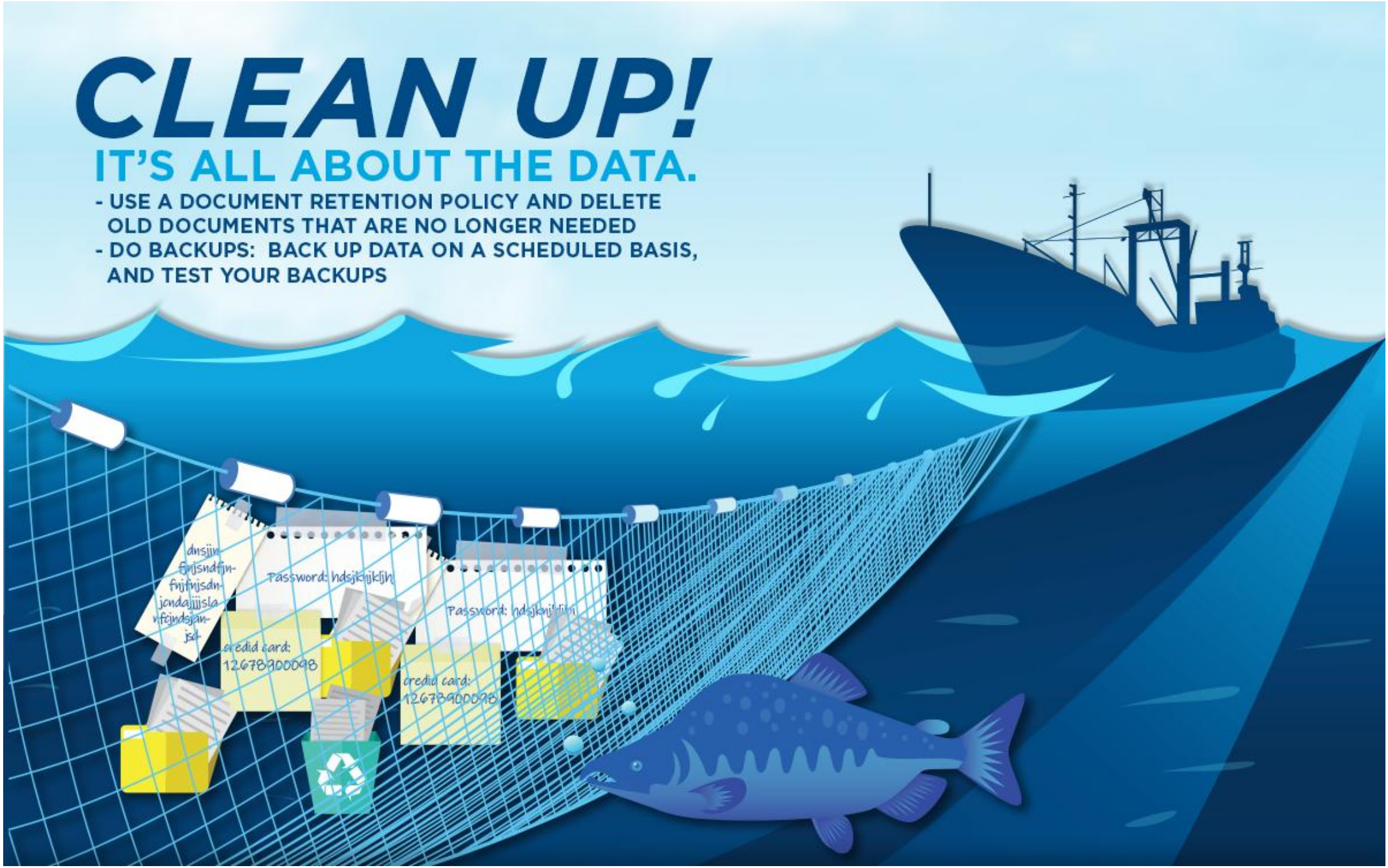
QUICK
TIPS
BE CAREFUL
WHAT YOU POST ONLINE
DON'T BE
AN EASY TARGET

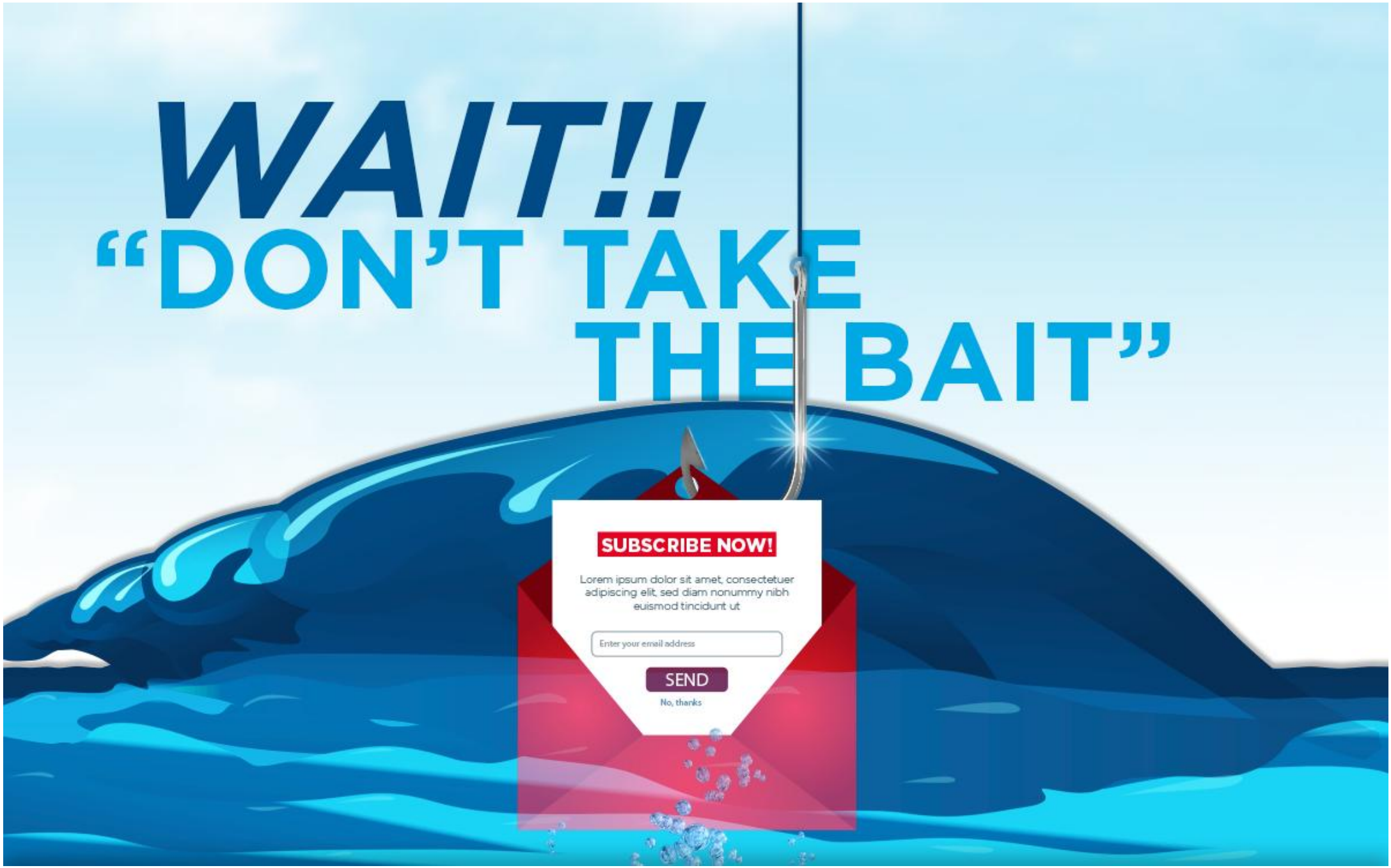
QUICK TIPS
DON'T USE CRACKED SOFTWARE
NEVER DOWNLOAD PIRATED APPS/SOFTWARE AS THEY WILL OFTEN CONTAIN MALWARE.

