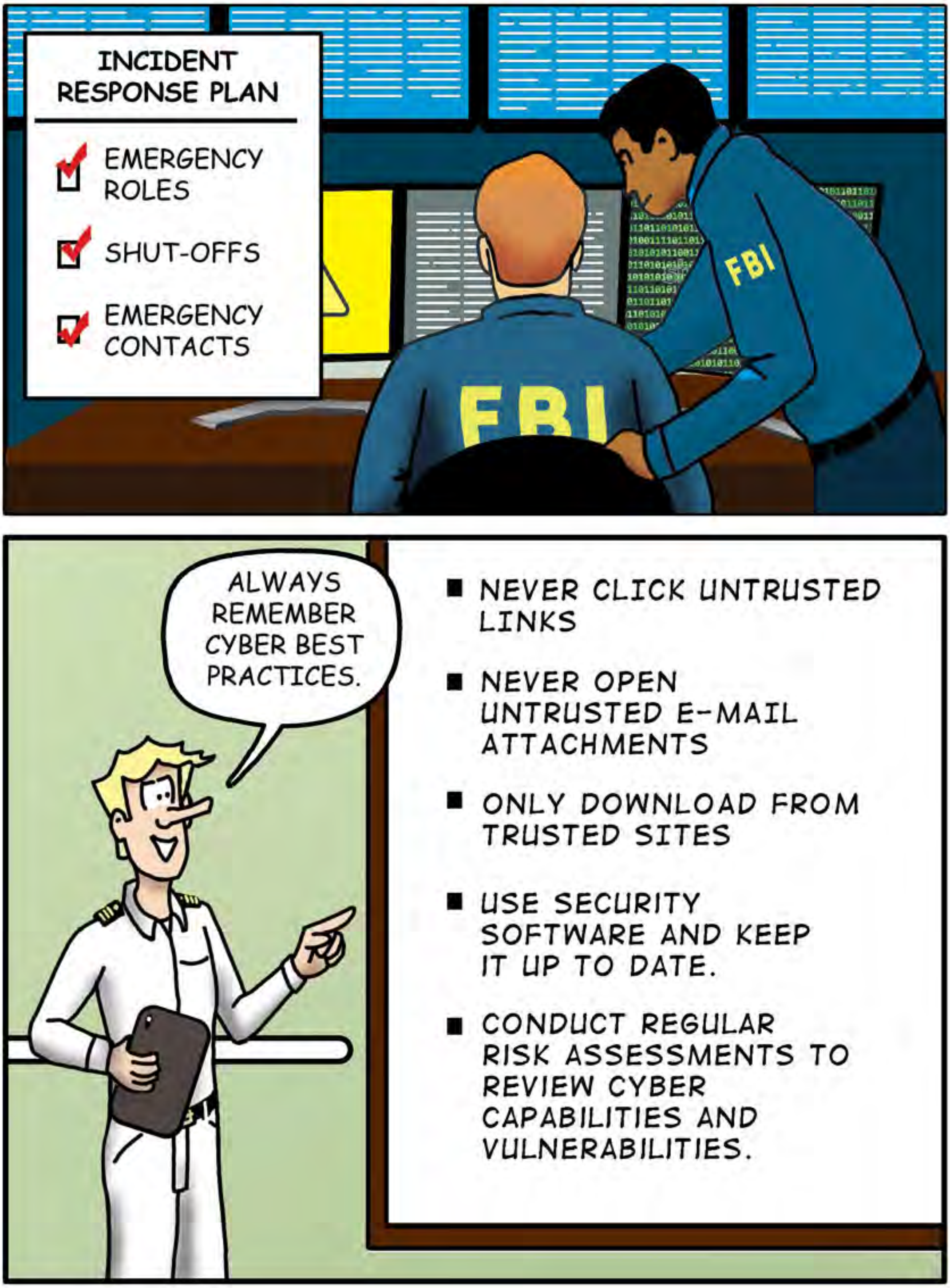
- AUTHENTIC INSTITUTIONS DO NOT RANDOMLY SEND YOU EMAILS WITH ATTACHMENTS, BUT INSTEAD DIRECT YOU TO DOWNLOAD DOCUMENTS OR FILES FROM THEIR WEBSITE.
- CYBER CRIMINALS ARE LIKELY TO ACT DURING TAX OR SHOPPING SEASONS WHEN THESE EMAILS ARE RELEVANT.

