Luce, Patrick W

From: Luce, Patrick W
Sent: Thursday, April 8, 2021 6:03 PM
To: Liao, Sui Y; Liao, Sui Y; Nish, Melinda A; Cornner, Ryan M; Gutierrez, Mercedes C; Lidz, Carmen V; Gordon, Jeanette L; Prieto, Jeffrey M; Smith, Rueben C; #-Presidents; Delahoussaye, Ronald; Perez, Monte E; Boyer, William H; Moffett, Valencia M; Dorado, Luis
Cc: Roman, Alberto J; Montevirgen, Alexis S; Gallagher, Mary P; Awan, Seher; Lee, Otto W; Limbaugh, James M; Albo-Lopez, Nicole M; Luce, Patrick W; Gribbons, Barry C
Subject: RE: Information Security Awareness for Executives: Slides and Contact Information
Attachments: LACCD_Infosec_Training_for_Executives_FINAL_2021_04_08B.pptx

All,

Thank you again for having me at the cabinet meeting today to discuss information security. The slides from today's presentation are attached for your reference. Please feel free to reach out to me with any follow-up questions you may have. I have also provided contact information for the information security team below.

- Suspicious email: phishing@laccd.edu
- Security incident: infosecincidents@laccd.edu
- Questions: infosecrequests@laccd.edu

With Best Regards,

Patrick Luce
Chief Information Security Officer
Information Technology

Los Angeles Community College District
770 Wilshire Boulevard, Los Angeles, CA 90017
Office: (213) 891-2121 | Mobile (213) 298-0488 | Fax: (213) 891-2304
lucepw@laccd.edu | www.laccd.edu

CITY / EAST / HARBOR / MISSION / PIERCE / SOUTHWEST / TRADE-TECH / VALLEY / WEST

-----Original Appointment-----
From: Liao, Sui Y
Sent: Tuesday, April 6, 2021 5:09 PM
To: Liao, Sui Y; Nish, Melinda A; Cornner, Ryan M; Gutierrez, Mercedes C; Lidz, Carmen V; Gordon, Jeanette L; Prieto, Jeffrey M; Smith, Rueben C; #-Presidents; Delahoussaye, Ronald; Perez, Monte E; Boyer, William H; Moffett, Valencia M; Dorado, Luis
Cc: Roman, Alberto J; Montevirgen, Alexis S; Gallagher, Mary P; Awan, Seher; Lee, Otto W; Limbaugh, James M; Albo-Lopez, Nicole M; Luce, Patrick W; Gribbons, Barry C
Subject: Cabinet Call
When: Thursday, April 8, 2021 4:00 PM-5:00 PM (UTC-08:00) Pacific Time (US & Canada).
Where: Zoom

Please join us at Cabinet meeting on Thursday for the Information Security Awareness session.

Zoom Link below.

Thank you for all your work on this!

With Best Regards,
Carmen V. Lidz
Vice Chancellor & Chief Information Officer
Los Angeles Community College District

From: LIAOSY@email.laccd.edu
When: 4:00 PM - 5:00 PM April 8, 2021
Subject: Cabinet Call
Location: Zoom

Topic: Cabinet
Join Zoom Meeting
https://laccd.zoom.us/j/392751545

Meeting ID: 392 751 545
One tap mobile
+16699006833,,392751545# US (San Jose)
+13462487799,,392751545# US (Houston)

Dial by your location
+1 669 900 6833 US (San Jose)
+1 346 248 7799 US (Houston)
+1 253 215 8782 US (Tacoma)
+1 312 626 6799 US (Chicago)
+1 929 205 6099 US (New York)
+1 301 715 8592 US (Washington D.C)
Meeting ID: 392 751 545
Find your local number: https://laccd.zoom.us/u/adtRoTfCnz

Los Angeles Community College District

Information Security Awareness Tactical Training for LACCD Executives

Patrick Luce, LACCD CISO

Version 1.0 April 8, 2021

Training goal

The purpose of this training session is to provide LACCD executives with awareness of specific information security risks they face, and how they can help protect themselves, their staff, their students and the district.

Agenda

- Executives as targets
  - Why and how executives are targeted by attackers, and how to protect yourself
- Executives as bait
  - How attackers leverage executives to lure staff into compromising security, and how to protect your employees
- Questions and Answers

Why are executives targets?

