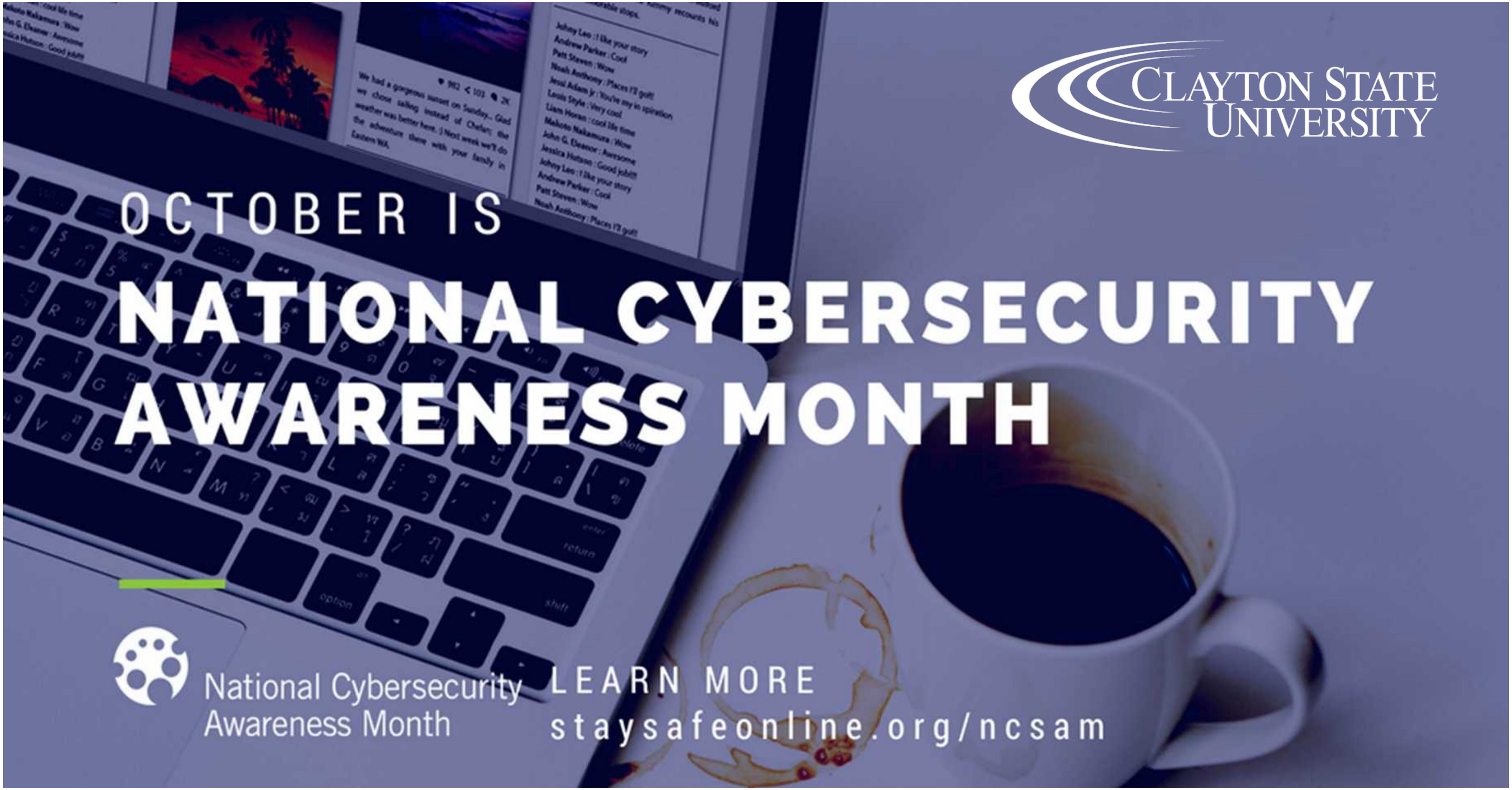


CLAYTON STATE UNIVERSITY

OCTOBER IS

NATIONAL CYBERSECURITY AWARENESS MONTH

National Cybersecurity Awareness Month

LEARN MORE

staysafeonline.org/ncsam

LaMarcus Lawrence

Information Security Officer

lamarcuslawrence@clayton.edu

678.466.4390

Information Technology Services

STATE MANDATE

- Georgia Gov. Brian Kemp issued an executive order instructing state employees to undergo semiannual cybersecurity training and stipulates that the first round of training be completed within 90 days of Kemp's directive, and that employees who do not comply with the training requirements may receive corrective actions.
- To comply with State and BOR we will be rolling out cybersecurity training in phase one of the HR rollout.
- Memorandum from the U.S. Department of Homeland Security's Cybersecurity and Infrastructure Security Agency that urged state and local governments to take "immediate action" to shore up their defenses against ransomware.

CLAYTON STATE UNIVERSITY

WHAT IS SECURITY AWARENESS TRAINING?

& WHY IS IT IMPORTANT?

CLAYTON STATE
UNIVERSITY

WHAT IS CYBER AWARENESS TRAINING?

Security awareness training is a formal process for educating employees about computer security.

A good security awareness program should educate employees about corporate policies and procedures for working with information technology (IT). Employees should receive information about who to contact if they discover a security threat and be taught that data is a valuable University asset.

WHY IS IT IMPORTANT

- Regulatory Requirements
- The Vanishing Perimeter (Bring Your Own Devices policies).
- Vanishing Perimeter, refers to your network being less defensible because people in your organization are using devices and connections that are not under our direct security posture. Vanishing perimeter places an even greater emphasis on proper **cyber hygiene**, which can be taught by a good security training program.
- Constant Changes in the Threat Landscape
- Finally, our team has to stay on top of the latest cyber threats out there that look to exploit our community.

READY FOR SOME SCARY STATISTICS FOR 2019?

- The state has paid out 1.6 million in ransom attacks.
- The average financial cost of a data breach is $3.86m (IBM).
- Phishing accounts for 90% of data breaches.
- 15% of people successfully phished will be targeted at least one more time within the year.
- Business Email C scams accounted for over $12 billion in losses (FBI).
- Phishing attempts have grown 65% in the last year.

CLAYTON STATE UNIVERSITY

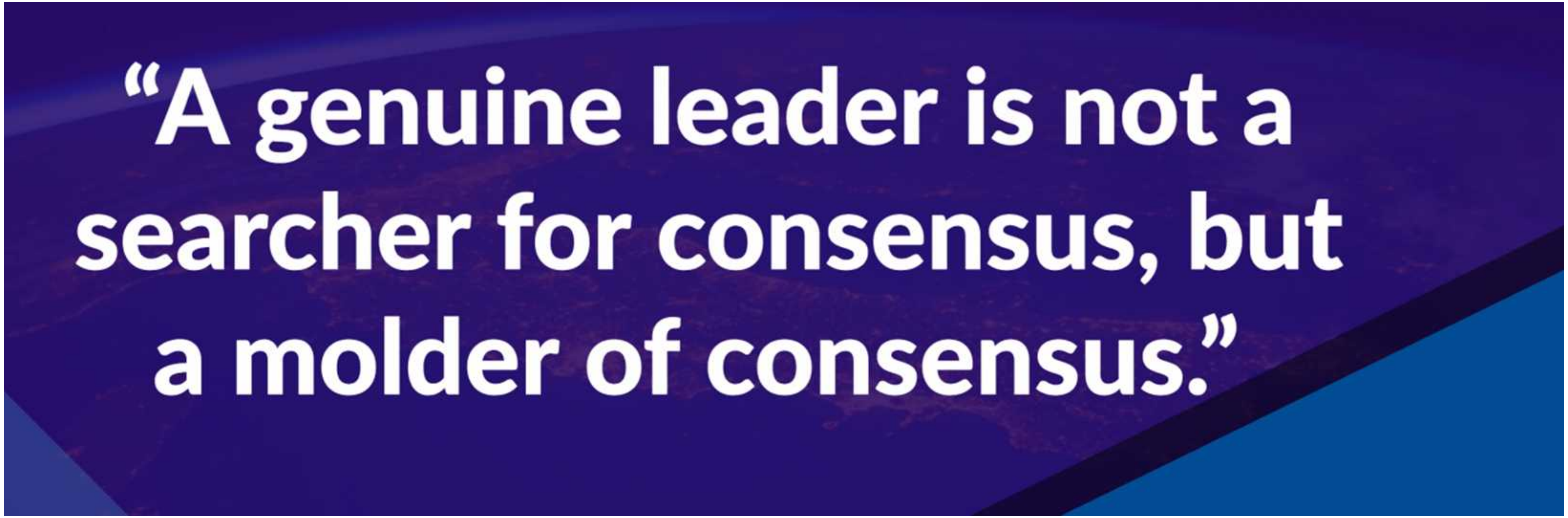
WHY DO WE IT - IMPLEMENT CYBERSECURITY?

- 1. To prevent breaches and attacks. (Prepare the college to be resilient to cybersecurity attacks and failures.)
- 2. To influence University culture.
- 3. Ensuring the confidentiality, integrity, and availability of its information systems, data, & intellectual property, while make technological defenses more robust.
- 4. To better serve our internal and external teams and customers.
- 5. Ensure that the college is compliant with all applicable laws and regulations.
- 6. Socially responsible for the care of data.
- 7. For employee's wellbeing and secure workplace.
- Support the President and other leadership in data driven decision making.

- We are depending on you – the leadership of CSU.

CLAYTON STATE UNIVERSITY

CYBER-MOTIVATION



"A genuine leader is not a searcher for consensus, but a molder of consensus."

TOPICS ADDRESSED IN THE TRAINING

- The Increasing types of threats. The approaches are ever-changing.
- Confidentiality, Availability, Integrity.
- Legal and Regulatory standards that apply to USG organizations.
- Data Governance and Management.
- Personal Information Security
- Identifying threats and reporting them. (HUB, itsecurity@clayton.edu, Contact ISO)
- Policies, Standards, and Guidelines.

- We are in the process of updating training content. We listen to your feedback!

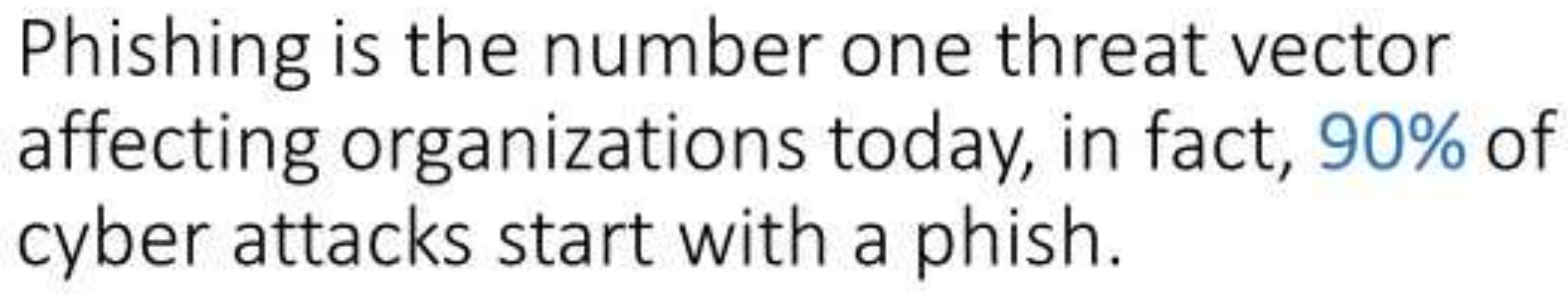
IMPORTANT POINTS TO REMEMBER

- Cyber Security Awareness Training
- Phishing Simulation Exercise
- Table Top Exercise
- Take a look and keep an eye for all the fun informative Cybersecurity Announcements this month
- Cyber-Security Sub-Committee to Information Technology Council

CLAYTON STATE UNIVERSITY

CSU CYBER-SECURITY SUB-COMMITTEE

- The CSU Cyber-Security Sub-Committee is a campus wide partnership comprised of key stakeholders, subject matter experts, student organizations and education professionals from CSU's academic community.
- The Cyber-Security Sub-Committee will serves as an reporting and advisory body to the Information Technology Council in matters related to Cybersecurity.



