PHIGHT THE PHISH

A PROGRAM TO BUILD CYBER HYGIENE AND SECURITY AWARENESS

PRESENTED BY

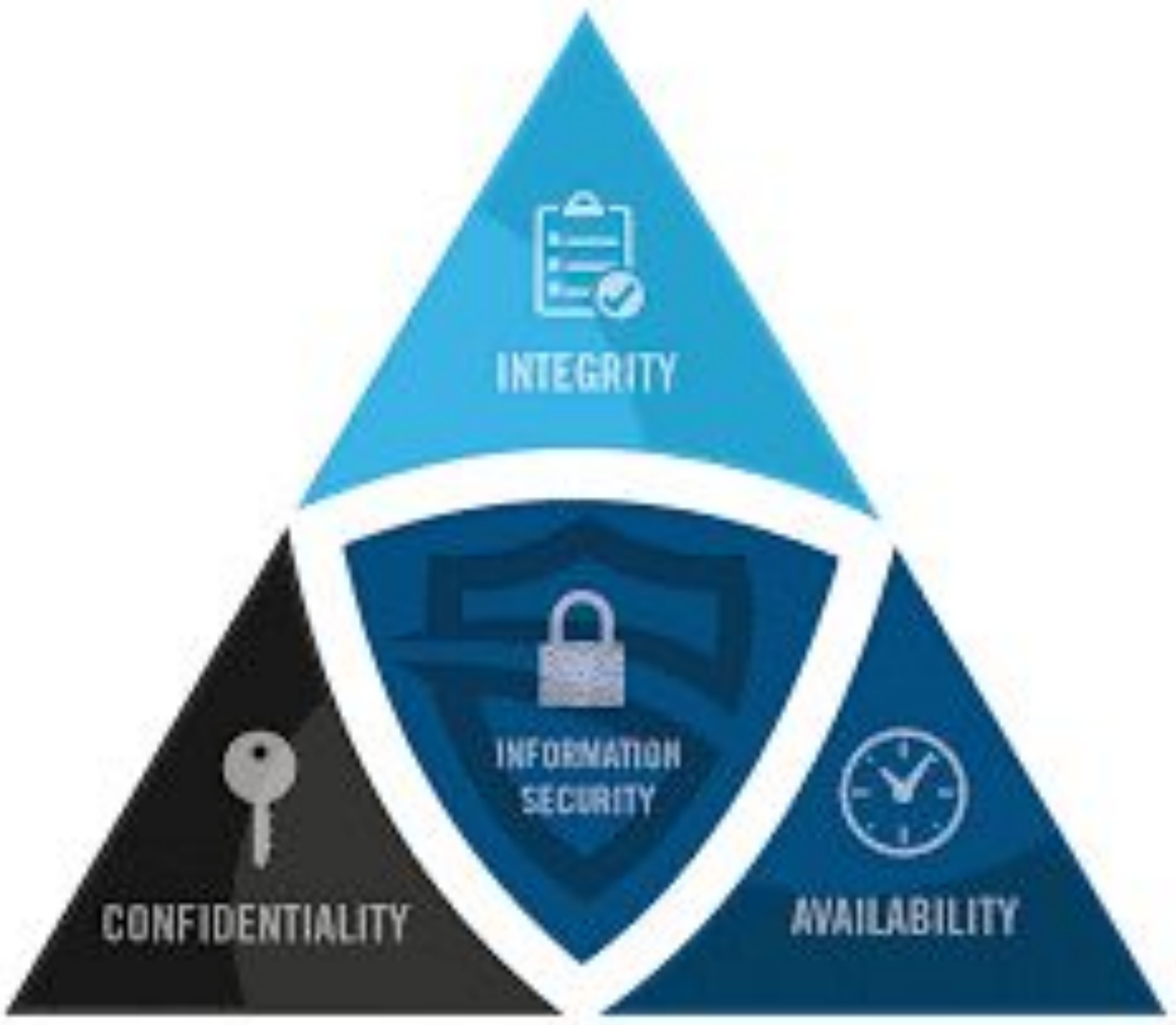
MCAFEE&TAFT

WHO & WHY

McAfee&Taft

- OKLAHOMA'S LARGEST LAW FIRM
- 70-YEAR HISTORY OF SERVING OKLAHOMANS IN LAW
- OKLAHOMA CITY, SPRINGFIELD (MO), TULSA
- CYBERSECURITY & PRIVACY
- LARGEST & MOST DIVERSE INDUSTRY GROUP

SECURITY BASICS



SOCIAL ENGINEERING

SOCIAL ENGINEERING ATTACKS OCCUR WHEN AN ATTACKER USES HUMAN INTERACTION (SOCIAL SKILLS) TO OBTAIN OR COMPROMISE INFORMATION ABOUT AN ORGANIZATION OR ITS COMPUTER SYSTEMS.