- Attackers are criminals after money
  - Extortion (Ransomware)
  - Theft (SSNs, Credit Card Numbers, etc.)
  - Fraud (Hijacked financial accounts, fraudulent invoices or payments, etc.)
- Executives have more access to more money
  - Access to financial accounts and/or sensitive data, authority over business operations, etc.
- Larger payouts merit more attention and investment
  - Executives draw more skilled attackers who invest more time and energy
- Many executives (tend to) make themselves easy targets
  - Public figures, require constant connectivity, time constraints

How are executives targeted?

GOOGLE

DEMONSTRATION

Most attacks begin with user communications

- Attackers begin by sending fraudulent emails, text messages or phone calls to induce people to:
  - Install malware (for ransomware or keystroke logging)
  - Provide personal information or account login information (to steal data or transfer funds)
  - Induce someone to send money to a fraudulent account or user
- These communication techniques have common names:
  - Phishing: General in nature
  - Spear Phishing: Targeted attacks from an attacker who performed research
  - Whaling: Spear-phishing attack of a high-level employee
  - Business Email Compromise: Induce user to commit wire fraud
    - Bogus invoices, CEO impersonation, Attorney impersonation, etc.

Phishing

From: Kevin Griffin <kgriffin@lbdnhXXX.org>
Sent: Wednesday, October 7, 2020 9:50 AM
To: Doe, Monica <doemo@elac.edu>
Subject: Wednesday, October 7 2020

SharePoint

You have a new fax! Click the attachment to view.

https://online.pubhtml5.com/jufw/hhpv/
Ctrl+Click to follow link

http://online.pubhtml5.com/xxx

Print & Preview Here

Fax Details

Date Received: 2020-10-07 07:35:14 CDT
Type: Attached in pdf
Number of Pages: 3
File Size: 18.5MB

Thank you for choosing MetroFax!

Sincerely,
The MetroFax Team

Tip: Switch to an annual plan and save! Call (888) 322-3121.

Home | Features | Mobile App | Support

Spear Phishing

From: 8 June, 2020 Elac.edu Support-HQ <support@receptionhq.com>
Sent: Monday, June 8, 2020 12:01 PM
To: Example, Monica <EXAMPLEM@ELAC.EDU>
Subject: Open Ticket: Ref: KTR7RBG6PG

Hi Examplem,

Your **examplem@elac.edu** Password has expired and Outlook access will be suspended. Proceed below to continue with your current Password.

https://www.epirusnet.eu/happiness2020/zgvsyxbhbublbgfjlmvkdq==
Ctrl+Click to follow link

Keep Same Details

Thank you,
Elac.edu Microsoft Corporation

https://www.epirusnet.eu/happiness2020/...

Side Note

DEMONSTRATION

CREDENTIAL STUFFING

https://haveibeenpwned.com/

How to protect yourself (and the District)

- Be mindful of the information you choose to make public (both personal and District information)
- Always keep applications and antivirus up to date (don't delay the updates)
- Use a different password (or passphrase) on every single account, and change passwords periodically.
  - Use passphrases instead of words
  - Use a password database if necessary
- Never share your password with anyone for any reason, especially for your email account or sensitive systems (i.e. SAP or SIS)
- Never ask for anyone's password for anything, and never send passwords via email.
- Be vigilant with every email, text or phone call before responding

Email/text/phone vigilance

- The message came from a person you know who identifies themselves in a way that you understand
  - They have a name, caller ID matches, etc.
- You are an appropriate person to be contacted for the purpose of the message.
- The person addresses you in a way that you understand
- The domain name of the email sender makes sense to you, and matches the domain name in the link
  - Hover over all links before clicking and compare the domain
  - Look at the link again in the browser after clicking the link
- The grammar and tone realistically reflect the organization who is communicating with you
- IF YOU AREN'T SURE, REPORT TO PHISHING@LACCD.EDU

A real email…

From: Microsoft (do not reply) <maccount@microsoft.com>
Sent: Monday, September 30, 2019 3:15 AM
To: …; Luce, Patrick W <LUCEPW@EMAIL.LACCD.EDU>; …
Subject: Action Required – over-assigned licenses

Microsoft

Looks like you're using more licenses of Visio Online Plan 2 for faculty than are available to you.

The highlighted subscriptions have expired, and those licenses are not available.

What do I need to do?

- **Purchase additional licenses** - Purchase at least 3 more licenses to stay in compliance and continue using Visio Online Plan 2 for faculty.
- **Reassign licenses** - For subscriptions that are not expired, you can reclaim licenses for inactive users and assign them to other people.