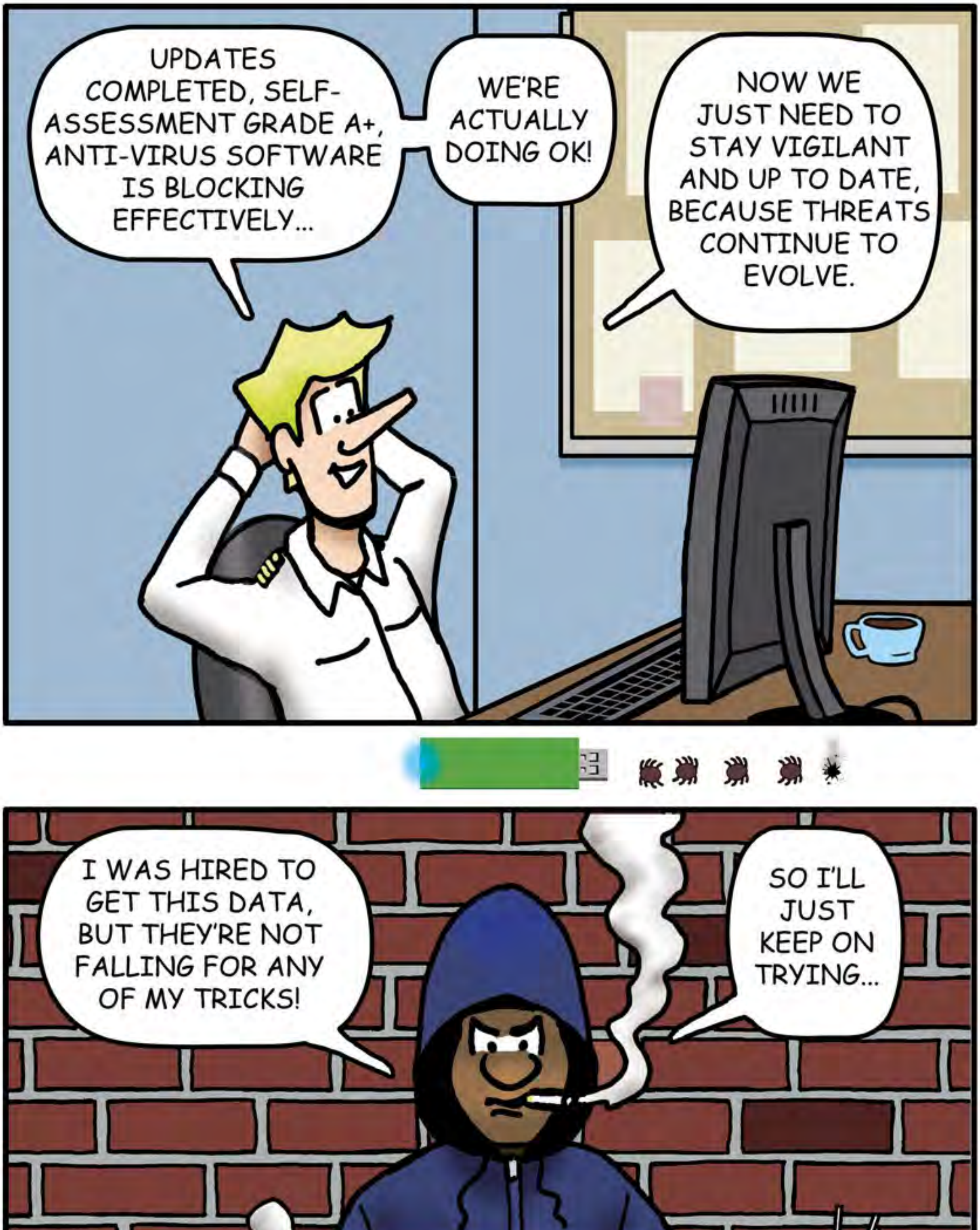
EMAIL SCAMS ARE BECOMING EVER MORE SOPHISTICATED. WE MUST BE ALERT, AWARE, AND SMART WHEN OPENING AND DOWNLOADING EMAIL ATTACHMENTS.