BUSINESS EMAIL COMPRIMISE

BUSINESS EMAIL COMPROMISE (OR EMAIL ACCOUNT COMPROMISE) IS A SOPHISTICATED SCAM THAT TARGETS BOTH BUSINESSES AND INDIVIDUALS WHO PERFORM LEGITIMATE TRANSFER-OF-FUNDS REQUESTS.

BEC IS ONE OF THE MOST FINANCIALLY DAMAGING ONLINE CRIMES.

PHISHING

PHISHING IS A FORM OF SOCIAL ENGINEERING
THAT USES EMAIL OR MALICIOUS WEBSITES TO SOLICIT PERSONAL INFORMATION
OR TO GET YOU TO DOWNLOAD MALICIOUS SOFTWARE BY POSING AS A TRUSTWORTHY ENTITY.

TYPES OF PHISHING

SPEAR-PHISHING

WHALING

VISHING

SMISHING

SPEAR-PHISHING

SPEAR-PHISHING IS PHISHING TARGETED AT AN INDIVIDUAL BY INCLUDING KEY INFORMATION ABOUT THEM.

WHALING

WHALING IS PHISHING TARGETED AT A HIGH-PROFILE INDIVIDUAL TO STEAL SENSITIVE AND HIGH-VALUE INFORMATION.

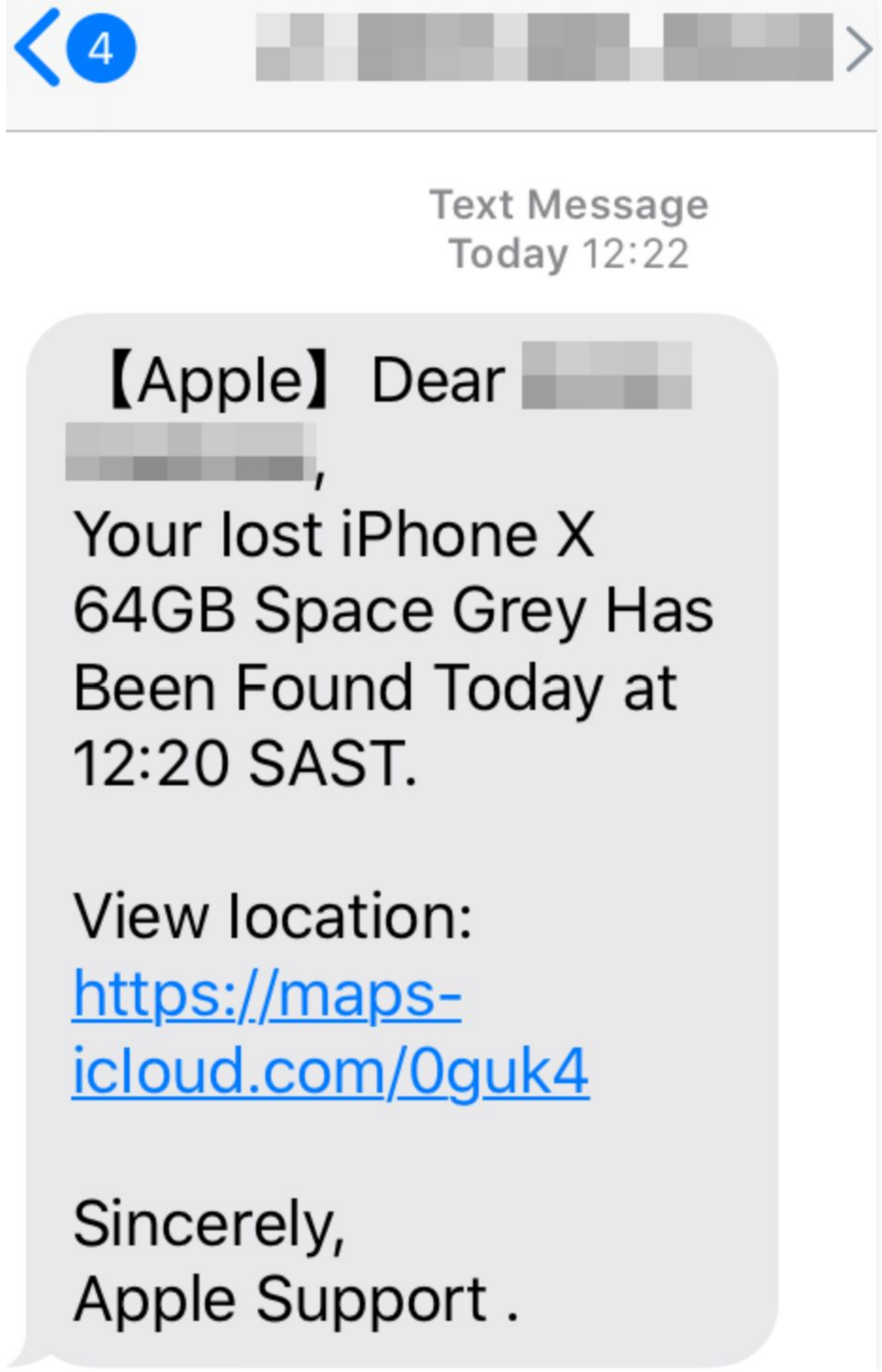
VISHING

**VISHING IS PHISHING VIA VOICE COMMUNICATION
TO ENTICE THE VICTIM TO ENGAGE IN CONVERSATION & BUILD TRUST.**

SMISHING

SMISHING IS PHISHING VIA TEXT MESSAGES
TO GET THE VICTIM TO CLICK ON A LINK, DOWNLOAD FILES AND APPLICATIONS, OR BEGIN A CONVERSATION.