Product Name: Visio Online Plan 2 for faculty

Number of assigned licenses: 3

Number of available licenses: 0

https://privacy.microsoft.com/…

Subscription ID	Number of Licenses	Subscription State	Agreement Number
caf1cc23-9ba6-44a8-9c2f-1af9dffe6e56	5	Expired	65099149

https://privacy.microsoft.com/en-us/privacystatement
Ctrl+Click to follow link

Microsoft respects your privacy. Review our online Privacy Statement.

Additional questions?
Please visit Customer Support site.
View the Store for Business and Education Agreement.

Microsoft Corporation
One Microsoft Way
Redmond, WA 98052 USA

Executives as Bait for Employees

From: Diane Ringading <areyouaprincess01@gmail.com>
Sent: Monday, July 13, 2020 7:36 AM
To: Smith, Denice A <SMITHDA@LATTC.EDU>
Subject: Re: REQUEST

Denice, I'm tied up in a meeting at the moment, Can you purchase Google play gift cards 8 pieces -$100 each at any nearby store? I would reimburse you when am through later today. i would prefer to call you but can't receive or call at the moment with my line so email will be fine.

Sincerely,
Diane Ringading

From: Smith, Denice A <SMITHDA@LATTC.EDU>
Sent: Monday, July 13, 2020 7:33 AM
To: Diane Ringading <areyouaprincess01@gmail.com>
Subject: Re: REQUEST

Good morning Diane,
Hope you had a great weekend, and sorry, I don't view my emails on Saturdays. How may I help you? Denice

---

From: Diane Ringading <areyouaprincess01@gmail.com>
Sent: Saturday, July 11, 2020 12:03 PM
To: Smith, Denice A <SMITHDA@LATTC.EDU>
Subject: REQUEST

Denice, Are you free at the moment?
Sincerely,
Diane Ringading

A more thoughtful attack

From: Diane Ringading <RINGADINGR_LATTCEDU@GMAIL.COM>
To: Smith, Denice A <SMITHDA@LATTC.EDU>
Subject: REQUEST

Denice, Are you free at the moment?
Sincerely,

Diane Ringading
Vice President of Important Things
Los Angeles Trade Technical College (LATTC)

An even more thoughtful attack

From: Diane Ringading <RINGADINGR_LATTCEDU@GMAIL.COM>
To: Smith, Denice A <SMITHDA@LATTC.EDU>
Subject: REQUEST

Hi Denice,

I am hosting a luncheon for potential donors and forgot my CalCard. Can you pay the lunch invoice in the link below with my CalCard ASAP?

https://larrysdeli.com/invoice3927265

Thanks Denice!

Diane Ringading
Vice President of Important Things
Los Angeles Trade Technical College (LATTC)

LOS ANGELES TRADE-TECH
LATTC
A Community College

The ultimate attack…

From: Diane Ringading <RINGADINGDR@LATTC.EDU>
To: Smith, Denice A <SMITHDA@LATTC.EDU>
Subject: REQUEST

Hi Denice,

I am hosting a luncheon for potential donors and forgot my CalCard. Can you pay the lunch invoice in the link below with my CalCard ASAP?

https://larrysdeli.com/invoice3927265

Thanks Denice!

Diane Ringading
Vice President of Important Things
Los Angeles Trade-Technical College

LOS ANGELES TRADE-TECH
LATTC
A Community College

Why?

DISCUSSION

What would lead an employee to pay the invoice?

How could it be prevented?

Why security breaks down…

Possible reasons the payment is made	How we can prevent it
The employee thought the email was real	Awareness training, phishing training
The employee had access to the CalCard	Be diligent with financial account numbers of any kind
The employee has high implicit trust	Encourage employees to scrutinize unusual financial requests, especially if they are from you

Compromise of an executive account can be devastating

- Use complex passwords or passphrases for your LACCD accounts (particularly email, SAP and SIS)
- Do not give your password(s) to any LACCD employee at any time, including your administrative assistant
- Encourage your staff to be wary of unusual requests from you, particularly that involve money or sensitive information
  - “Is this something he or she would normally ask me to do?”
  - Encourage them to call and ask

Executives set the tone for their employees

- Communicate with your staff that you (and your executive team):
  - will never discuss District business of any type from a non-District email address
  - will never ask for a financial transaction to be committed via email or text under any circumstances, including from District phones and email addresses
  - Will never share a password to any account for any reason, and will never ask them for a password for any reason
  - Require all employees to follow all District security rules at all times
- Assure your employees attend mandatory information security training

Avoid self-inflicted wounds

- A single lost spreadsheet with 500 or more social security numbers is a public event
- Scrutinize access requests for any District system that allows an employee to generate personal data for multiple students or employees
  - Beware of “occasional need”

Report Incidents

- Report anything you believe is suspicious, and encourage your employees to do the same
  - Suspicious email?: phishing@laccd.edu
  - Security incident?: infosecincidents@laccd.edu
  - Questions?: infosecrequests@laccd.edu

Questions?