Phishing is the number one threat vector affecting organizations today, in fact, 90% of cyber attacks start with a phish.

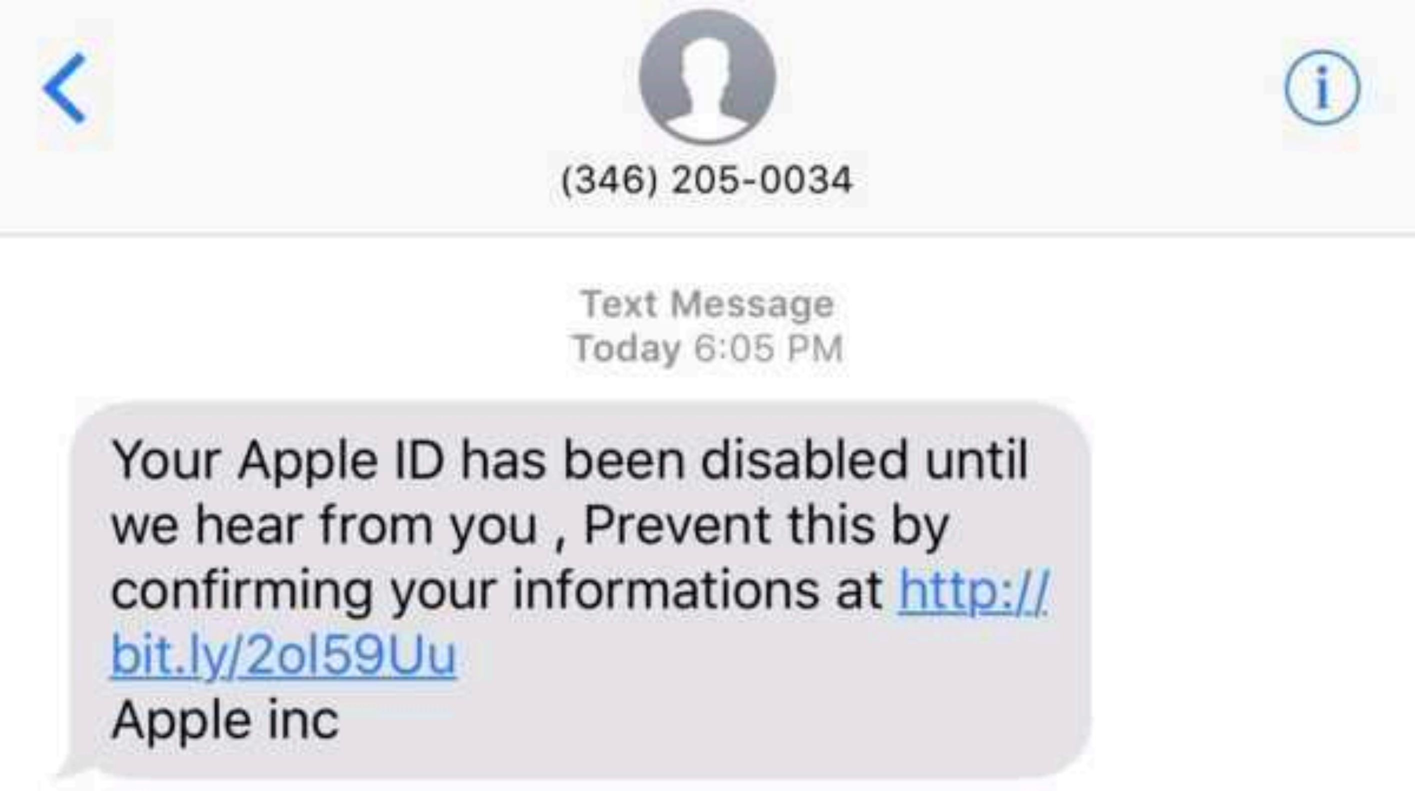
Research shows 48% of phishing attacks take place on mobile devices, and users are 3x more vulnerable to phishing on mobile than on desktop.

WHAT IS PHISHING?

- Phishing is a hacking method in which the attacker sends a malicious message, usually an email, but sometimes a text message, Skype, or Slack message.

- The attacker impersonates a trusted entity with the intention of convincing the recipient to share sensitive information, transfer funds, or connect to a fraudulent website.

SMISHING IS PHISHING DONE THROUGH SMS.

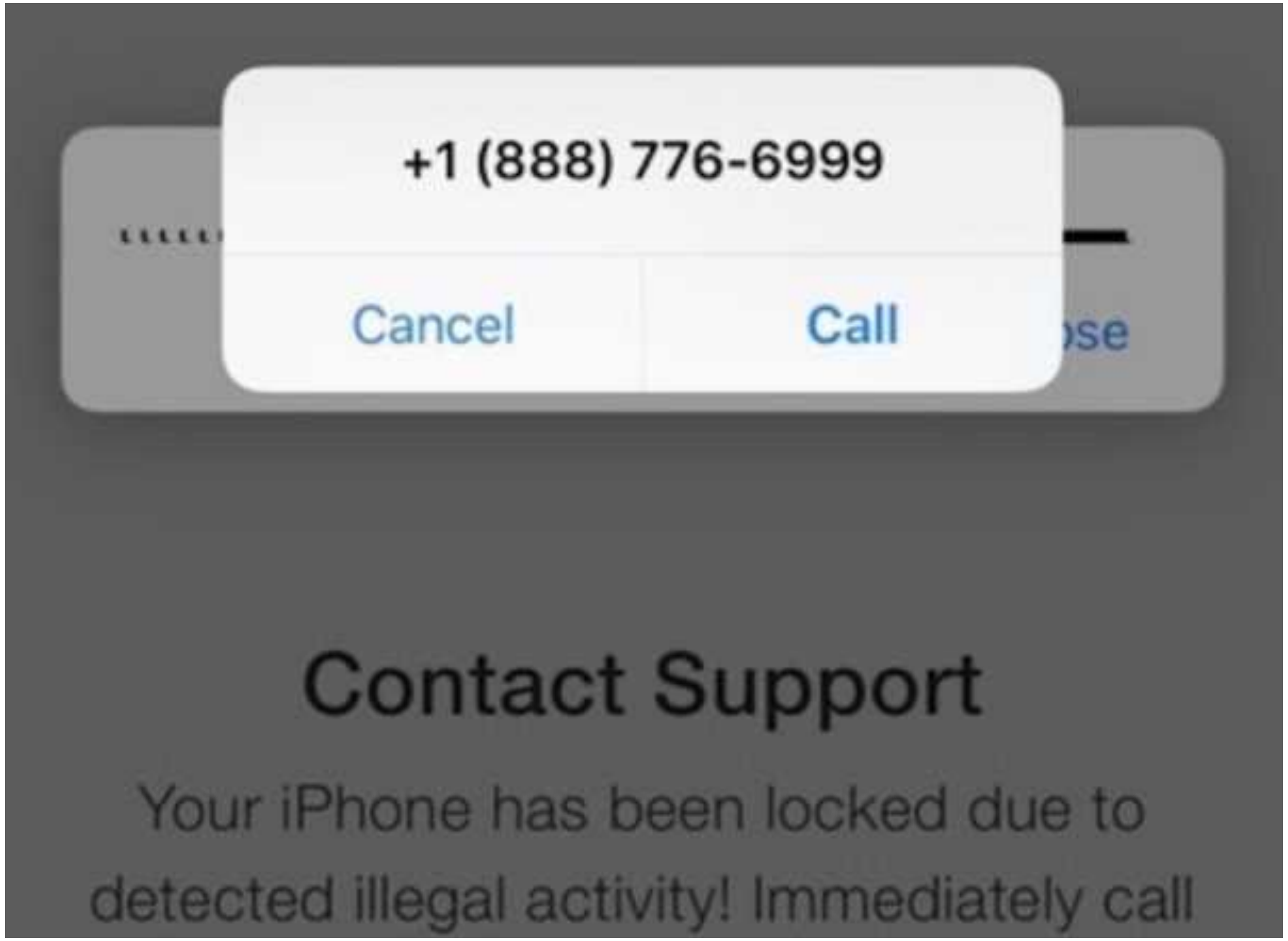


(346) 205-0034

Text Message
Today 6:05 PM

Your Apple ID has been disabled until we hear from you , Prevent this by confirming your informations at http://bit.ly/2ol59Uu
Apple inc

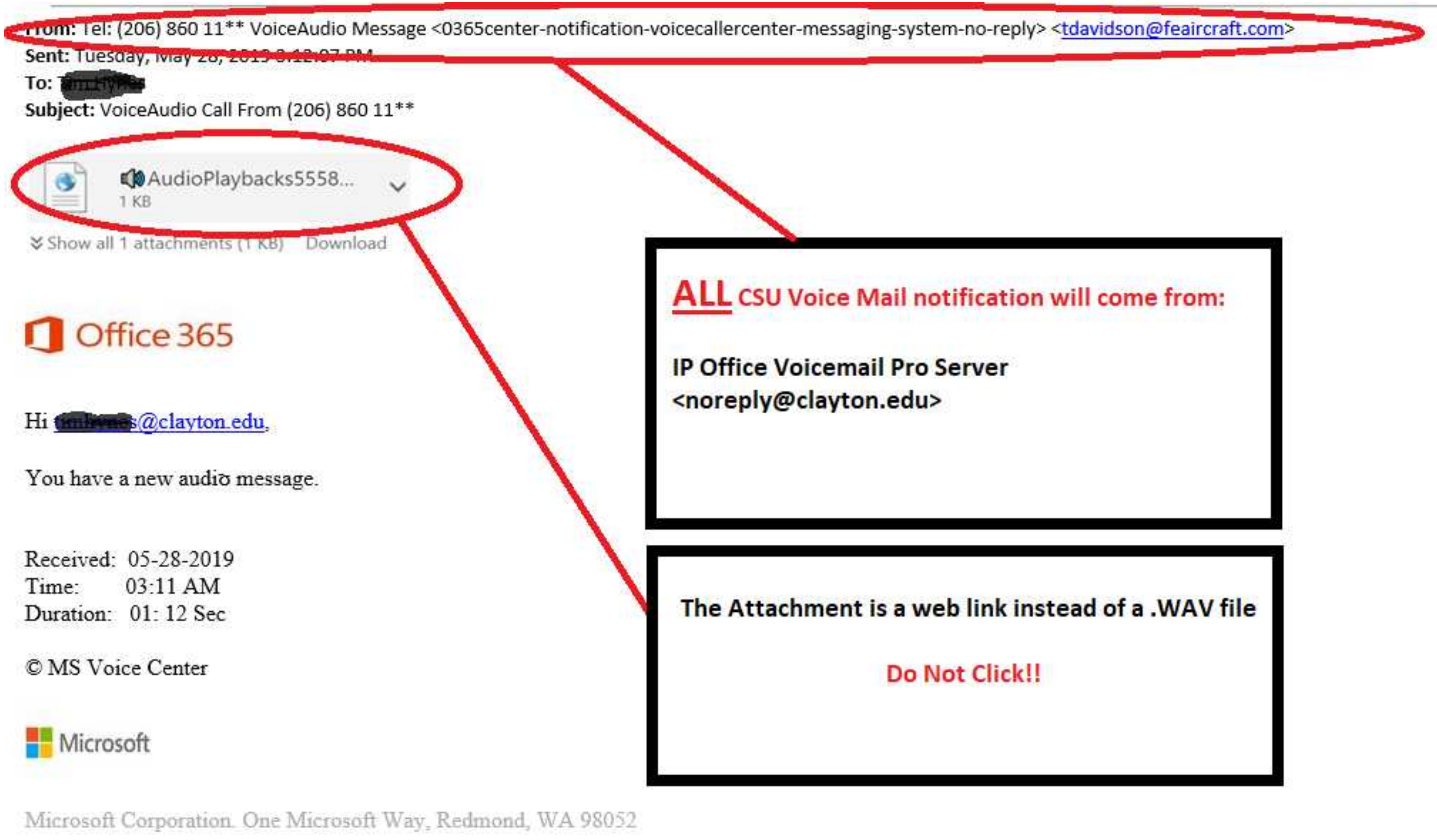
VISHING, OR VOICE-MAIL PHISHING, IS PHISHING DONE WITH THE USE OF A DEVICE'S CALL FEATURE.