SMISHING

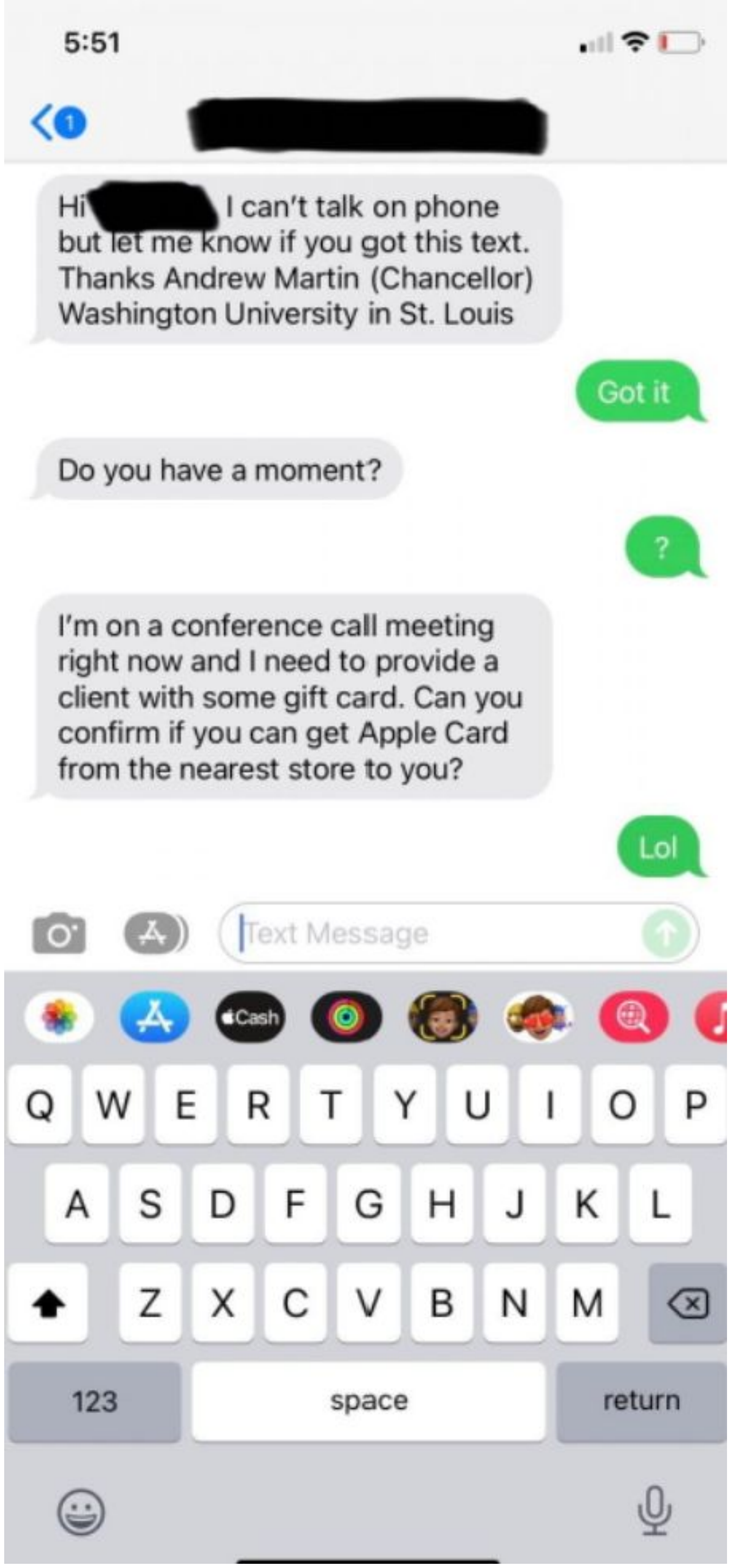


Text Message
Today 12:22

【Apple】 Dear [redacted],
Your lost iPhone X 64GB Space Grey Has Been Found Today at 12:20 SAST.

View location: https://maps-icloud.com/0guk4

Sincerely,
Apple Support .



Hi [redacted] I can't talk on phone but let me know if you got this text. Thanks Andrew Martin (Chancellor) Washington University in St. Louis

Got it

Do you have a moment?

?

I'm on a conference call meeting right now and I need to provide a client with some gift card. Can you confirm if you can get Apple Card from the nearest store to you?