Information Security Awareness Tactical Training

For LACCD Executives

Thank You

Patrick Luce, Chief Information Security Officer, LACCD

lucepw@laccd.edu

Luce, Patrick W

From: Luce, Patrick W
Sent: Friday, June 4, 2021 5:10 PM
To: Lidz, Carmen V; Duran, Andrew; Nersisyan, Christopher B; Saryan, Albert; Henderson, Mark E; Clarke, Ivan; Tran, Hanh; Mata, Jorge C; Mendoza, Gonzalo; Austria, Rodrigo G; Pinto, Savio C; Fujii, Takeshi; Yamamoto, Kirk M; Molina, Ed
Cc: George McCalmon (MCCALMG@EMAIL.LACCD.EDU)
Subject: Information Security Awareness Course

Dear OIT Management Team,

Thank you for testing our new Information Security Awareness Course for all LACCD employees. Most of you should have received an invitation to the course via email. You can access the course from the invitation, or navigate to https://ilearn.laccd.edu and click “Courses”, then “Infosec_Development.”

The course should take approximately 45 minutes. Please let me or George know of any issues or suggestions by the end of day next Wednesday, June 9. We will make any final edits and publish the course by the end of next week.

Please note I had an issue enrolling Ed, Andy, Ivan and Kirk. I will follow up with the SIS team to get you enrolled ASAP.

Thank you for your support in helping us to roll this out, and have a great weekend!

Best,
Patrick

Luce, Patrick W

From: Luce, Patrick W
Sent: Wednesday, July 14, 2021 5:27 PM
To: Rodriguez, Francisco C; Nish, Melinda A; Ryan M Cornner (CORNNERM@EMAIL.LACCD.EDU); Prieto, Jeffrey M; Gordon, Jeanette L; Gutierrez, Mercedes C; Smith, Rueben C; #-Presidents
Cc: Lidz, Carmen V
Subject: Memo regarding Mandatory Information Security Awareness for All Employees
Attachments: Memo_SecurityAwareness_2021_07_14.pdf

To all LACCD Executives and College Presidents,

Please refer to the attached memo regarding Mandatory Information Security Awareness for all employees.

With Best Regards,

Patrick Luce
Chief Information Security Officer
Information Technology

Los Angeles Community College District
770 Wilshire Boulevard, Los Angeles, CA 90017
Office: (213) 891-2121 | Mobile (213) 298-0488 | Fax: (213) 891-2304
lucepw@laccd.edu | www.laccd.edu

CITY / EAST / HARBOR / MISSION / PIERCE / SOUTHWEST / TRADE-TECH / VALLEY / WEST

Luce, Patrick W

From: Luce, Patrick W
Sent: Monday, June 14, 2021 4:30 PM
Subject: Mandatory Information Security Awareness Training for All Employees

Dear OIT Team,

The Office of Information Technology has developed a new foundational Information Security Awareness Course. It will be mandatory for all LACCD employees, and will be released soon.

In the meantime, we have provided the course to all OIT personnel now. You can access the course by navigating to https://ilearn.laccd.edu, clicking on “Courses”, then clicking on “Infosec Training Awareness 2021”. The course should take approximately 45 minutes.

Please complete the course no later than Friday, June 16, 2021. If you have any issues accessing the course, please email infosectraining@laccd.edu.

With Best Regards,

Patrick Luce
Chief Information Security Officer
Information Technology

Los Angeles Community College District
770 Wilshire Boulevard, Los Angeles, CA 90017
Office: (213) 891-2121 | Mobile (213) 298-0488 | Fax: (213) 891-2304
lucepw@laccd.edu | www.laccd.edu

CITY / EAST / HARBOR / MISSION / PIERCE / SOUTHWEST / TRADE-TECH / VALLEY / WEST

CITY
EAST
HARBOR
MISSION
PIERCE
SOUTHWEST
TRADE-TECH
VALLEY
WEST

TO: **All LACCD Executives**
All LACCD College Presidents

CC: **Carmen V. Lidz, Vice Chancellor and Chief Information Officer**

FROM: **Patrick Luce, Chief Information Security Officer**
DATE: **July 14, 2021**
SUBJECT: **Mandatory Information Security Awareness for All Employees**

The LACCD Board of Trustees has adopted Board Policy 3720, Computer and Network Use, to assure that all who access District computers and networks, use those resources responsibly.