+1 (888) 776-6999

Contact Support

Your iPhone has been locked due to detected illegal activity! Immediately call



From: Tel: (206) 860 11** VoiceAudio Message <0365center-notification-voicecallercenter-messaging-system-no-reply> <tdavidson@feaircraft.com>
Sent: Tuesday, May 28, 2019 3:12:07 PM
To: [redacted]
Subject: VoiceAudio Call From (206) 860 11**

Hi [redacted]@clayton.edu,

You have a new audio message.

Received: 05-28-2019
Time: 03:11 AM
Duration: 01: 12 Sec

© MS Voice Center

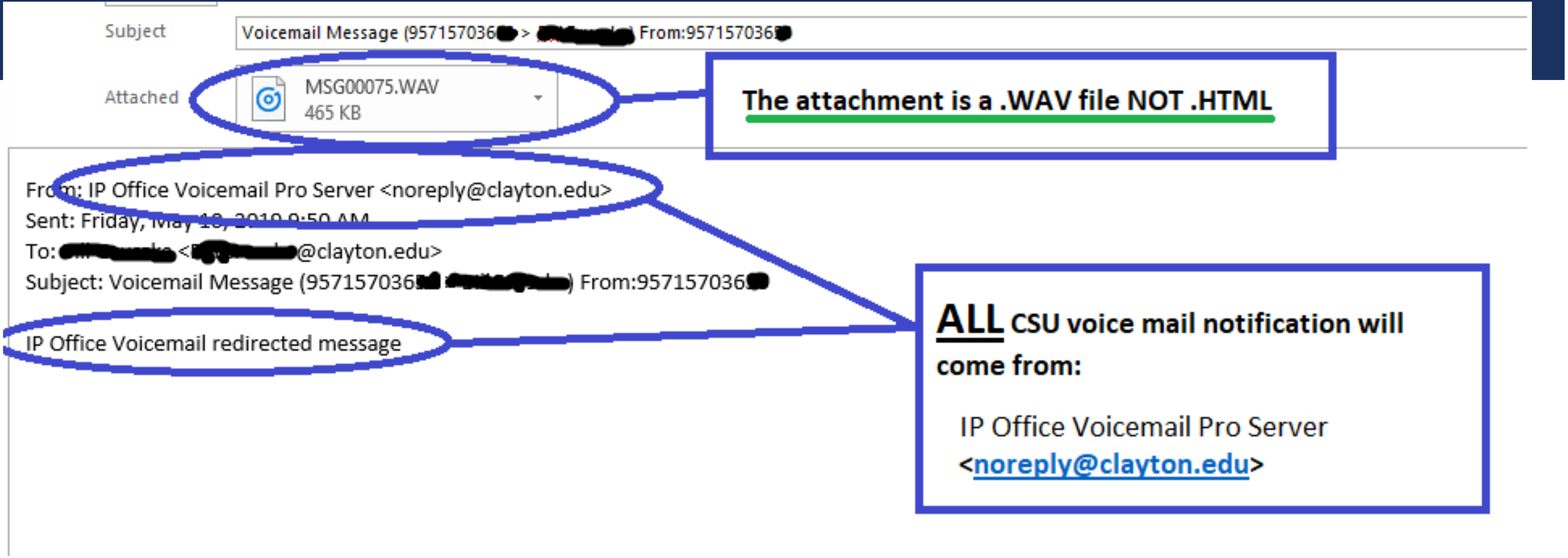
Microsoft Corporation. One Microsoft Way, Redmond, WA 98052

ALL CSU Voice Mail notification will come from:

IP Office Voicemail Pro Server
<noreply@clayton.edu>

The Attachment is a web link instead of a .WAV file

Do Not Click!!



Subject: Voicemail Message (957157036[redacted]> [redacted] From:957157036[redacted]

Attached: MSG00075.WAV
465 KB

From: IP Office Voicemail Pro Server <noreply@clayton.edu>
Sent: Friday, May 10, 2019 9:50 AM
To: [redacted] <[redacted]@clayton.edu>
Subject: Voicemail Message (957157036[redacted] [redacted]) From:957157036[redacted]

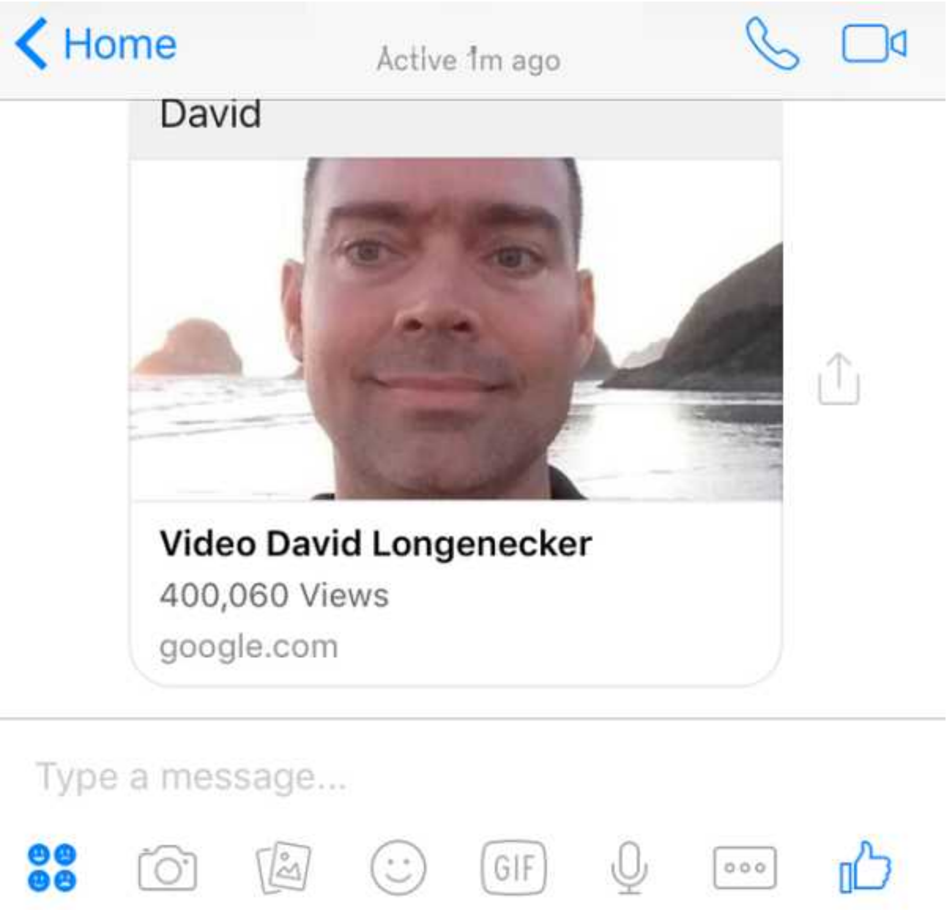
IP Office Voicemail redirected message

The attachment is a .WAV file NOT .HTML

<u>**ALL**</u> **CSU voice mail notification will come from:**

IP Office Voicemail Pro Server
<noreply@clayton.edu>

Messenger phishing: uses messaging services on mobile devices. Examples: WhatsApp, Instagram, Viber, Skype, Snapchat, and Slack.



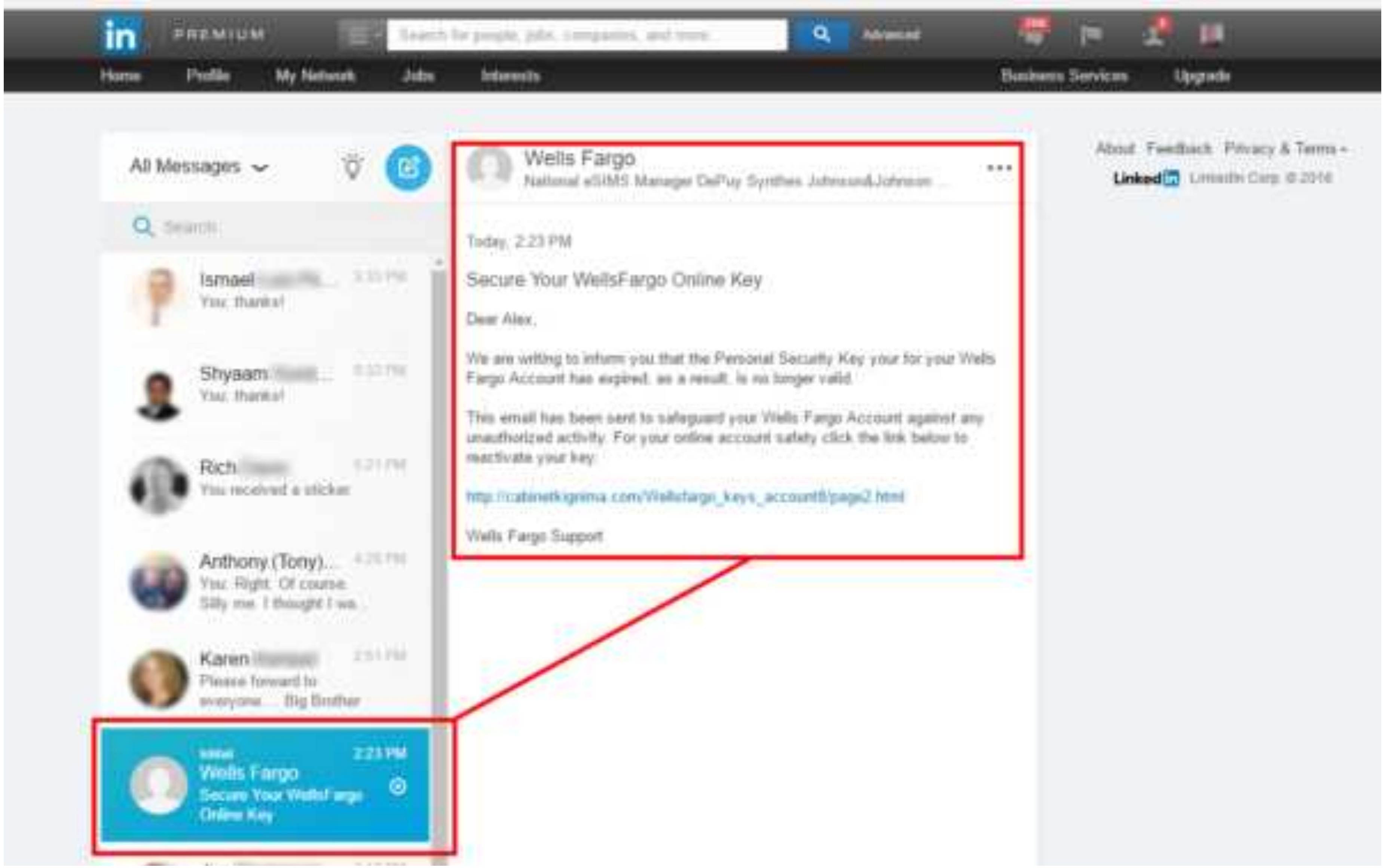
David

Video David Longenecker

400,060 Views

google.com

PHISHING MESSAGE SENT TO A RECIPIENT VIA LINKEDIN'S INMAIL FEATURE:


PREMIUM
Search for people, jobs, companies, and more...
Advanced
Home
Profile
My Network
Jobs
Interests
Business Services
Upgrade
All Messages
Search
Ismael [redacted] 3:33 PM
You: thanks!
Shyaam [redacted] 3:32 PM
You: thanks!
Rich [redacted] 3:21 PM
You received a sticker
Anthony (Tony)... 4:26 PM
You: Right. Of course. Silly me. I thought I wa...
Karen [redacted] 2:51 PM
Please forward to everyone.... Big Brother
InMail 2:23 PM
Wells Fargo
Secure Your WellsFargo Online Key
About Feedback Privacy & Terms
LinkedIn LinkedIn Corp. © 2016

Wells Fargo
National eSIMS Manager DePuy Synthes Johnson&Johnson ...