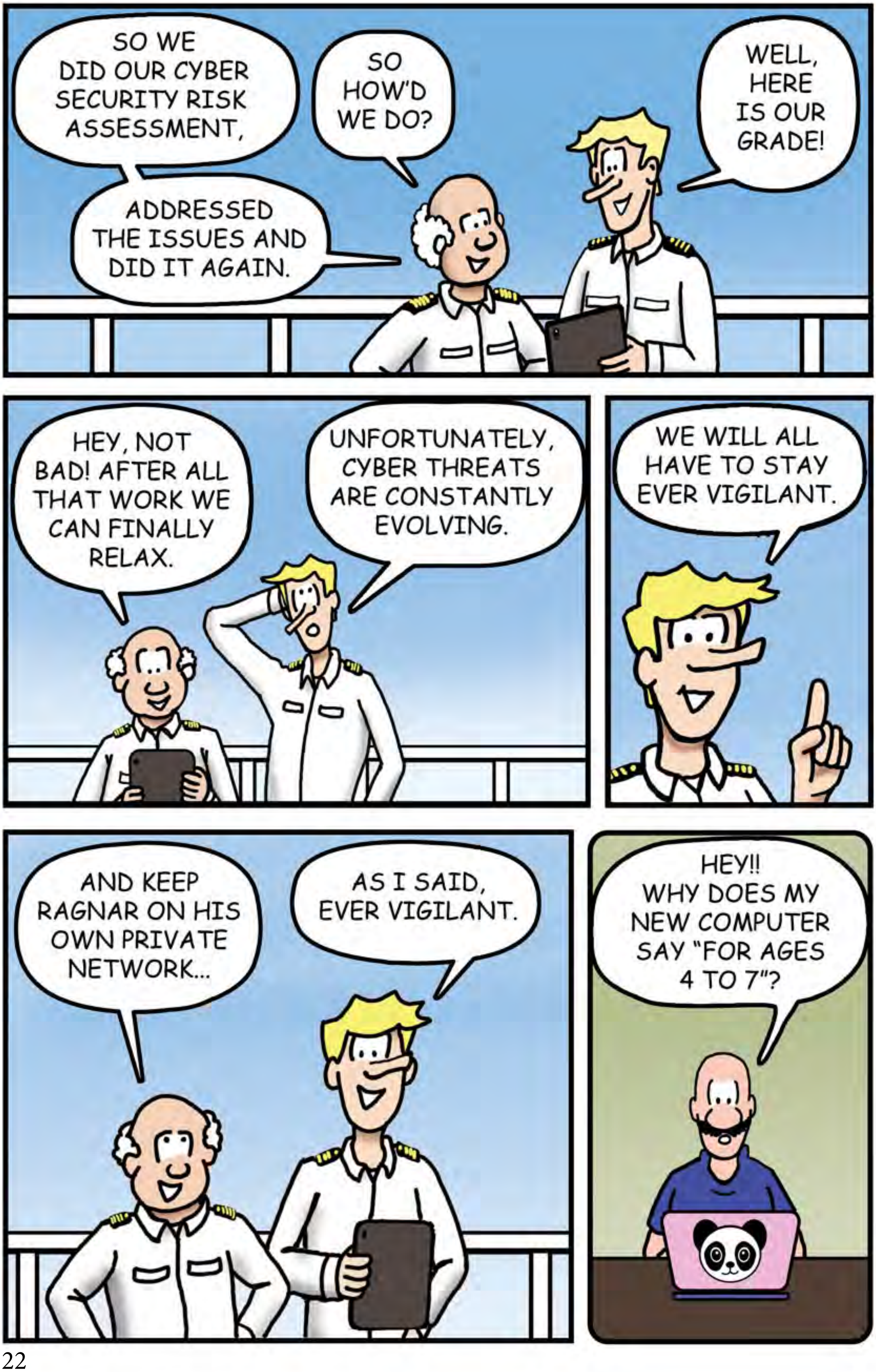

DEFENSE AND CONTINGENCY PLANS ARE YOUR LIFESAVERS IN A CYBER INCIDENT.