Lol

THE RISKS

OPERATIONS

REGULATORY INVESTIGATION & FINES

LITIGATION

DAMAGE TO REPUTATION

FINANCIAL DAMAGES

LOSS OF PUBLIC TRUST

THE OPERATIONS RISK

9.6

DAYS

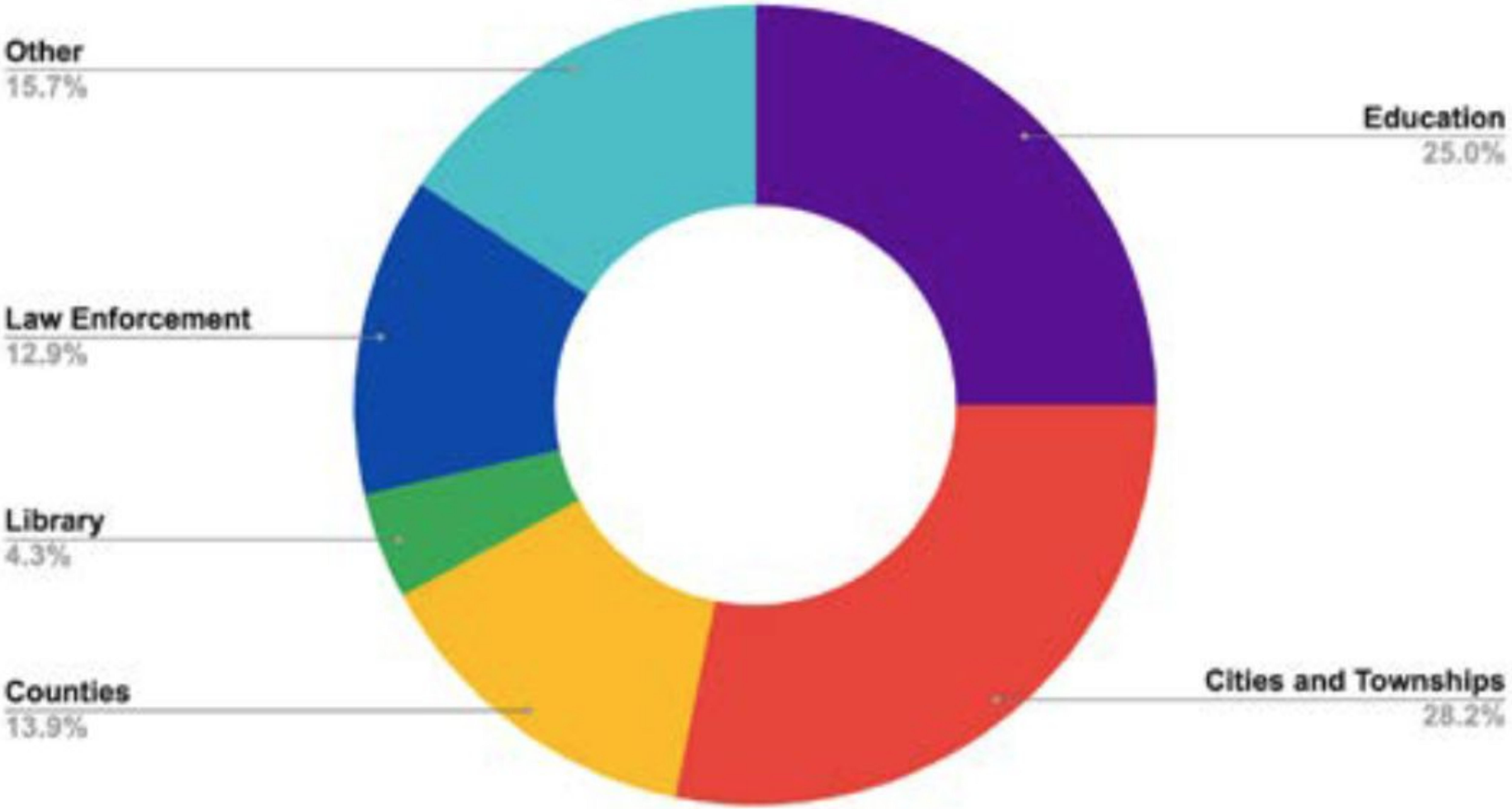
THE AVERAGE DOWNTIME FROM AN ATTACK

THE FINANCIAL RISK

$125,697

ESTIMATED RANSOM PAID PER EVENT BY MUNICIPALITIES

WHY ARE YOU AT RISK?



THE ECONOMIC IMPACT OF CYBER ATTACKS ON MUNICIPALITIES
KNOWBE4, 2020

WHY ARE YOU AT RISK?

50

PERCENT

OF STATES DO NOT HAVE A COMMITTED CYBERSECURITY LINE-ITEM IN THE BUDGET

WHY ARE YOU AT RISK?