Today, 2:23 PM

Secure Your WellsFargo Online Key

Dear Alex,

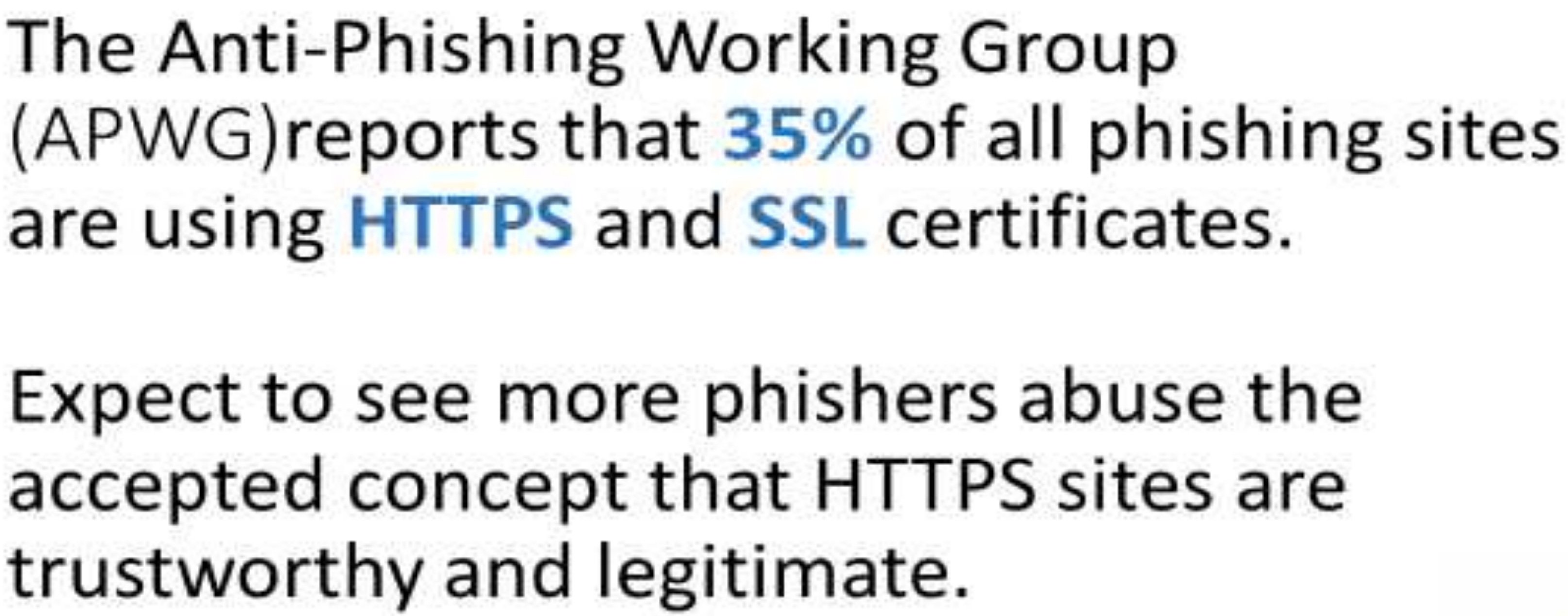
We are writing to inform you that the Personal Security Key your for your Wells Fargo Account has expired, as a result, is no longer valid.

This email has been sent to safeguard your Wells Fargo Account against any unauthorized activity. For your online account safety click the link below to reactivate your key:

http://cabinetkigema.com/Wellsfargo_keys_account8/page2.html

Wells Fargo Support

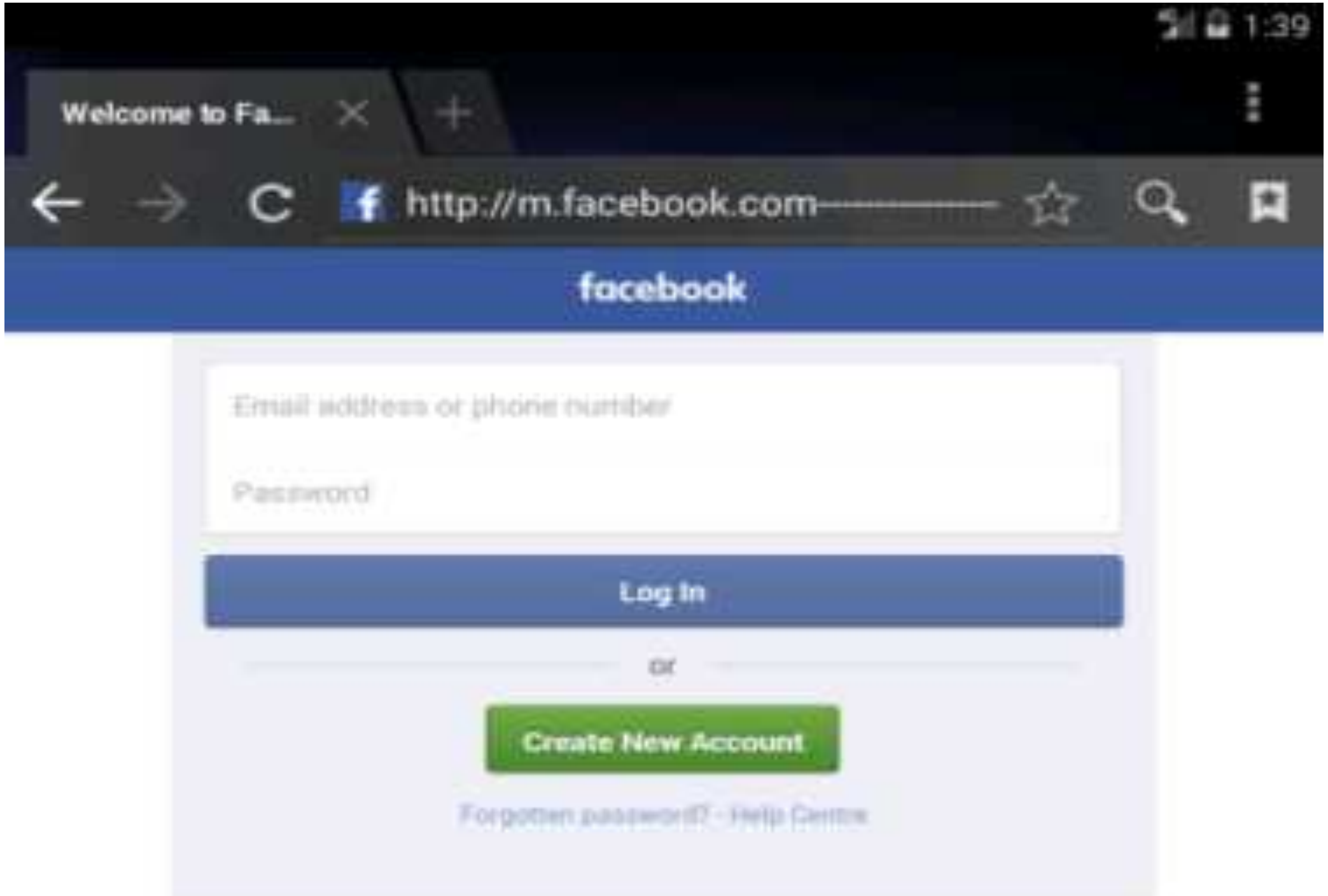
FACT:



The Anti-Phishing Working Group (APWG)reports that **35%** of all phishing sites are using **HTTPS** and **SSL** certificates.

Expect to see more phishers abuse the accepted concept that HTTPS sites are trustworthy and legitimate.

WHAT WRONG WITH THIS ONE?



UNEXPLAINED DASHES AFTER A URL CAN REDIRECT TO BOGUS SITE:

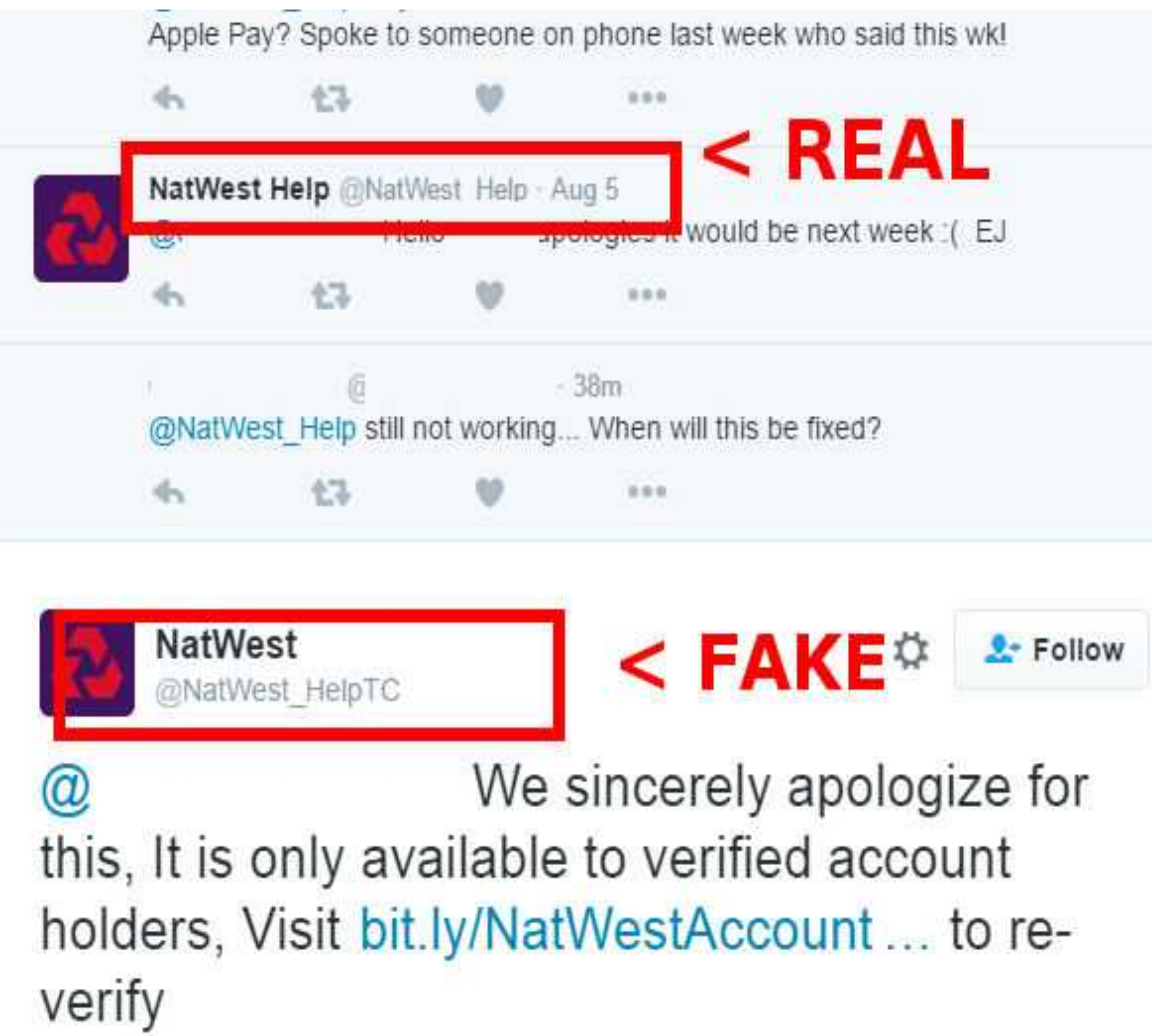
- In this example, the complete URL is:

hxxp://m.facebook.com----------------validate----step1.rickytaylk[dot]com/sign_in.html,

where rickytaylk[dot]com is the domain and m.facebook.com----------------validate----step1 is the long subdomain.

*****Copy the URL and paste it on a notepad app*****

A Twitter account posing as NatWest bank inserted itself into a live conversation between a NatWest bank client and NatWest's official Twitter channel.



Apple Pay? Spoke to someone on phone last week who said this wk!

NatWest Help @NatWest_Help · Aug 5

@ Hello apologies it would be next week :(EJ

< REAL

@ · 38m

@NatWest_Help still not working... When will this be fixed?