The LACCD Office of Information Technology (OIT) has developed Information Security Awareness appropriate for all employees, and integrated it with our Canvas Learning Management System. By completing this forty-five-minute introduction, employees will gain understanding of current threats to the District's computing systems and information, and their role in helping to protect the District and our students, faculty and staff. Employees will also acknowledge that they have read, understand and agree to comply with Board Policy 3720 and the associated procedures outlined in Administrative Procedure 3720.

On August 4, 2021, all District employees, including full-time and adjunct faculty, staff and student-workers that had/have an active employee assignment for spring or summer of 2021 will be sent an introductory email with guidance for accessing the content. Please inform all your staff that participation is mandatory and request that they complete it prior to October 15, 2021.

Should you or any members of your staff have any questions regarding information security awareness, please email infosecrequests@laccd.edu.

Luce, Patrick W

From: Luce, Patrick W
Sent: Monday, July 19, 2021 11:51 AM
Cc: George McCalmon (MCCALMG@EMAIL.LACCD.EDU)
Subject: Mandatory Security Awareness for OIT Personnel PAST DUE

Dear OIT Team Members,

On June 14th, I sent a memo to all OIT personnel to complete mandatory Security Awareness by Friday, June 16. Our records show that you have not yet completed the content. Please access the content by navigating to https://ilearn.laccd.edu, clicking on "Courses", then clicking on "Infosec Training Awareness 2021". The content should take approximately 45 minutes to complete.

If you have any issues accessing the content, please email infosecrequests@laccd.edu.

Patrick Luce
Chief Information Security Officer
Information Technology

Los Angeles Community College District
770 Wilshire Boulevard, Los Angeles, CA 90017
Office: (213) 891-2121 | Mobile (213) 298-0488 | Fax: (213) 891-2304
lucepw@laccd.edu | www.laccd.edu

CITY / EAST / HARBOR / MISSION / PIERCE / SOUTHWEST / TRADE-TECH / VALLEY / WEST

CITY
EAST
HARBOR
MISSION
PIERCE
SOUTHWEST
TRADE-TECH
VALLEY
WEST

TO: **All LACCD Executives**
All LACCD College Presidents

CC: **Carmen V. Lidz, Vice Chancellor and Chief Information Officer**

FROM: **Patrick Luce, Chief Information Security Officer**
DATE: **July 14, 2021**
SUBJECT: **Mandatory Information Security Awareness for All Employees**

The LACCD Board of Trustees has adopted Board Policy 3720, Computer and Network Use, to assure that all who access District computers and networks, use those resources responsibly.

The LACCD Office of Information Technology (OIT) has developed Information Security Awareness appropriate for all employees, and integrated it with our Canvas Learning Management System. By completing this forty-five-minute introduction, employees will gain understanding of current threats to the District's computing systems and information, and their role in helping to protect the District and our students, faculty and staff. Employees will also acknowledge that they have read, understand and agree to comply with Board Policy 3720 and the associated procedures outlined in Administrative Procedure 3720.

On August 4, 2021, all District employees, including full-time and adjunct faculty, staff and student-workers that had/have an active employee assignment for spring or summer of 2021 will be sent an introductory email with guidance for accessing the content. Please inform all your staff that participation is mandatory and request that they complete it prior to October 15, 2021.

Should you or any members of your staff have any questions regarding information security awareness, please email infosecrequests@laccd.edu.

Luce, Patrick W

From: Luce, Patrick W
Sent: Wednesday, July 28, 2021 3:22 PM
To: Rodriguez, Francisco C; Nish, Melinda A; Ryan M Cornner (CORNNERM@EMAIL.LACCD.EDU); Prieto, Jeffrey M; Gordon, Jeanette L; Gutierrez, Mercedes C; Smith, Rueben C; #-Presidents
Cc: Lidz, Carmen V
Subject: RE: Memo regarding Mandatory Information Security Awareness for All Employees
Attachments: Memo_SecurityAwareness_2021_07_14.pdf

Dear LACCD Executives and College Presidents,

This is a reminder that we are providing mandatory information security awareness for all active employees beginning next week. They will receive an introduction email with instructions on Wednesday, August 4. Thank you for supporting this important effort to protect our information resources, and please let me know of any questions you may have.