CLEAN UP!

IT'S ALL ABOUT THE DATA.

- USE A DOCUMENT RETENTION POLICY AND DELETE OLD DOCUMENTS THAT ARE NO LONGER NEEDED
- DO BACKUPS: BACK UP DATA ON A SCHEDULED BASIS, AND TEST YOUR BACKUPS




WAIT!!
"DON'T TAKE THE BAIT"
SUBSCRIBE NOW!
Lorem ipsum dolor sit amet, consectetuer adipiscing elit, sed diam nonummy nibh euismod tincidunt ut
Enter your email address
SEND
No, thanks

FIREWALLS
DON'T PROVIDE
COMPLETE COVERAGE.
•BEWARE OF EMAIL ATTACHMENTS AND LINKS
•CHECK PRIVACY SETTINGS
•DON'T POST PERSONAL INFORMATION

"IT'S NOT GOLD IT'S MALWARE"

BE CAREFUL WHAT YOU PLUG INTO YOUR COMPUTER.
NEVER USE A USB FROM AN UNKNOWN SOURCE.
DON'T LET CURIOSITY GET THE BEST OF YOU.

WHEN IT COMES TO SECURITY THERE IS NOTHING FOR FREE. *DON'T* TRADE YOUR PERSONAL INFORMATION FOR A FREEBIE

GET SHREDDING

REMOVE NON-TECHNICAL VULNERABILITIES AS PART OF A PROACTIVE CYBERSECURITY SOLUTION. (INCLUDING PASSWORDS ON PAPER, INVOICES, & PRINTED CREDIT CARD INFORMATION)

DON'T FEED THE PHISH
DON'T SHARE YOUR Prepaid CARD DETAILS OVER EMAILS, CHAT MESSAGES OR THROUGH UN-TRUSTED WEBSITES, AND REVIEW REGULARLY YOUR PPC STATEMENTS FOR FRAUD
Prepaid Card

JUST A CLICK
CAN SINK A SHIP

TRUST NO ONE ON SOCIAL MEDIA. DON'T ACCEPT INVITES FROM PEOPLE YOU DON'T KNOW. THEY MAY BE TRYING TO HARVEST YOUR PERSONAL INFORMATION.

PROTECT
YOUR SYSTEMS
MAKE SURE ANTIVIRUS, FIREWALL, AND AD-BLOCKER SOLUTIONS ARE PATCHED AND UPDATED ON A REGULAR BASIS.

USE COMMON SENSE AND BE
CYBERSMART!
• CREATE PASSWORDS THAT ARE STRONG, UNIQUE AND EASY TO REMEMBER
• KEEP YOUR SOFTWARE UP TO DATE
• INSTALL ANTIVIRUS & DESKTOP FIREWALL SOLUTIONS AGAINST MALWARE AND UNAUTHORIZED ACCESS
• SECURE YOUR WEB BROWSER BEFORE ACCESSING INTERNET
****
****
Card

BE AWARE
WHERE YOU
SURF
INTERNET

IF IT'S NOT YOURS
DON'T TAKE IT
DON'T TRUST FREE GAMES.
THEY ARE OFTEN TROJANS

DON'T FALL FOR THE TRAP

ROGUE WIFI HOTSPOTS CAN STEAL CREDENTIALS

USE A VPN

QUICK TIPS

ONLINE SHOPPING

IF A DEAL IS TOO GOOD TO BE TRUE IT PROBABLY IS

- SOME SCAMMERS USE STOLEN CREDIT CARDS TO PURCHASE PRODUCTS AND THEN RESELL THEM ON THE INTERNET.
- VERIFY E-COMMERCE SITES. LOOK AT REVIEWS, AND OTHER VERIFICATIONS.
- DON'T SET UP ACCOUNTS WITH SITES YOU RARELY USE.
- USE ESCROW SERVICES LIKE PAYPAL.
- READ SHIPPING INVOICES CAREFULLY.