NatWest
@NatWest_HelpTC

< FAKE

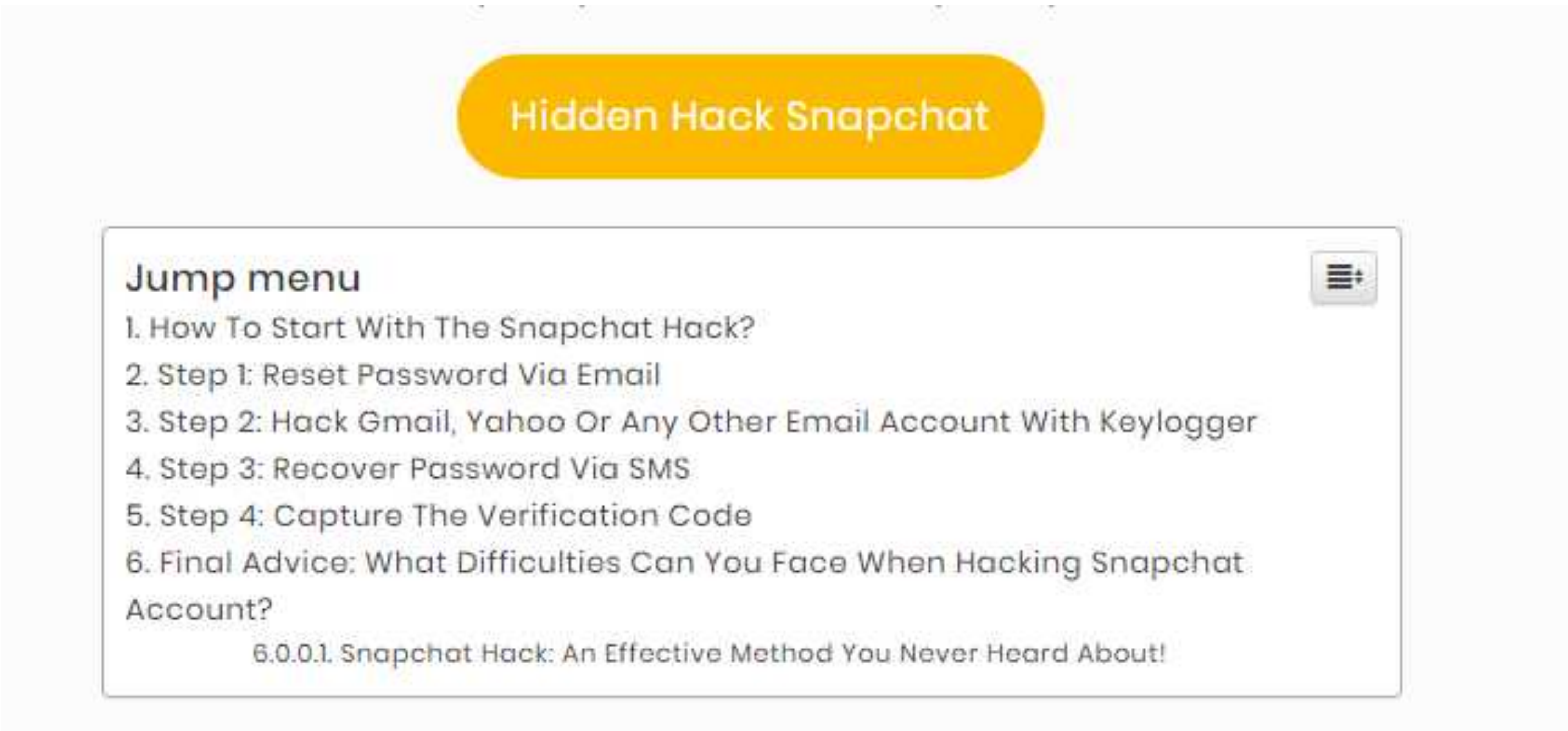
Follow

@ We sincerely apologize for this, It is only available to verified account holders, Visit bit.ly/NatWestAccount ... to re-verify

Research has found messaging apps and social media are fast becoming the most popular delivery method for mobile phishing attacks:
(2018)

- 170% increase in messenger app phishing.
- 102% increase in social app phishing.

SEARCH RESULTS – “HOW TO HACK SNAPCHAT?”



Jump menu

1. How To Start With The Snapchat Hack?
2. Step 1: Reset Password Via Email
3. Step 2: Hack Gmail, Yahoo Or Any Other Email Account With Keylogger
4. Step 3: Recover Password Via SMS
5. Step 4: Capture The Verification Code
6. Final Advice: What Difficulties Can You Face When Hacking Snapchat Account?

6.0.0.1. Snapchat Hack: An Effective Method You Never Heard About!

MOBILE DEVICE SECURITY

- User Authentication
- Update Your Mobile OS with Security Patches
- Regularly Back Up Your Mobile Device
- Enable Remote Data Wipe as an Option

- Avoid All Jailbreaks
- Add a Mobile Security App
- Disable Wi-Fi and Bluetooth When Not Needed
- Utilize Encryption
- Don't Fall for Phishing Schemes

CLAYTON STATE UNIVERSITY

MOBILE APPLICATION SECURITY

- Avoid potentially harmful apps (PHAs)
- Be savvy with your apps
- Review app permissions
- Limit location permissions
- Be cautious with signing into apps with social network accounts
- Delete apps you do not need
- Keep app software up to date

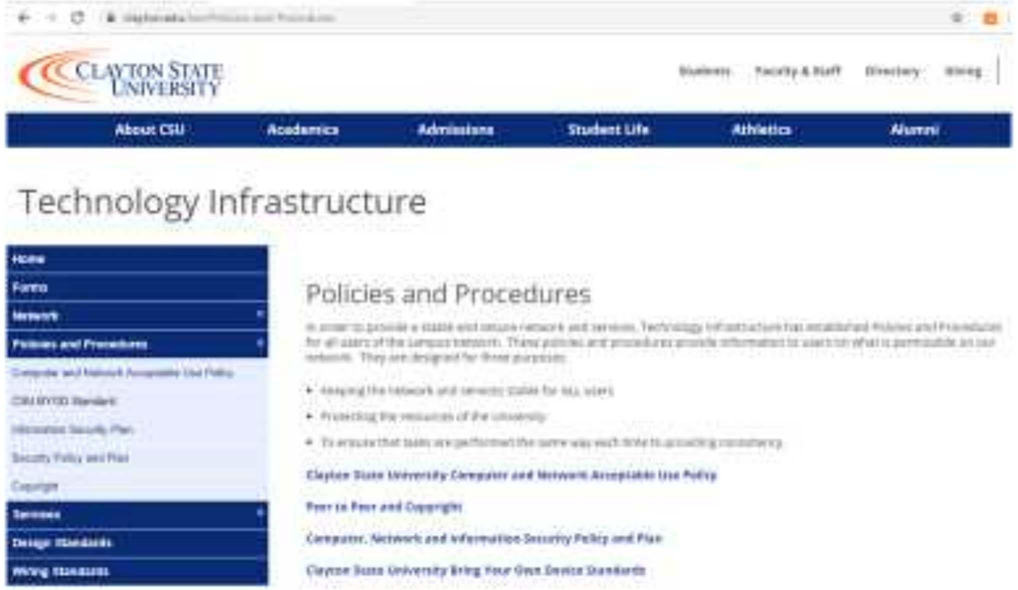
CLAYTON STATE UNIVERSITY

MOBILE DEVICE ADDITIONAL STEPS

- **Limit activities on public Wi-Fi networks** (VPN software)**.**
- **Be cautious when charging (**charging station at an airport terminal or a shared computer at a library).
- **Protect your device from theft (**Do not leave your device unattended in public or in easily accessible areas).
- **Protect your data if your device is stolen (**password or biometric identifier).

POLICIES AND PROCEDURES

https://www.clayton.edu/nes/Policies-and-Procedures



Technology Infrastructure

Policies and Procedures

In order to provide a stable and secure network and services, Technology Infrastructure has established Policies and Procedures for all users of the campus network. These policies and procedures provide information to users on what is permissible on our network. They are designed for three purposes:

- Keeping the network and services stable for ALL users
- Protecting the resources of the university
- To ensure that tasks are performed the same way each time to providing consistency

Clayton State University Computer and Network Acceptable Use Policy

Peer to Peer and Copyright

Computer, Network and Information Security Policy and Plan

Clayton State University Bring Your Own Device Standards

QUESTIONS?

CLAYTON STATE UNIVERSITY
OWN
SECURE
PROTECT
IT.
OCTOBER
2019
National Cybersecurity
Awareness Month
#BeCyberSmart

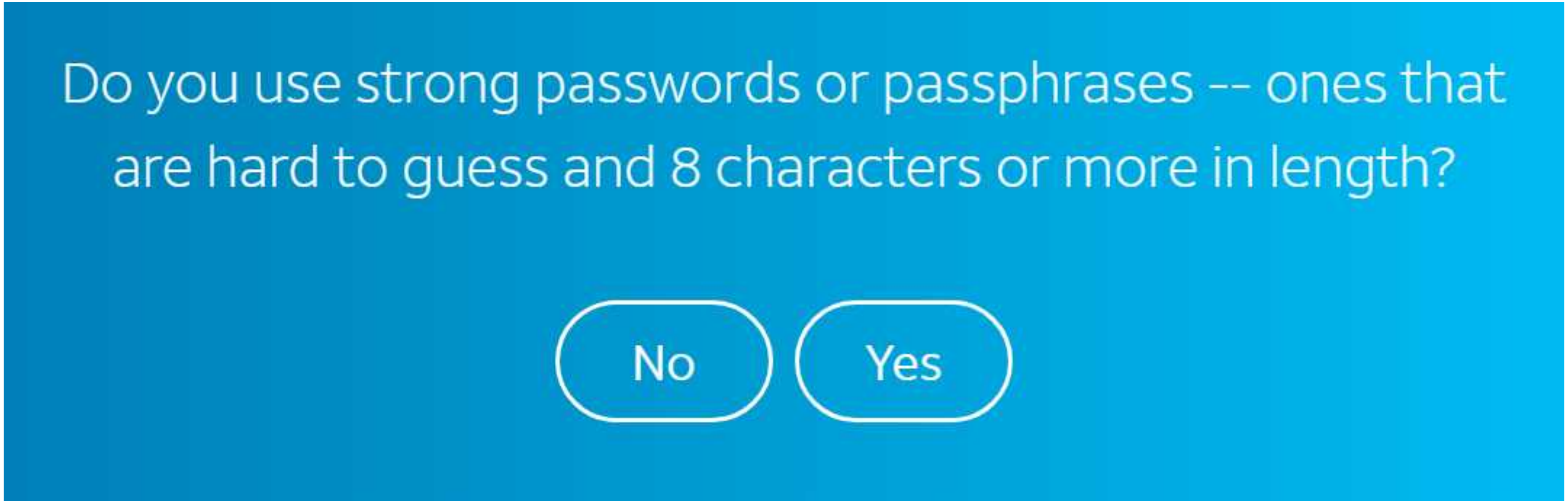
THANK YOU

LaMarcus Lawrence
Information Security Officer
lamarcuslawrence@clayton.edu
678.466.4390

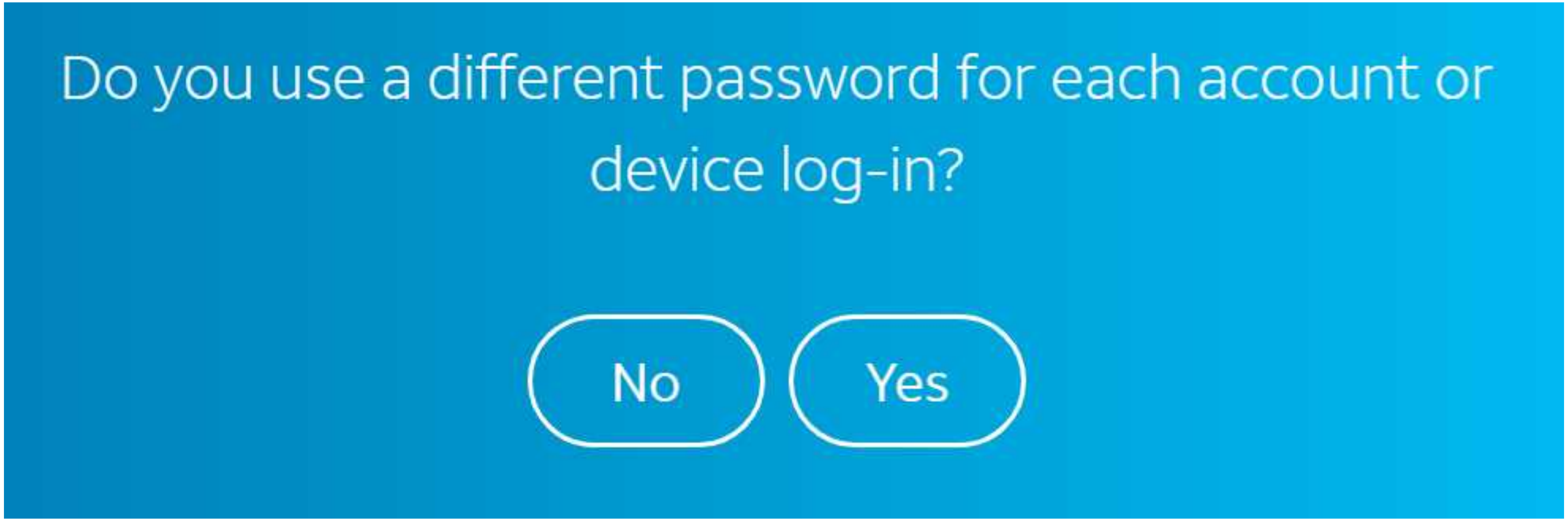
Information Technology Services

HOW CYBER SECURE ARE YOU?