37

PERCENT

OF STATES HAVE SEEN A REDUCTION OR NO CHANGE IN THE BUDGET FOR CYBERSECURITY OR TECHNOLOGY

ANATOMY OF A PHISH

SUSPICIOUS SENDER

GENERIC GREETINGS AND/OR SIGNATURE

CALL TO ACTION

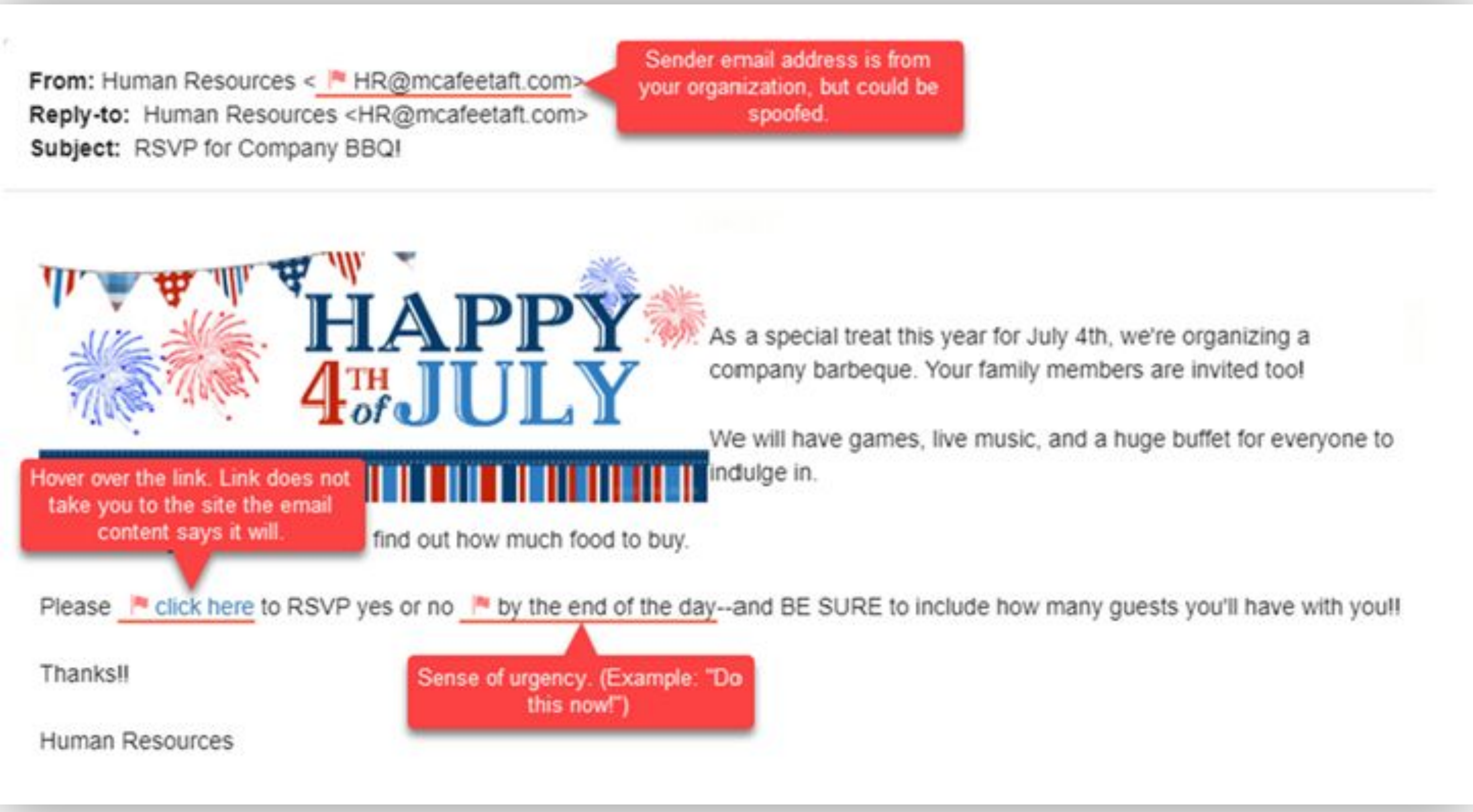
SENSE OF URGENCY

SPOOFED HYPERLINKS

GRAMMAR & SPELLING

SUSPICIOUS ATTACHMENTS

ANATOMY OF A PHISH



From: Human Resources < HR@mcafeetaft.com>
Reply-to: Human Resources <HR@mcafeetaft.com>
Subject: RSVP for Company BBQ!

Sender email address is from your organization, but could be spoofed.

As a special treat this year for July 4th, we're organizing a company barbeque. Your family members are invited too!

We will have games, live music, and a huge buffet for everyone to indulge in.

Hover over the link. Link does not take you to the site the email content says it will.

find out how much food to buy.