QUICK TIPS

KEEP YOUR SOFTWARE UP-TO-DATE

MOST UPDATES INCLUDE SECURITY FIXES.

- IF YOUR MANUFACTURER RELEASES AN UPDATE, INSTALL IT AS SOON AS POSSIBLE. ALMOST ALL SOFTWARE UPDATES INCLUDE SECURITY PATCHES TO CLOSE VULNERABILITIES.

- VERIFY UPDATES ARE COMING FROM A LEGITIMATE SOURCE.

QUICK TIPS

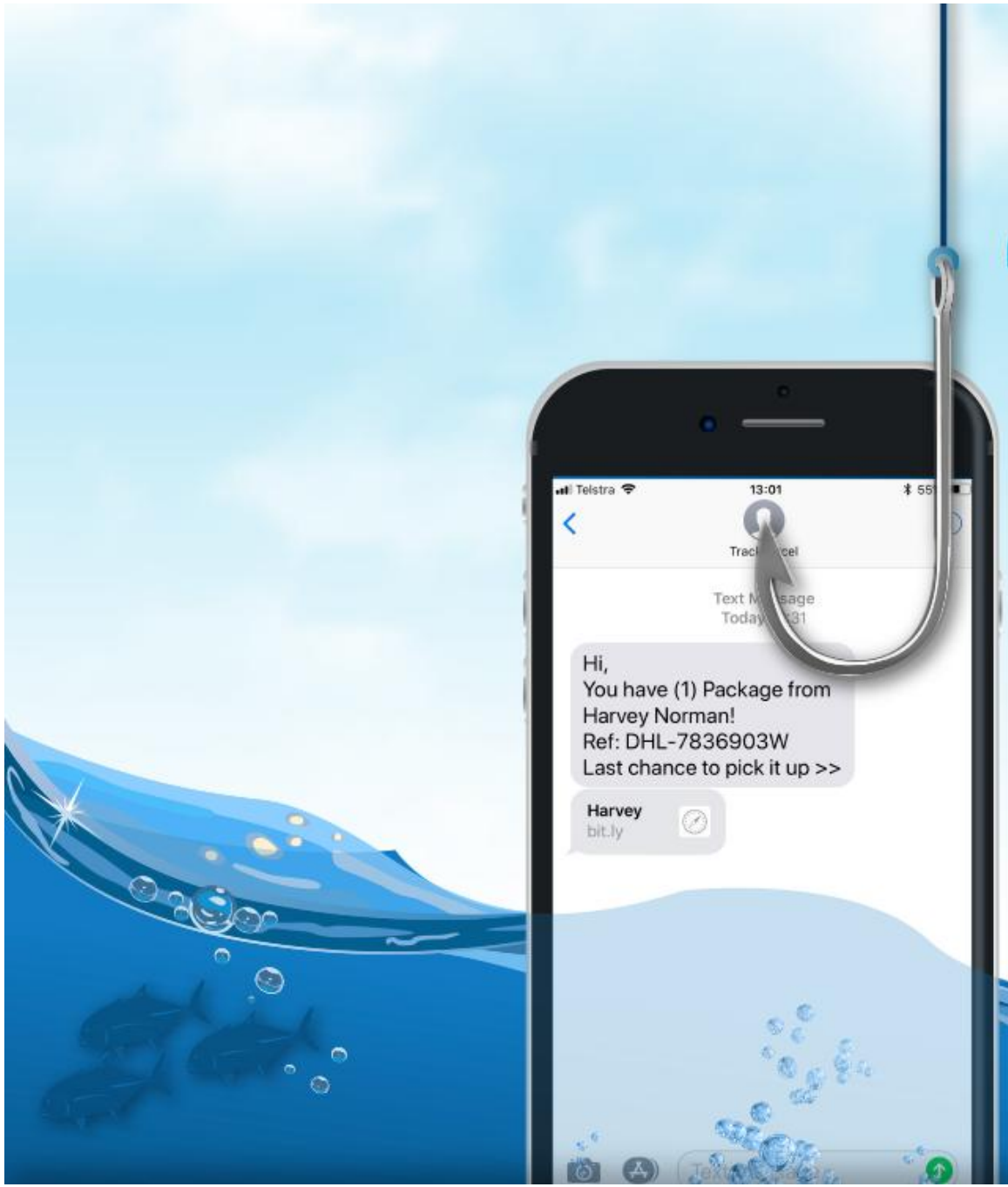
1. IT HAS TO CONTAIN A RANDOM COLLECTION OF LETTERS (UPPERCASE AND LOWERCASE), NUMBERS AND SYMBOLS