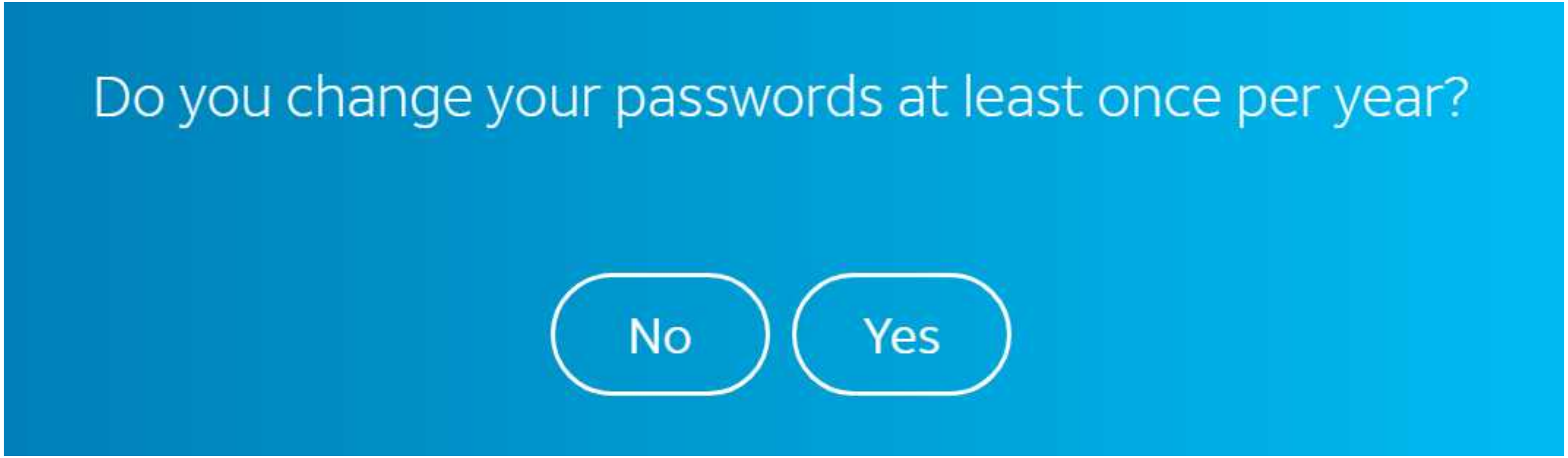
Yes , a test ☺! Please number 1-12



Do you use strong passwords or passphrases -- ones that are hard to guess and 8 characters or more in length?

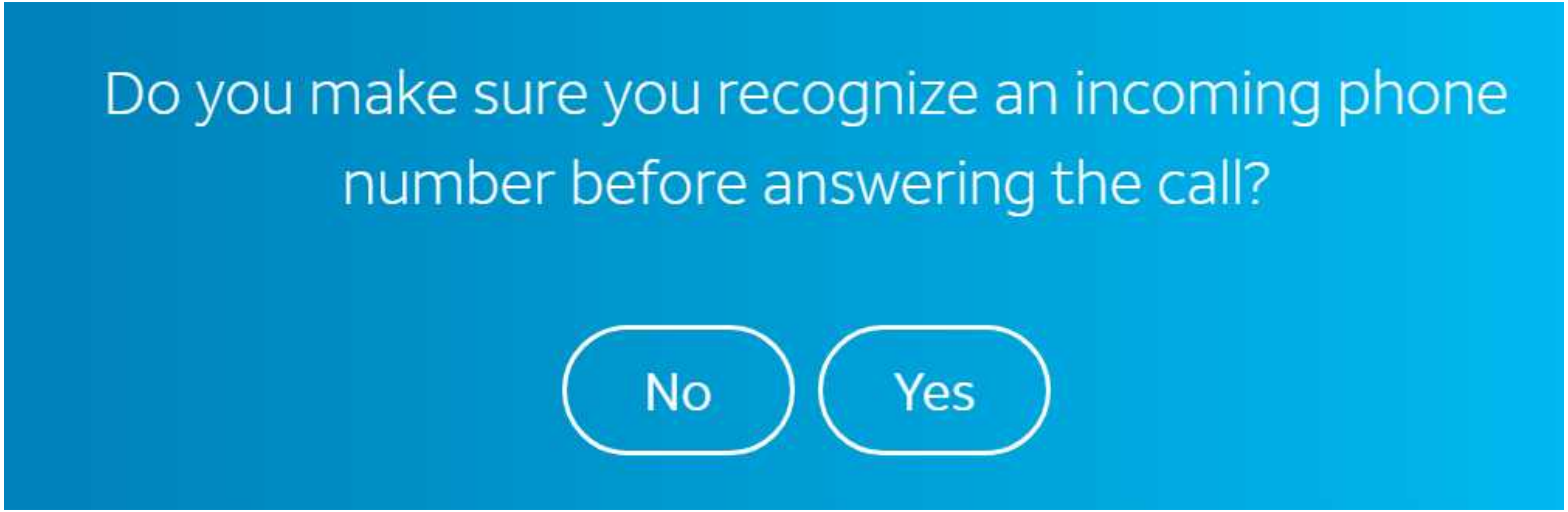


Do you use a different password for each account or device log-in?

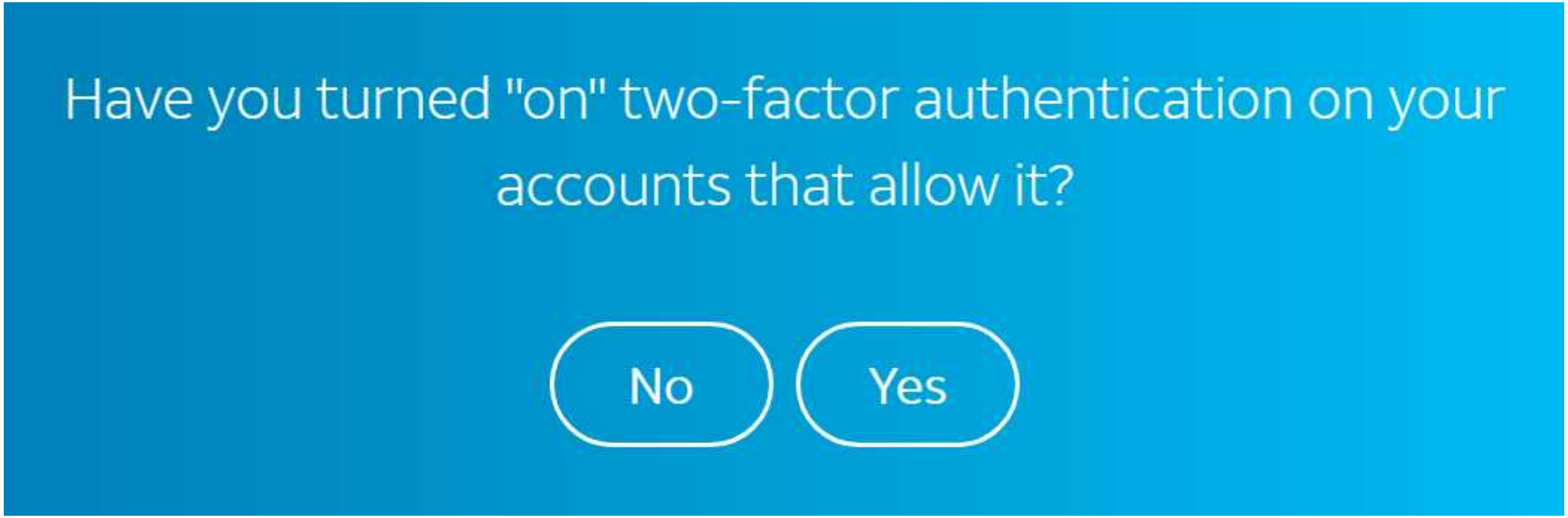


Do you change your passwords at least once per year?

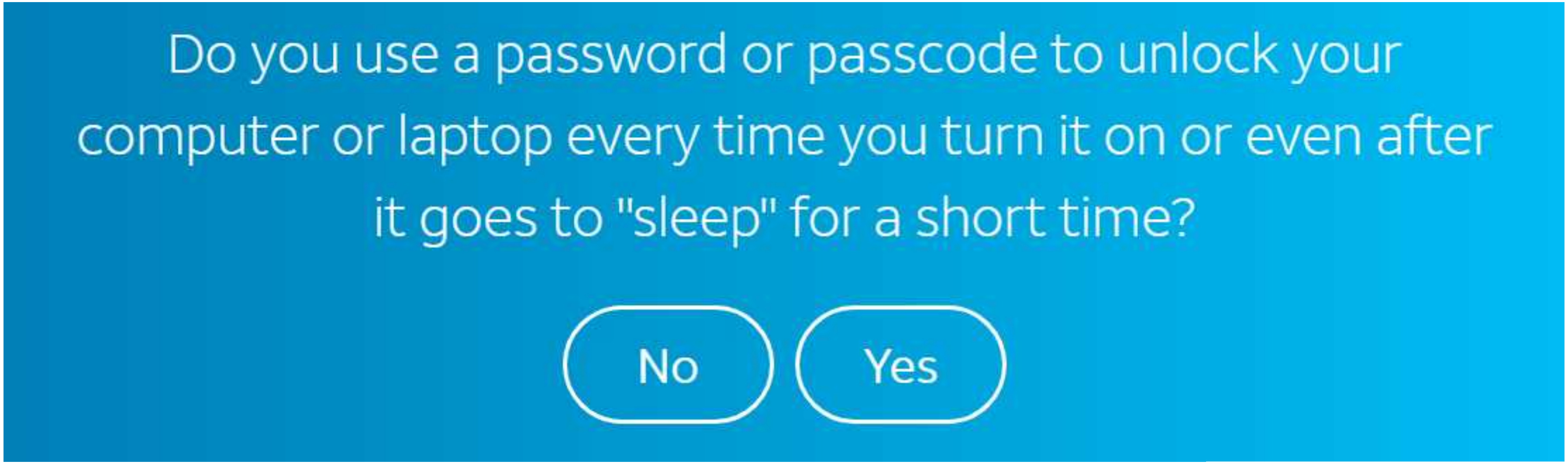
CLAYTON STATE UNIVERSITY



Do you make sure you recognize an incoming phone number before answering the call?