With Best Regards,

Patrick Luce
Chief Information Security Officer
Information Technology

Los Angeles Community College District
770 Wilshire Boulevard, Los Angeles, CA 90017
Office: (213) 891-2121 | Mobile (213) 298-0488 | Fax: (213) 891-2304
lucepw@laccd.edu | www.laccd.edu

CITY / EAST / HARBOR / MISSION / PIERCE / SOUTHWEST / TRADE-TECH / VALLEY / WEST

From: Luce, Patrick W
Sent: Wednesday, July 14, 2021 5:27 PM
To: Rodriguez, Francisco C <RODRIGFC@EMAIL.LACCD.EDU>; Nish, Melinda A <NISHMA@EMAIL.LACCD.EDU>; Ryan M Cornner (CORNNERM@EMAIL.LACCD.EDU) <CORNNERM@EMAIL.LACCD.EDU>; Prieto, Jeffrey M <PRIETOJM@EMAIL.LACCD.EDU>; Gordon, Jeanette L <gordonjl@laccd.edu>; Gutierrez, Mercedes C <GUTIERMC4@EMAIL.LACCD.EDU>; Smith, Rueben C <SMITHRC@EMAIL.LACCD.EDU>; #-Presidents <#-Presidents@email.laccd.edu>
Cc: Lidz, Carmen V <carmen@laccd.edu>
Subject: Memo regarding Mandatory Information Security Awareness for All Employees

To all LACCD Executives and College Presidents,

Please refer to the attached memo regarding Mandatory Information Security Awareness for all employees.

With Best Regards,

Patrick Luce
Chief Information Security Officer
Information Technology

Los Angeles Community College District
770 Wilshire Boulevard, Los Angeles, CA 90017
Office: (213) 891-2121 | Mobile (213) 298-0488 | Fax: (213) 891-2304
lucepw@laccd.edu | www.laccd.edu

CITY / EAST / HARBOR / MISSION / PIERCE / SOUTHWEST / TRADE-TECH / VALLEY / WEST

Luce, Patrick W

From: Luce, Patrick W
Sent: Wednesday, August 4, 2021 2:37 PM
Subject: Mandatory Information Security Awareness for All Employees

Dear LACCD Employees,

LACCD has adopted Board Policy 3720, Computer and Network Use, and associated procedures to assure that all who access District information systems use those resources responsibly.

The District is providing mandatory information security awareness for all employees to help you understand your role in protecting the District's information resources, and to acknowledge your agreement to comply with the District's Administrative Procedure 3720, Computer and Network Use.

To access this important information, navigate to https://ilearn.laccd.edu, click on "Courses", and then click on "Information Security Awareness 2021." You will review a series of videos that contain important security guidance, and review District policy and procedures.

We urge you to complete information security awareness by October 15, 2021. If you have any questions or have difficulty accessing the material, please email infosec@laccd.edu.

With Best Regards,

Patrick Luce
Chief Information Security Officer
Information Technology

Los Angeles Community College District
770 Wilshire Boulevard, Los Angeles, CA 90017
Office: (213) 891-2121 | Mobile (213) 298-0488 | Fax: (213) 891-2304
lucepw@laccd.edu | www.laccd.edu

CITY / EAST / HARBOR / MISSION / PIERCE / SOUTHWEST / TRADE-TECH / VALLEY / WEST

Luce, Patrick W

From: Luce, Patrick W
Sent: Friday, September 24, 2021 4:24 PM
Subject: Mandatory Information Security Awareness for All Employees

Dear LACCD Employees,

LACCD has adopted Board Policy 3720, Computer and Network Use, and associated procedures to assure that all who access District information systems use those resources responsibly.

The District is providing mandatory information security awareness for all employees to help you understand your role in protecting the District's information resources, and to acknowledge your agreement to comply with the District's Administrative Procedure 3720, Computer and Network Use.

To access this important information, navigate to https://ilearn.laccd.edu, click on "Courses", and then click on "Information Security Awareness 2021." You will review a series of videos that contain important security guidance, and review District policy and procedures.

We urge you to complete information security awareness by October 15, 2021. If you have any questions or have difficulty accessing the material, please email infosec@laccd.edu.

With Best Regards,

Patrick Luce
Chief Information Security Officer
Information Technology

Los Angeles Community College District
770 Wilshire Boulevard, Los Angeles, CA 90017
Office: (213) 891-2121 | Mobile (213) 298-0488 | Fax: (213) 891-2304
lucepw@laccd.edu | www.laccd.edu

CITY / EAST / HARBOR / MISSION / PIERCE / SOUTHWEST / TRADE-TECH / VALLEY / WEST

Luce, Patrick W

From: Luce, Patrick W
Sent: Friday, September 24, 2021 7:56 PM
Subject: Mandatory Information Security Awareness for All Employees - REMINDER

Dear LACCD Employees,

LACCD has adopted Board Policy 3720, Computer and Network Use, and associated procedures to assure that all who access District information systems use those resources responsibly.