2. IT HAS TO BE AT LEAST 8 CHARACTERS OR LONGER

3. YOU MUST USE A UNIQUE PASSWORD FOR EVERY DIFFERENT ACCOUNT

4. CHANGE YOUR PASSWORDS REGULARLY

PICK STRONG PASSWORDS *THAT* HACKERS CAN'T GUESS



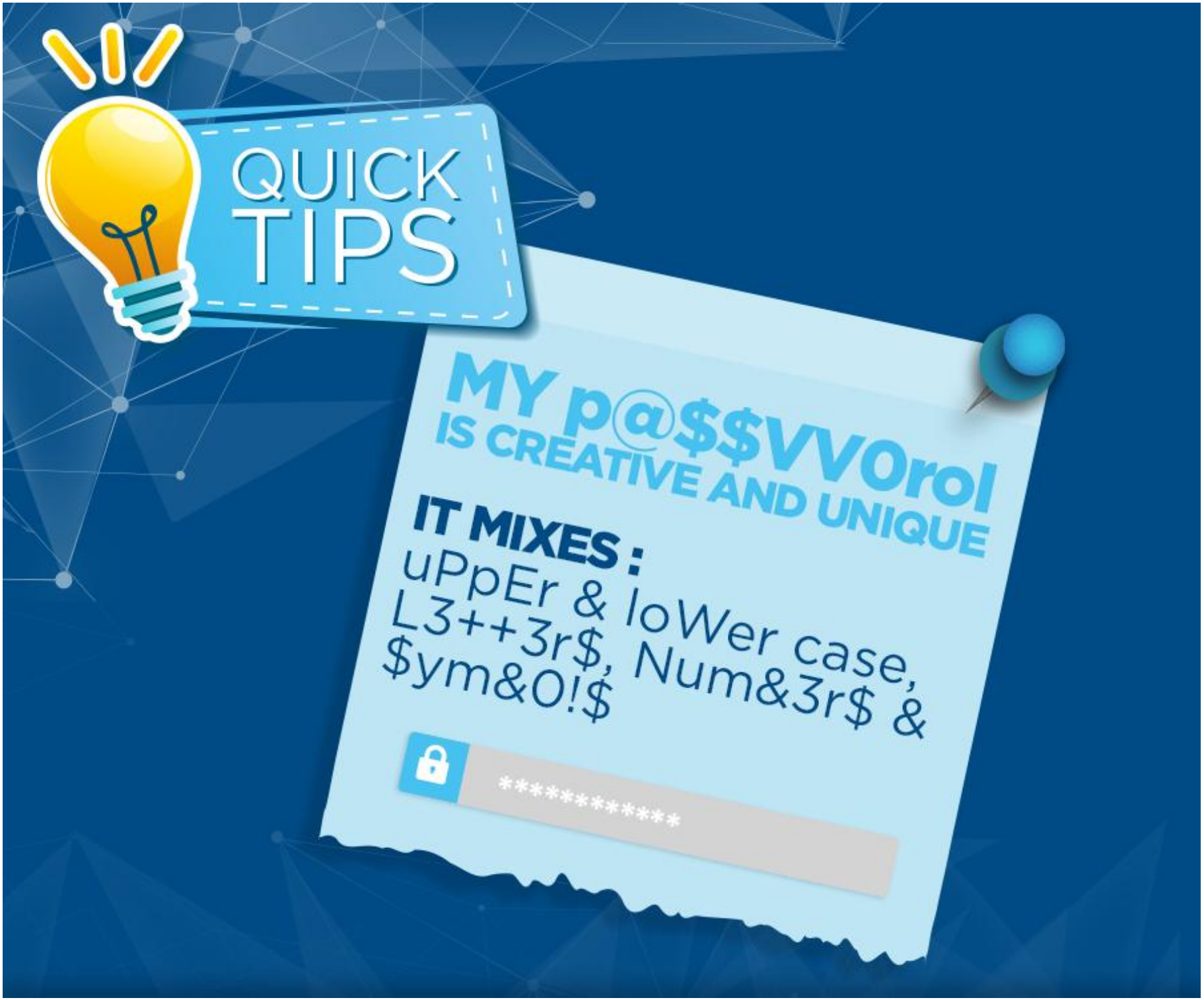
"SMISHING"
SMS-PHISHING

DELETE TEXT MESSAGES THAT ASK YOU TO CONFIRM OR PROVIDE PERSONAL INFORMATION: LEGITIMATE COMPANIES DON'T ASK FOR INFORMATION LIKE YOUR ACCOUNT NUMBERS OR PASSWORDS BY EMAIL OR TEXT.

DON'T REPLY, AND DON'T CLICK ON LINKS PROVIDED IN THE MESSAGE: LINKS CAN INSTALL MALWARE ON YOUR COMPUTER AND TAKE YOU TO SPOOF SITES THAT LOOK REAL BUT WHOSE PURPOSE IS TO STEAL YOUR INFORMATION.

TREAT YOUR PERSONAL INFORMATION LIKE CASH: YOUR SOCIAL SECURITY NUMBER, CREDIT CARD NUMBERS, AND BANK AND UTILITY ACCOUNT NUMBERS CAN BE USED TO STEAL YOUR MONEY OR OPEN NEW ACCOUNTS IN YOUR NAME. DON'T GIVE THEM OUT IN RESPONSE TO A TEXT.

QUICK TIPS
https://w w.fcebook.com
"AVOID PHISHING ATTACKS"
VALIDATE THE URL
FOR THE WEBSITES YOU ACCESS BEFORE
PROVIDING YOUR PERSONAL DATA


QUICK TIPS
MY p@$$VV0rol IS CREATIVE AND UNIQUE
IT MIXES :
uPpEr & loWer case, L3++3r$, Num&3r$ & $ym&O!$
****

THEY LOOK FRIENDLY

BUT THEY'RE NOT

"DON'T TRUST ANONYMOUS FACEBOOK REQUESTS; THEY OFTEN TURN OUT TO BE SCAMS"

REPORT SUSPICIOUS MESSAGES TO FACEBOOK BY TAPPING THE 'SOMETHING'S WRONG' BUTTON.

IF YOU RECEIVE A SUSPICIOUS EMAIL FROM FACEBOOK, FORWARD IT TO phish@fb.com.

BLOCK, REPORT, IGNORE, OR DELETE ANY SUSPICIOUS FACEBOOK REQUESTS OR MESSAGES

IF YOU SUSPECT THAT AN ACCOUNT IS FAKE OR IMPERSONATING SOMEONE, REPORT IT.