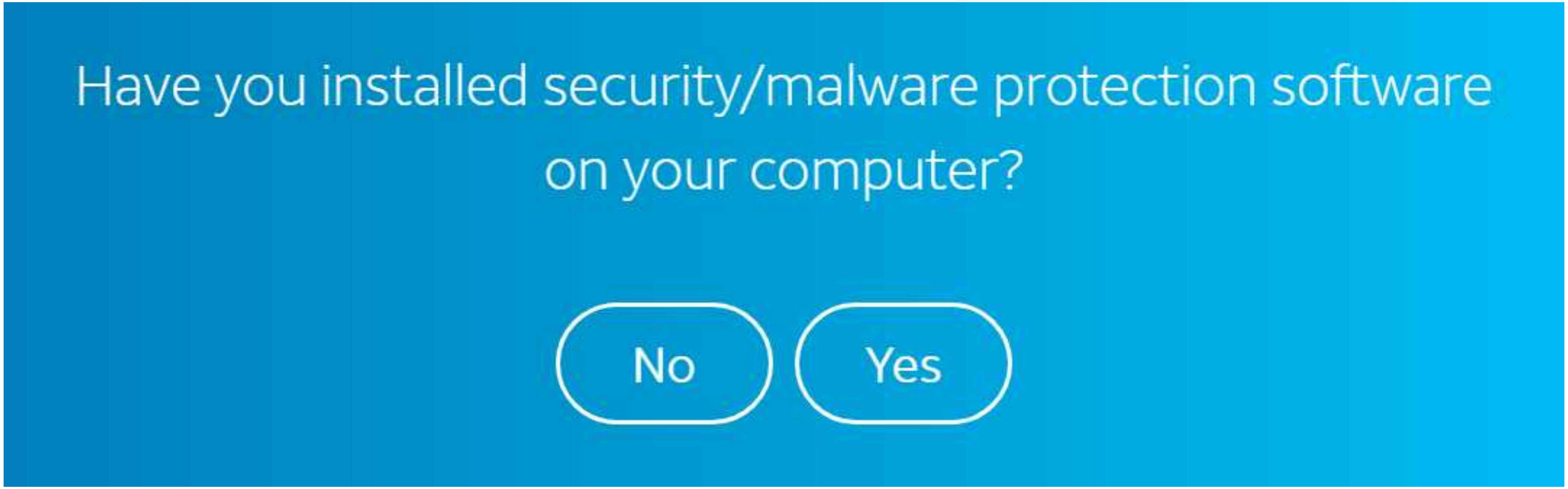


Have you turned "on" two-factor authentication on your accounts that allow it?

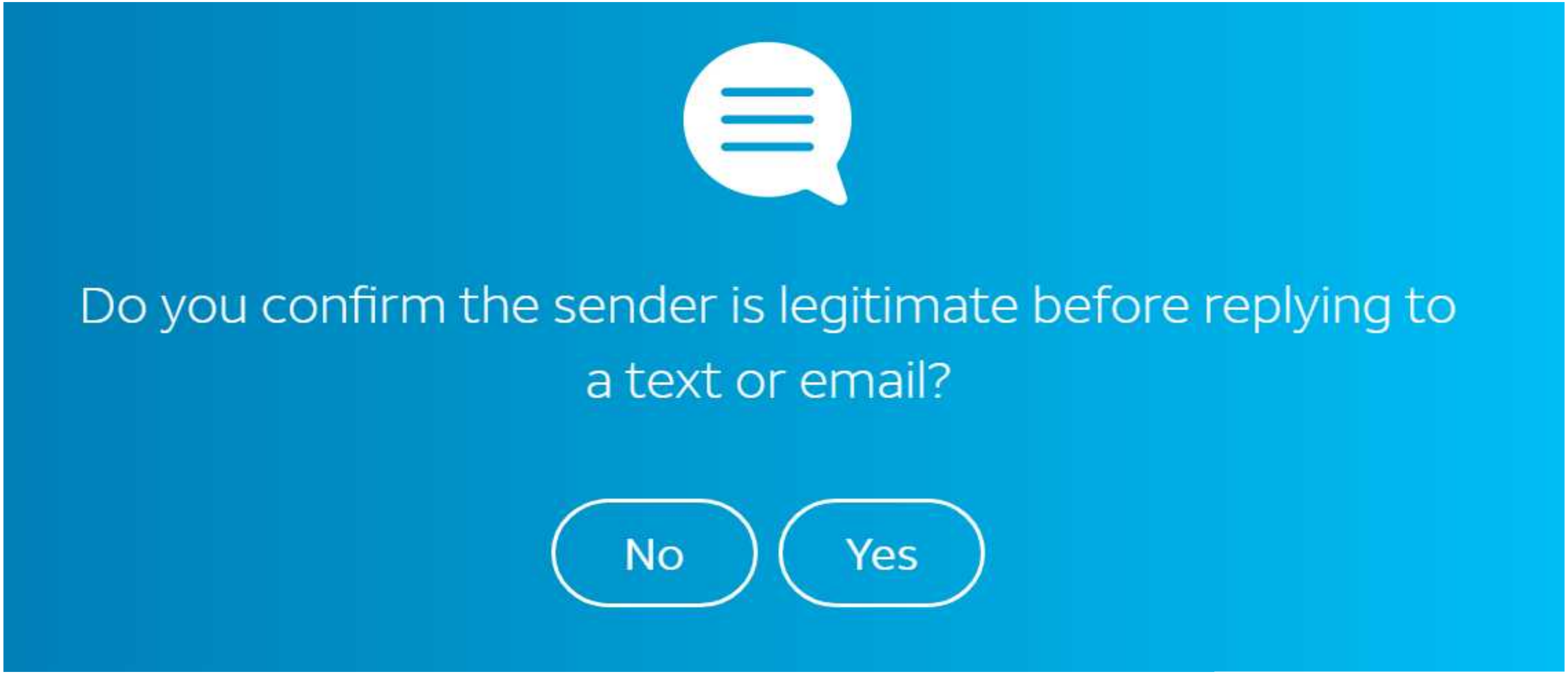


Do you use a password or passcode to unlock your computer or laptop every time you turn it on or even after it goes to "sleep" for a short time?

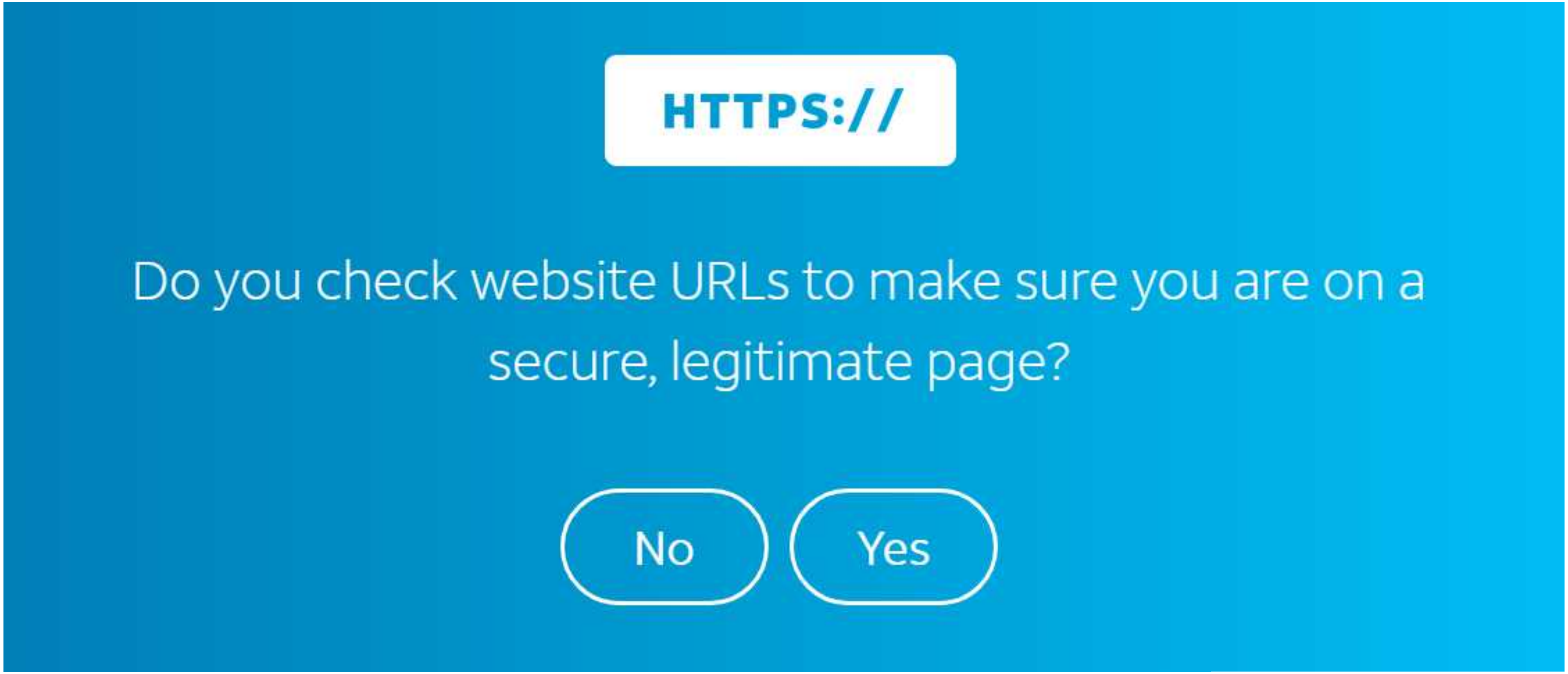
CLAYTON STATE UNIVERSITY



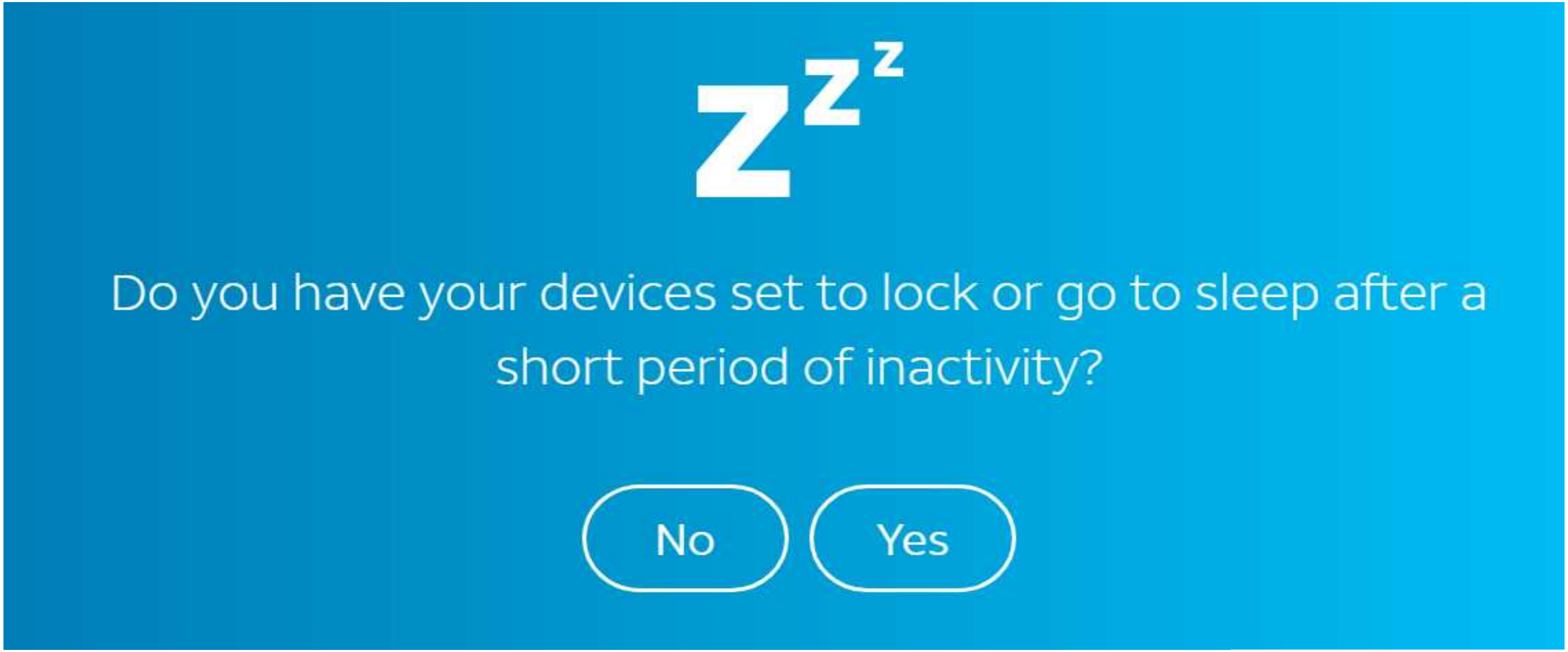
Have you installed security/malware protection software on your computer?