The District is providing mandatory information security awareness for all employees to help you understand your role in protecting the District's information resources, and to acknowledge your agreement to comply with the District's Administrative Procedure 3720, Computer and Network Use. Our records show that you have not yet completed the District's information security awareness and/or acknowledged your agreement to comply with AP 3720.

To access this important information, navigate to https://ilearn.laccd.edu, click on "Courses", and then click on "Information Security Awareness 2021." You will review a series of videos that contain important security guidance, and review District policy and procedures.

We urge you to complete information security awareness by October 15, 2021. If you have any questions or have difficulty accessing the material, please email infosec@laccd.edu.

With Best Regards,

Patrick Luce
Chief Information Security Officer
Information Technology

Los Angeles Community College District
770 Wilshire Boulevard, Los Angeles, CA 90017
Office: (213) 891-2121 | Mobile (213) 298-0488 | Fax: (213) 891-2304
lucepw@laccd.edu | www.laccd.edu

CITY / EAST / HARBOR / MISSION / PIERCE / SOUTHWEST / TRADE-TECH / VALLEY / WEST

Patrick Luce
Chief Information Security Officer
Information Technology

Los Angeles Community College District
770 Wilshire Boulevard, Los Angeles, CA 90017
Office: (213) 891-2121 | Mobile (213) 298-0488 | Fax: (213) 891-2304
lucepw@laccd.edu | www.laccd.edu

CITY / EAST / HARBOR / MISSION / PIERCE / SOUTHWEST / TRADE-TECH / VALLEY / WEST

Luce, Patrick W

From: Luce, Patrick W
Sent: Friday, October 22, 2021 2:48 PM
Subject: October is Cybersecurity Awareness Month!
Attachments: LACCD CyberSecurity Awareness Month.pdf

Dear Colleagues,

October is National Cybersecurity Awareness Month! Please review the attached flyer to help assure we all stay Alert, Informed, and CyberSmart!

Whenever in doubt, please reach out to our Information Security Team at infosec@laccd.edu with any questions or concerns you may have about Cybersecurity.

Thank you for all you do to help protect our information resources.

With Best Regards,

Patrick Luce
Chief Information Security Officer
Information Technology

Los Angeles Community College District
770 Wilshire Boulevard, Los Angeles, CA 90017
Office: (213) 891-2121 | Mobile (213) 298-0488 | Fax: (213) 891-2304
lucepw@laccd.edu | www.laccd.edu

CITY / EAST / HARBOR / MISSION / PIERCE / SOUTHWEST / TRADE-TECH / VALLEY / WEST

Los Angeles Community College District

CITY / EAST / HARBOR / MISSION / PIERCE / SOUTHWEST / TRADE-TECHNICAL / VALLEY / WEST

October, 2021 is

National Cybersecurity Awareness Month

Do Your Part; Be CyberSmart

Every day, technology helps us use information provide educational services to our community. However, the same technology has also created a marketplace for hackers to seek and steal sensitive information. The LACCD Office of Information Technology encourages all LACCD employees to help secure our information by keeping aware of threats to the security of information, and our shared role in keeping data safe.

Be Alert

Phishing attacks use malicious images or links in websites and emails to infect your computer or lure you to provide your login credentials to sensitive data. For tips on recognizing phishing, visit NCSAM Phishing.

BE INFORMED!