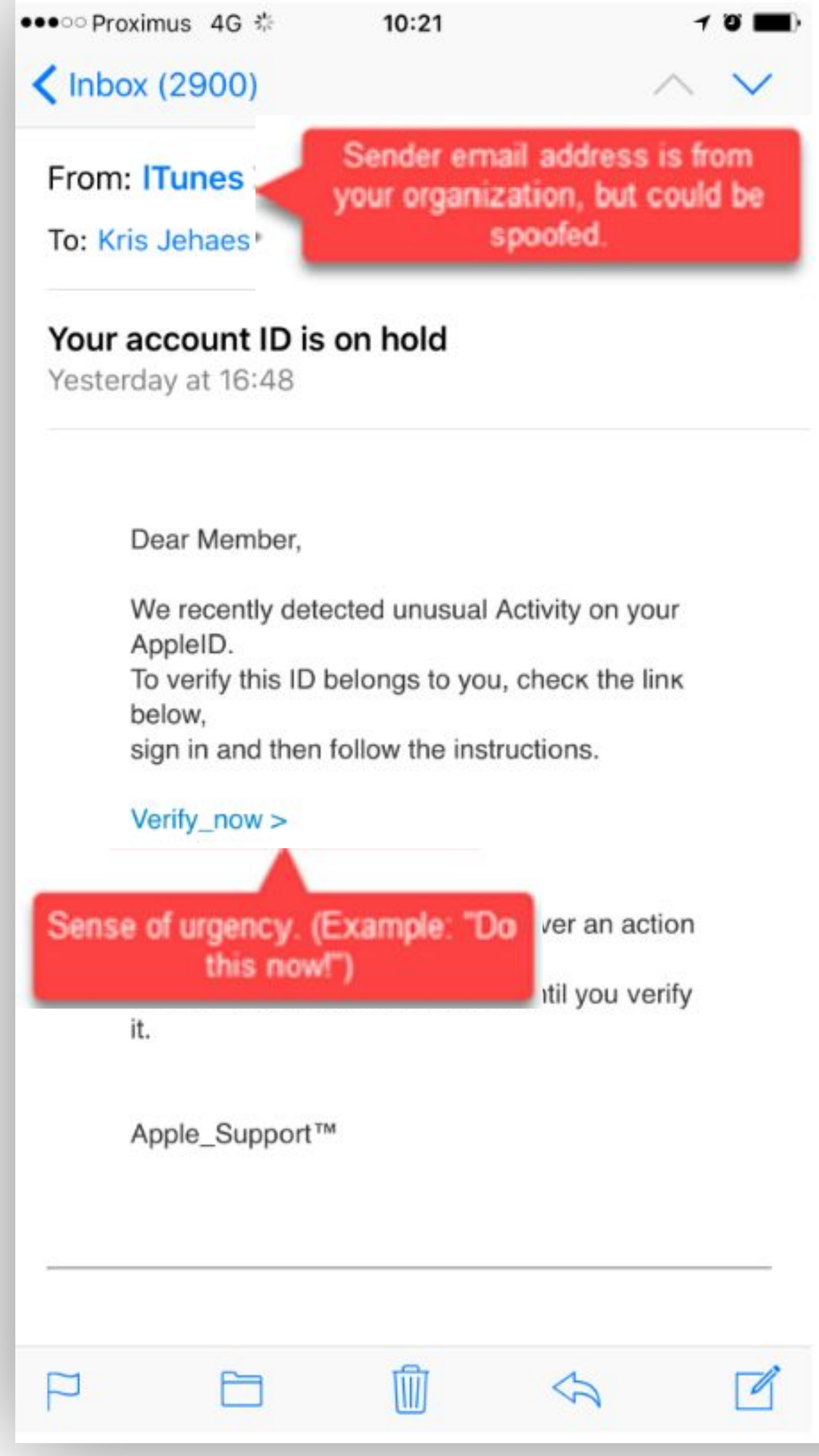
Please click here to RSVP yes or no by the end of the day--and BE SURE to include how many guests you'll have with you!!

Sense of urgency. (Example: "Do this now!")

Thanks!!

Human Resources

ANATOMY OF A PHISH



From: ITunes

To: Kris Jehaes

Sender email address is from your organization, but could be spoofed.

Your account ID is on hold
Yesterday at 16:48

Dear Member,

We recently detected unusual Activity on your AppleID.
To verify this ID belongs to you, check the link below,
sign in and then follow the instructions.