DON'T OPEN UNKNOWN FILES THAT END IN .exe

A FILE WHOSE NAME ENDS IN ".EXE" IS REALLY A PROGRAM THAT WHEN OPENED CAUSES THE OPERATING SYSTEM TO RUN THE PROGRAM. USERS WHO RECEIVE AN .EXE FILE AS AN E-MAIL ATTACHMENT SHOULD ALWAYS BE SURE THAT THE FILE COMES FROM A TRUSTED SOURCE AND DOES NOT CONTAIN A VIRUS

QUICK TIPS

SCARY TRENDS TO WATCH OUT FOR

NEVER SCAN A **QR-CODE** FROM AN UNKNOWN SOURCE

QR-CODES CAN BE USED TO **STEAL YOUR PERSONAL DATA** OR DIRECT YOU TO A MALICIOUS SITE THAT COULD EXPLOIT YOUR MOBILE

QUICK TIPS
SCARY TRENDS TO WATCH OUT FOR
NEVER SCAN A QR-CODE FROM AN UNKNOWN SOURCE
QR-CODES CAN BE USED TO STEAL YOUR PERSONAL DATA OR DIRECT YOU TO A MALICIOUS SITE THAT COULD EXPLOIT YOUR MOBILE

QUICK TIPS
WATCH OUT FOR MALVERTISING
CLICKING A MALICIOUS AD CAN EXPOSE YOUR COMPUTER TO MALWARE
YOU HAVE WON!
FREE
POPUP
ADVERTISMENT
SKIP AD

QUICK TIPS
PROTECT YOUR DATA
DON'T EXPECT ANYONE TO PROTECT IT FOR YOU
BE CAREFUL WHERE YOU SHOP ONLINE
KEEP YOUR ANTI-VIRUS SOFTWARE UP-TO-DATE
ALWAYS BACK UP YOUR IMPORTANT FILES
USE STRONG PASSWORDS ON ALL DEVICES

SECURITY DANGERS OF PUBLIC WI-FI

- **USE A VPN:** A VIRTUAL PRIVATE NETWORK (VPN) CONNECTION IS RECOMMENDED WHEN CONNECTING TO THE INTERNET THROUGH AN UNSECURED CONNECTION, LIKE A WI-FI HOTSPOT.
- **TURN OFF SHARING:** TURN OFF SHARING IN SYSTEM PREFERENCES OR IN THE CONTROL PANEL OF YOUR MOBILE DEVICE. OR DO IT AUTOMATICALLY BY CHOOSING "PUBLIC" THE FIRST TIME YOU CONNECT TO A NEW, UNSECURED NETWORK.
- **KEEP WI-FI OFF WHEN YOU DON'T NEED IT:** WHEN ON, THE WI-FI HARDWARE IN YOUR COMPUTER IS STILL TRANSMITTING DATA BETWEEN ANY NETWORK WITHIN RANGE. THERE ARE SECURITY MEASURES IN PLACE TO PREVENT THIS MINOR COMMUNICATION FROM COMPROMISING YOU, BUT NOT ALL WIRELESS ROUTERS ARE THE SAME, AND HACKERS CAN BE A PRETTY SMART BUNCH.

QUICK TIPS

KEEP YOUR INBOX SAFE ENABLE EMAIL SCANNING

- DON'T TRUST ATTACHMENTS
- DISABLE AUTOMATIC PREVIEWING
- NEVER RESPOND TO EMAIL REQUESTS FOR PERSONAL OR COMPANY ACCOUNT INFORMATION
- ACTIVATE THE EMAIL SCANNING FUNCTION IN YOUR ANTIVIRUS SOFTWARE