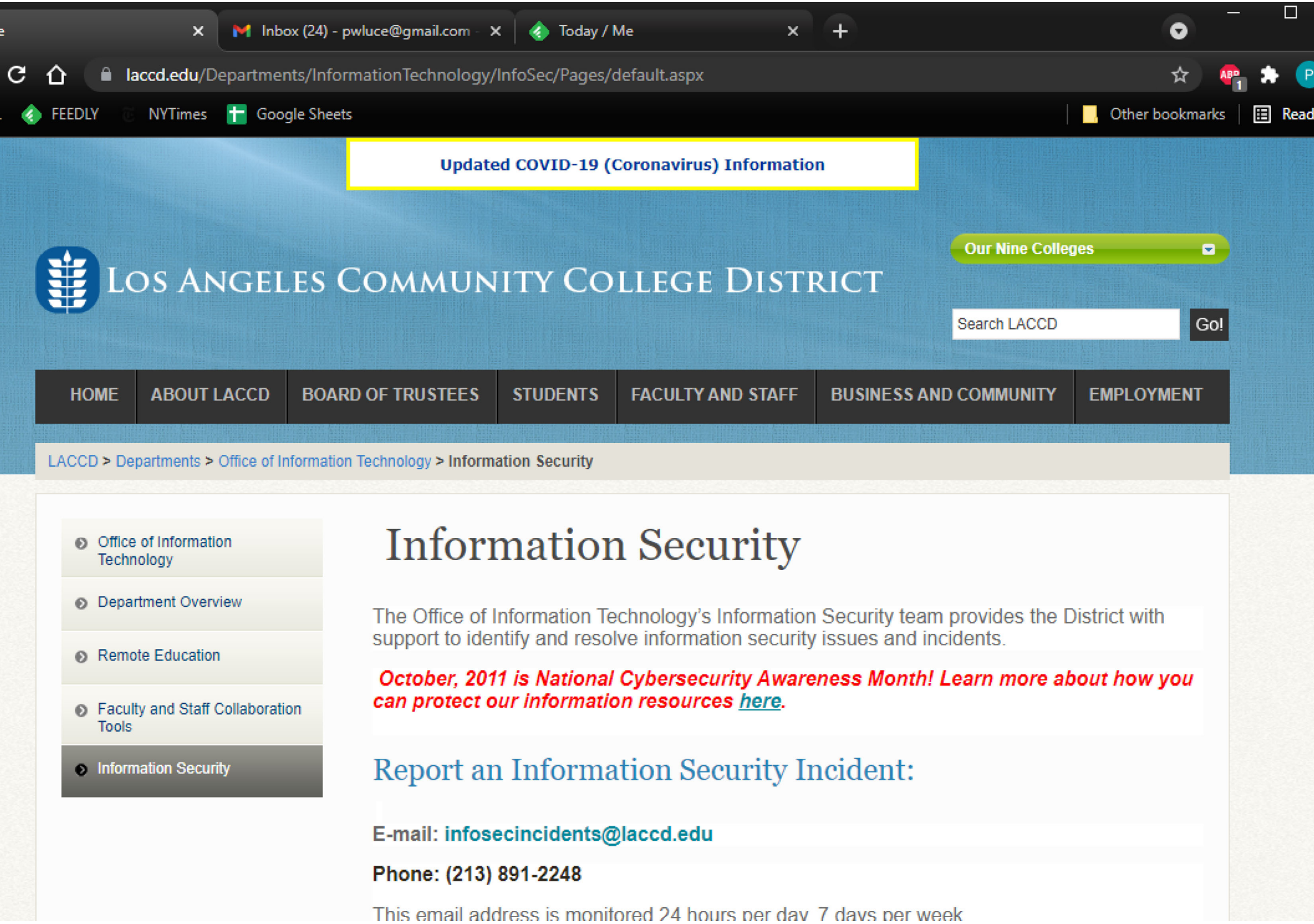
LACCD provides mandatory information security awareness information for all LACCD employees. If you haven't already completed it, go to ilearn.laccd.edu and click "Information Security Awareness 2021" to start.

Let Us Help

The LACCD Information Security Team is available to assist with any questions you may have about how to keep our computers and information safe. Contact us at infosec@laccd.edu.

CYBERSECURITY AWARENESS MONTH

Need Cybersecurity Assistance? Email: infosec@laccd.edu


Inbox (24) - pwluce@gmail.com
Today / Me
laccd.edu/Departments/InformationTechnology/InfoSec/Pages/default.aspx
FEEDLY
NYTimes
Google Sheets
Other bookmarks
Updated COVID-19 (Coronavirus) Information
Los Angeles Community College District
Our Nine Colleges
Search LACCD
Go!
HOME
ABOUT LACCD
BOARD OF TRUSTEES
STUDENTS
FACULTY AND STAFF
BUSINESS AND COMMUNITY
EMPLOYMENT
LACCD > Departments > Office of Information Technology > Information Security
Office of Information Technology
Department Overview
Remote Education
Faculty and Staff Collaboration Tools
Information Security
Information Security
The Office of Information Technology's Information Security team provides the District with support to identify and resolve information security issues and incidents.
October, 2011 is National Cybersecurity Awareness Month! Learn more about how you can protect our information resources here.
Report an Information Security Incident:
E-mail: infosecincidents@laccd.edu
Phone: (213) 891-2248
This email address is monitored 24 hours per day, 7 days per week