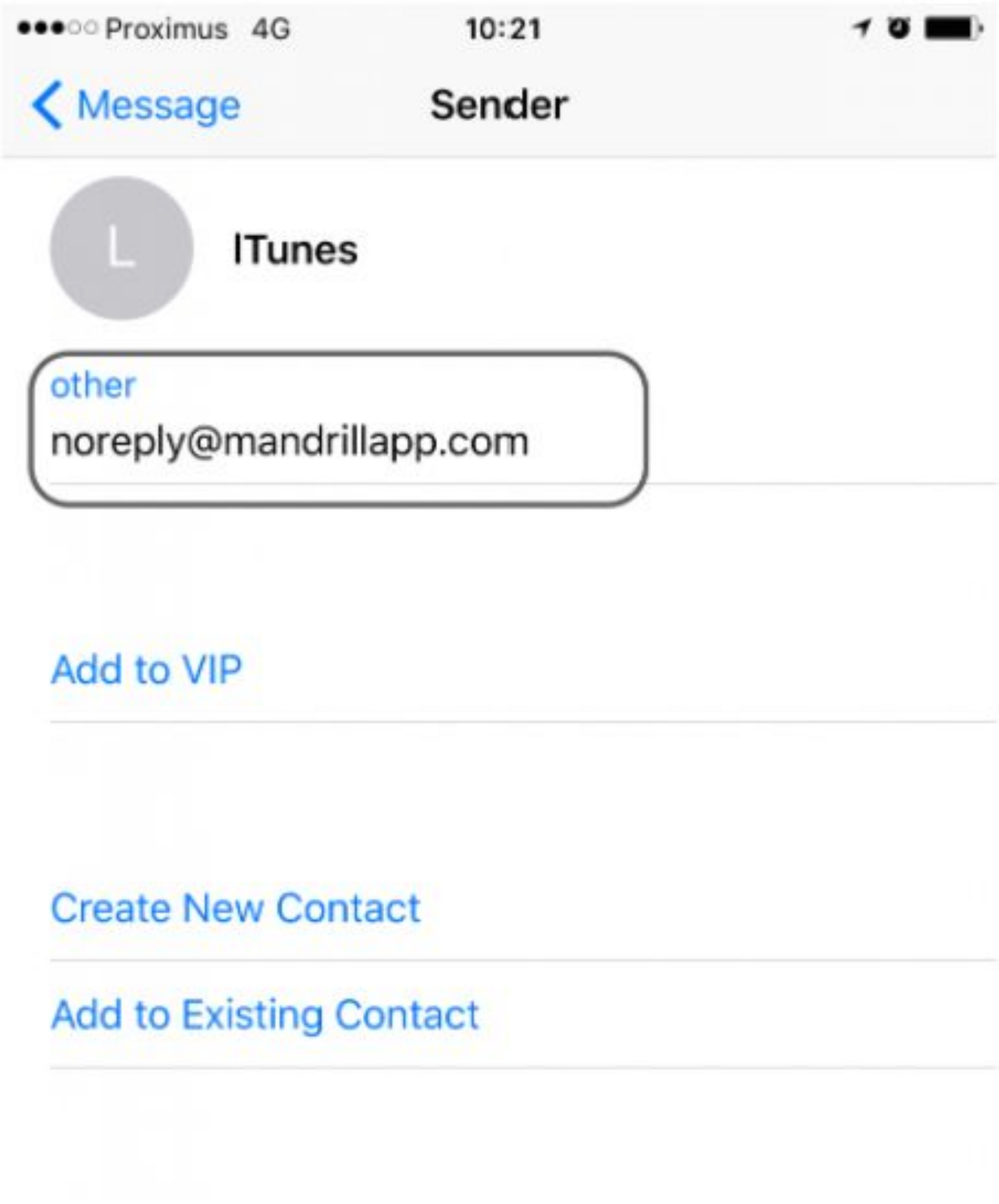
Verify_now >

Sense of urgency. (Example: "Do this now!")