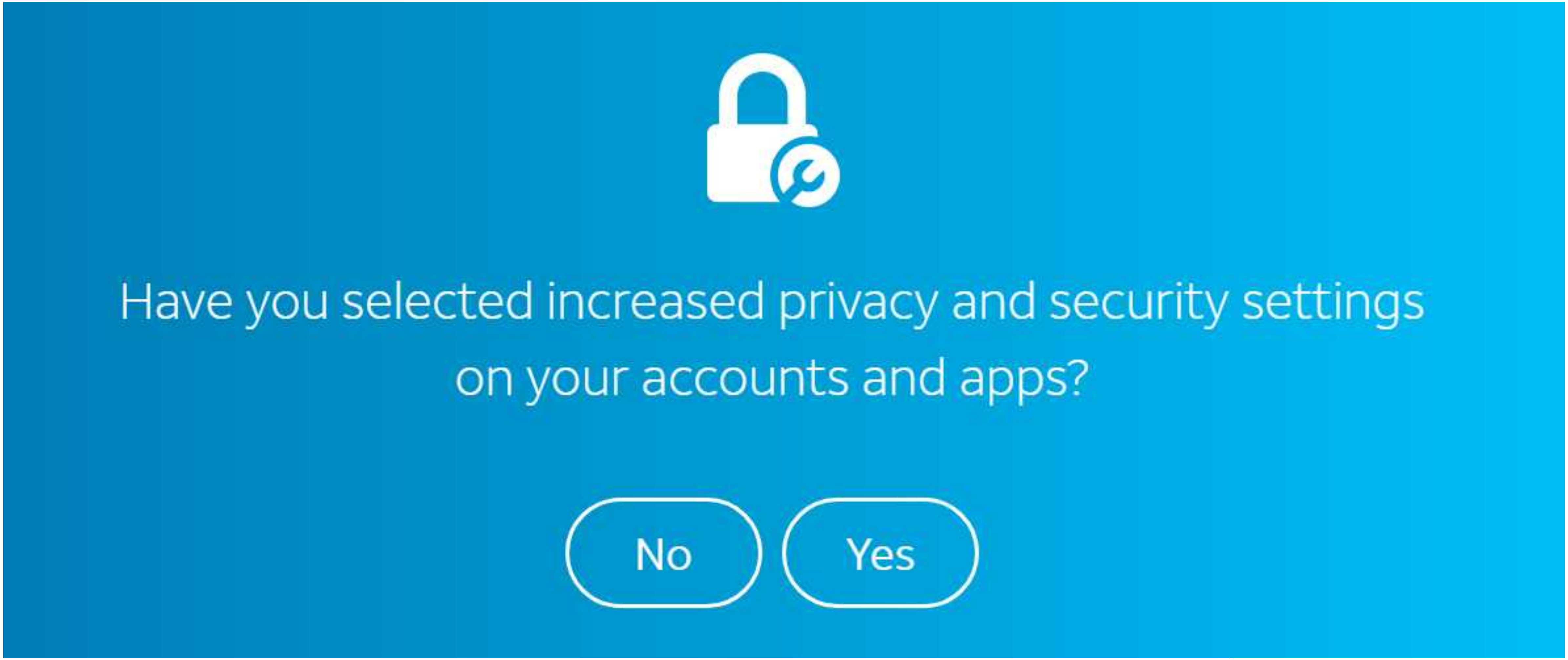
Do you confirm the sender is legitimate before replying to a text or email?



Do you check website URLs to make sure you are on a secure, legitimate page?

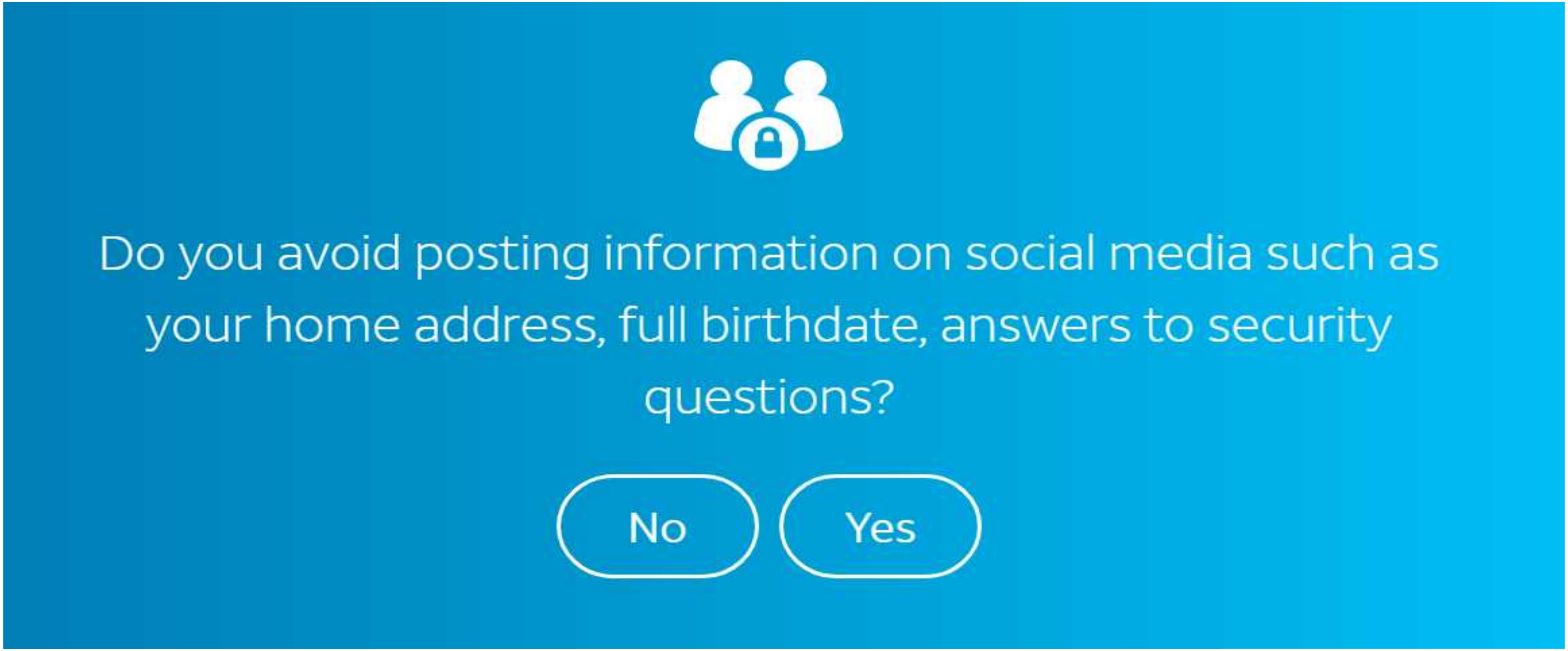


Do you have your devices set to lock or go to sleep after a short period of inactivity?

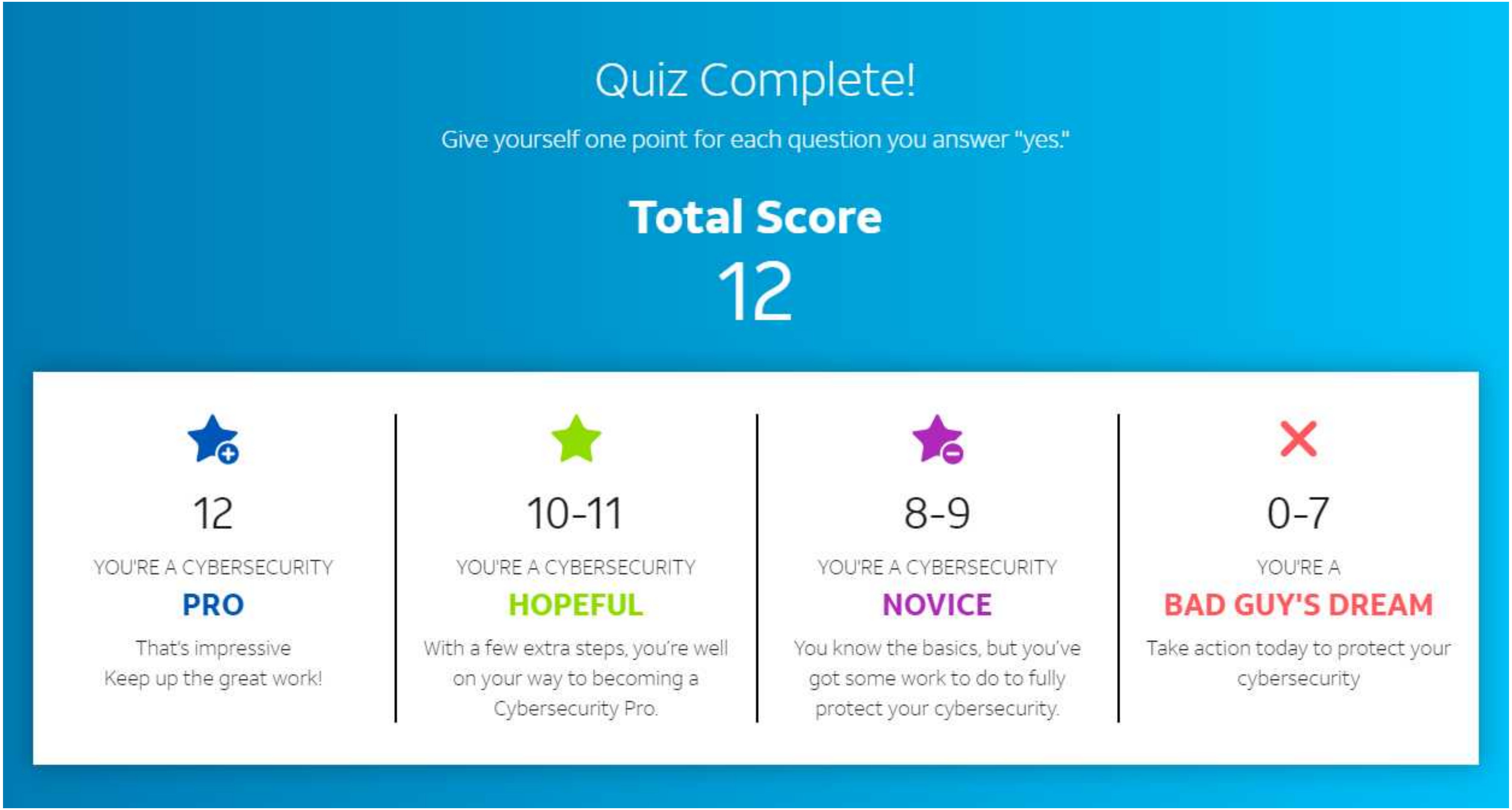


Have you selected increased privacy and security settings on your accounts and apps?

CLAYTON STATE UNIVERSITY



Do you avoid posting information on social media such as your home address, full birthdate, answers to security questions?



Quiz Complete!

Give yourself one point for each question you answer "yes."

Total Score

12

12

YOU'RE A CYBERSECURITY

PRO

That's impressive
Keep up the great work!

10-11

YOU'RE A CYBERSECURITY

HOPEFUL

With a few extra steps, you're well on your way to becoming a Cybersecurity Pro.

8-9

YOU'RE A CYBERSECURITY

NOVICE

You know the basics, but you've got some work to do to fully protect your cybersecurity.

0-7

YOU'RE A

BAD GUY'S DREAM

Take action today to protect your cybersecurity