CONTINGENCY PLANS

YOU CANNOT PREDICT EVERY SCENARIO, BUT IT IS IMPORTANT TO KNOW WHAT TO DO WHEN THINGS DO GO WRONG.


INCIDENT RESPONSE PLAN
☑ EMERGENCY ROLES
☑ SHUT-OFFS
☑ EMERGENCY CONTACTS
FBI
FBI
ALWAYS REMEMBER CYBER BEST PRACTICES.
■ NEVER CLICK UNTRUSTED LINKS
■ NEVER OPEN UNTRUSTED E-MAIL ATTACHMENTS
■ ONLY DOWNLOAD FROM TRUSTED SITES
■ USE SECURITY SOFTWARE AND KEEP IT UP TO DATE.
■ CONDUCT REGULAR RISK ASSESSMENTS TO REVIEW CYBER CAPABILITIES AND VULNERABILITIES.


UPDATES COMPLETED, SELF-ASSESSMENT GRADE A+, ANTI-VIRUS SOFTWARE IS BLOCKING EFFECTIVELY...
WE'RE ACTUALLY DOING OK!
NOW WE JUST NEED TO STAY VIGILANT AND UP TO DATE, BECAUSE THREATS CONTINUE TO EVOLVE.
I WAS HIRED TO GET THIS DATA, BUT THEY'RE NOT FALLING FOR ANY OF MY TRICKS!
SO I'LL JUST KEEP ON TRYING...


SO WE DID OUR CYBER SECURITY RISK ASSESSMENT,
ADDRESSED THE ISSUES AND DID IT AGAIN.
SO HOW'D WE DO?
WELL, HERE IS OUR GRADE!
HEY, NOT BAD! AFTER ALL THAT WORK WE CAN FINALLY RELAX.
UNFORTUNATELY, CYBER THREATS ARE CONSTANTLY EVOLVING.
WE WILL ALL HAVE TO STAY EVER VIGILANT.
AND KEEP RAGNAR ON HIS OWN PRIVATE NETWORK...
AS I SAID, EVER VIGILANT.
HEY!! WHY DOES MY NEW COMPUTER SAY "FOR AGES 4 TO 7"?

CYBER SECURE

AMERICAN STEAMSHIP OWNERS MUTUAL PROTECTION & INDEMNITY ASSOCIATION, INC.

SHIPOWNERS CLAIMS BUREAU, INC., MANAGER

One Battery Park Plaza, 31st Floor
New York, New York 10004 USA

TEL	+1 212 847 4500
FAX	+1 212 847 4599
WEB	www.american-club.com
EMAIL	info@american-club.com

2100 West Loop South, Suite 1525
Houston, TX 77027 USA

TEL	+1 346 223 9900
EMAIL	claims@american-club.com

SHIPOWNERS CLAIMS BUREAU (UK) LTD.

78-79 Leadenhall Street
London EC3A 3DH United Kingdom

TEL	+44 20 7709 1390
EMAIL	claims@scb-uk.com

SHIPOWNERS CLAIMS BUREAU (HELLAS), INC.

Filellinon 1-3 - 3rd Floor
Piraeus 185 36 Greece

TEL	+30 210 429 4990 1 2 3
FAX	+30 210 429 4187 8
EMAIL	claims@scb-hellas.com

SCB MANAGEMENT CONSULTING SERVICES, LTD.

The Workstation, 28th Floor
43 Lyndhurst Terrace
Central, Hong Kong SAR, People's Republic of China

TEL	+852 3905 2150
EMAIL	hkinfo@scbmcs.com

SCB MANAGEMENT CONSULTING (CHINA) CO., LTD.

Room 905, Cross Tower
No. 318 Fuzhou Road
Shanghai 200001, People's Republic of China

TEL	+86 21 3366 5000
FAX	+86 21 3366 6100
EMAIL	claims@scbmcs.com

THE
AMERICAN
CLUB
1917