ver an action

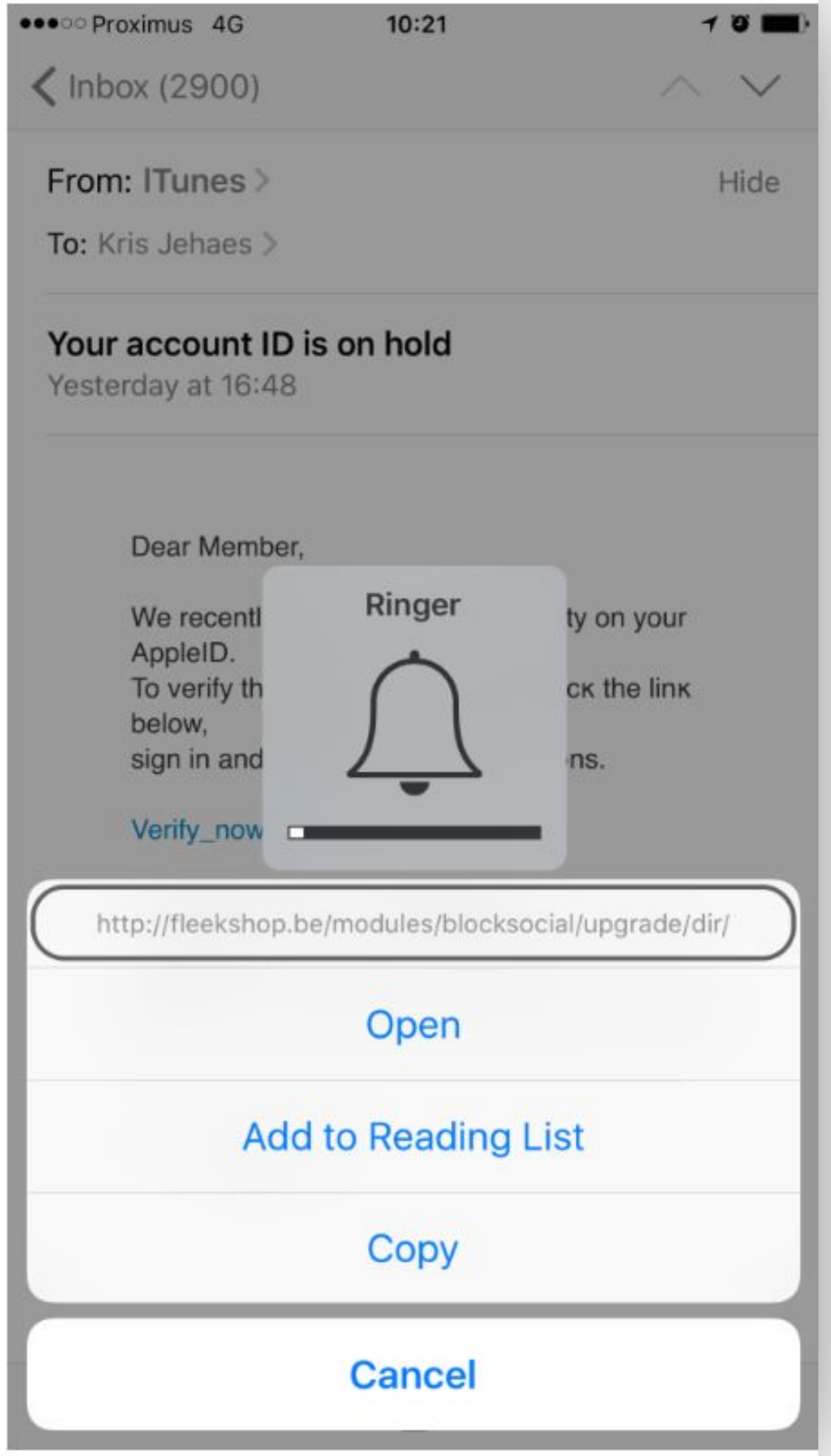
ntil you verify it.

Apple_Support™



ITunes

other
noreply@mandrillapp.com



From: ITunes

To: Kris Jehaes

Your account ID is on hold
Yesterday at 16:48

Dear Member,

We recentl ty on your AppleID.
To verify th ck the link below,
sign in and ns.

Verify_now

http://fleekshop.be/modules/blocksocial/upgrade/dir/

THE BOOM

[LEFT] BOOM [RIGHT]

WHAT KIND OF BOOM?

EVENT < INCIDENT < BREACH

LEFT OF BOOM: PREPARATION

WHEN IN DOUBT, REPORT IT OUT

MAKE PASSWORDS LONG & STRONG

MFA, IN EVERY WAY

HYPER-WARY OF HYPERLINKS

ALWAYS UP THE ANTI

TRAIN TO GAIN

LEFT OF BOOM: PREPARATION

TEACH A PERSON TO SEE A PHISH, AND THEY WILL STOP PHISH FOR A LIFETIME

THE BOOM: INCIDENT HANDLING

DETECTION & ANALYSIS

CONTAINMENT, ERADICATION & RECOVERY

POST-INCIDENT RECOVERY

RIGHT OF BOOM: POST-INCIDENT RECOVERY

LEGAL OBLIGATIONS & REPORTING

PUBLIC DISCLOSURES & MESSAGING

MITIGATION & TRAINING

MUNICIPALITIES MUST FOCUS ON

PEOPLE

PROCESS

TECHNOLOGY

PEOPLE

DOES OUR CITY HAVE AN INTERNAL OR EXTERNAL TECHNOLOGY TEAM?

DOES OUR CITY HAVE A DESIGNATED EMPLOYEE (FULL OR PART-TIME) FOR CYBERSECURITY?

DOES OUR CITY HAVE A DESIGNATED TEAM FOR CYBERSECURITY EVENTS?

PROCESS

DOES OUR CITY HAVE A **PROCESS FOR ASSESSING** CYBER RISKS?
DOES OUR CITY HAVE AN **INCIDENT RESPONSE PLAN**?
DOES OUR CITY HAVE A **CYBERSECURITY TRAINING** PROGRAM?

TECHNOLOGY

WHAT PLATFORM DOES OUR CITY USE FOR **EMAIL** AND **OFFICE MANAGEMENT**?

WHAT **SECURITY TOOLS** ARE ENABLED ON THIS PLATFORM?

DOES OUR CITY UTILIZE **MULTI-FACTOR AUTHENTICATION** FOR ALL OUR TECHNOLOGY SYSTEMS?

CONCLUSION

QUESTIONS?

SASHA BELING
405-270-6011
SASHA.BELING@MCAFEETAFT.COM

ZACH OUBRE
405-270-6023
ZACH.OUBRE@MCAFEETAFT.COM

JOSHUA SNAVELY
405-270-6027
JOSHUA.SNAVELY@MCAFEETAFT.COM