QUICK TIPS

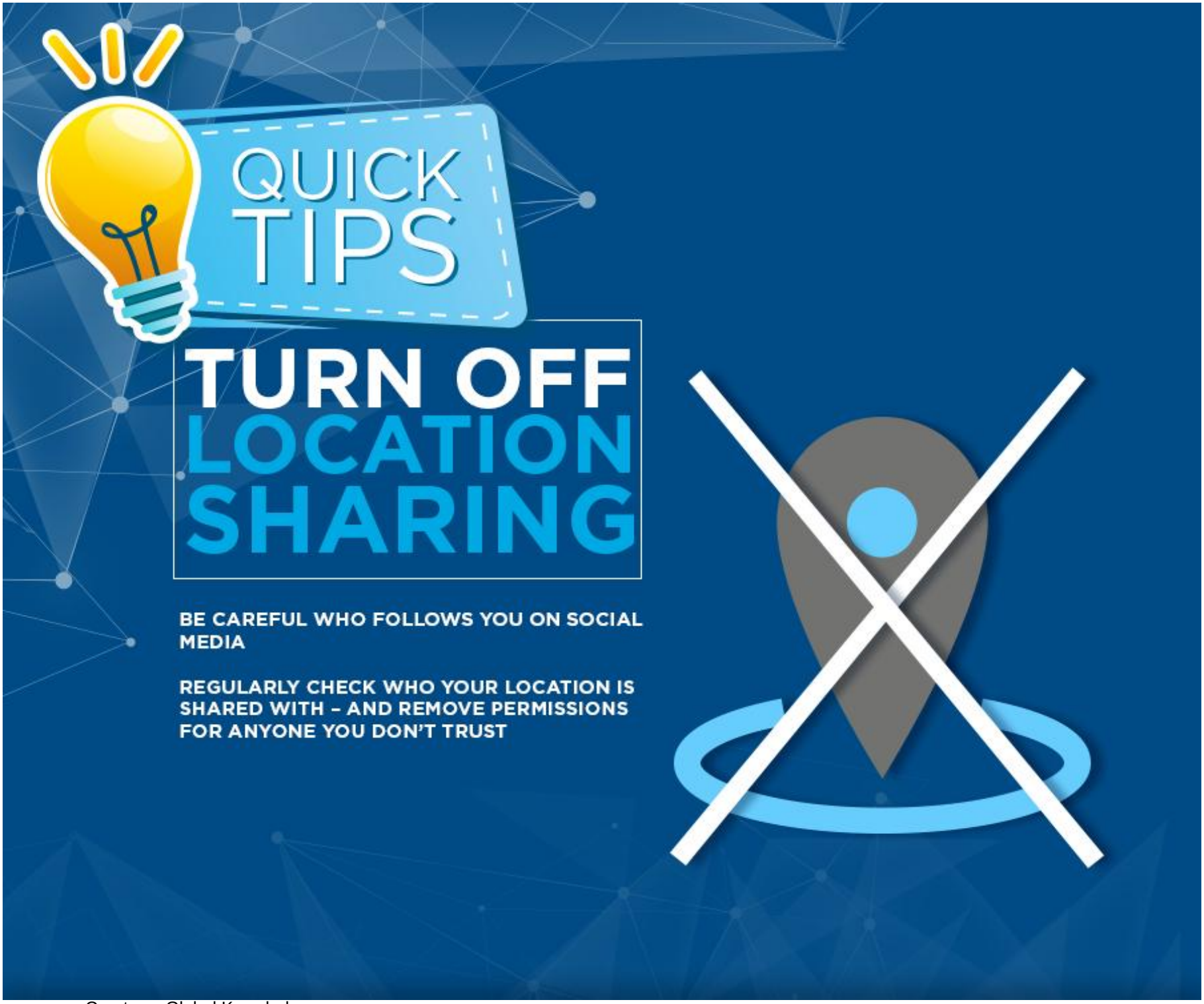
KEEP YOUR INBOX SAFE ENABLE EMAIL SCANNING

- DON'T TRUST ATTACHMENTS
- DISABLE AUTOMATIC PREVIEWING
- NEVER RESPOND TO EMAIL REQUESTS FOR PERSONAL OR COMPANY ACCOUNT INFORMATION
- ACTIVATE THE EMAIL SCANNING FUNCTION IN YOUR ANTIVIRUS SOFTWARE

QUICK TIPS

ALWAYS KEEP YOUR DEVICES LOCKED

SET YOUR DEVICES TO AUTOMATICALLY LOCK WHEN THEY'RE NOT IN USE



Courtesy: Global Knowledge