cbmi
COLLEGE BUSINESS MANAGEMENT INSTITUTE

Jason Wheat

Cybersecurity in Higher Education

Key Issues, Controls, and Partners

SACUBO
SOUTHERN ASSOCIATION OF COLLEGE AND UNIVERSITY BUSINESS OFFICERS

UK Auxiliary Services

Who am I?

Jason Wheat, MBA, MSCPM

Manager, Security Operations

University of Kentucky

Agenda

- Introductions
- Overview
- Key Issues
- Key Controls
- Key Partners

Bonus: Personal Cybersecurity

cbmi
COLLEGE BUSINESS MANAGEMENT INSTITUTE

What is Cybersecurity?

Protecting networks, devices, and data from unauthorized access while ensuring confidentiality, integrity, and availability.

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY

Source: https://www.cisa.gov/news-events/news/what-cybersecurity

cbmi
COLLEGE BUSINESS MANAGEMENT INSTITUTE

What is Cybersecurity?

- Protecting networks, devices, and data from unauthorized access while ensuring confidentiality, integrity, and availability.
- **Confidentiality**: Keeping data private and access-controlled
- **Integrity**: Ensuring data is accurate and untampered
- **Availability**: Systems function when and as expected

Source: https://www.cisa.gov/news-events/news/what-cybersecurity

cbmi
COLLEGE BUSINESS MANAGEMENT INSTITUTE

cbmi
COLLEGE BUSINESS MANAGEMENT INSTITUTE

Why are we here?

Auxiliary Services

SACUBO
SOUTHERN ASSOCIATION OF COLLEGE AND UNIVERSITY BUSINESS OFFICERS

What do you think keeps the Cybersecurity Team up at night (i.e., what are the cybersecurity threats to universities)?

What are the common organizational impacts of a cybersecurity event?

What was the average cost of a data breach in 2025?

Key issues

- **Ransomware**: Malware that encrypts data or threatens exposure until a ransom is paid
- **Phishing**: Social engineering that tricks users into revealing credentials or installing malware
- **Vendor Risk Management**: Monitoring and managing security risks from third-party relationships

cbmi
COLLEGE BUSINESS MANAGEMENT INSTITUTE

cbmi
COLLEGE BUSINESS MANAGEMENT INSTITUTE

Real World Examples

Auxiliary Services

SACUBO
SOUTHERN ASSOCIATION OF COLLEGE AND UNIVERSITY BUSINESS OFFICERS

Real World Examples

- Phishing is the primary cyber-attack vector worldwide
- Social engineering targets users for personal info and credentials
- Attacks typically start with deceptive emails

cbmi
COLLEGE BUSINESS MANAGEMENT INSTITUTE

Real World Examples

- Attacks target users, not technology
- Common lures: account deactivation threats and credential-harvesting forms
- Out-of-band attacks (phone/text) limit institutional visibility

cbmi
COLLEGE BUSINESS MANAGEMENT INSTITUTE

Direct Deposit Theft

12 Minutes

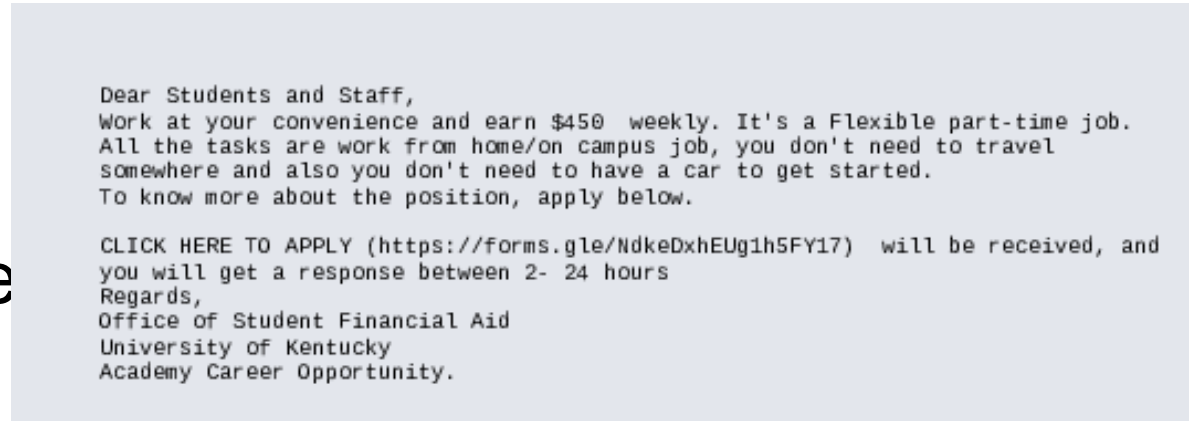
- Scouts public sites for high-earning employees
- Social engineers user or help desk to reset credentials and MFA
- Enrolls a new MFA device on the compromised account
- Changes direct deposit to attacker-controlled account
- Deletes the confirmation email from the inbox
- Paycheck deposited to the attacker on payday

Phishing — Abusing Trust

- **Trusted vendor relationship** — routine communications lower guard
- **Attacker compromises the vendor's email account**
- **Weaponized trust** — real address, familiar invoice, no red flags
- **Device code phishing** grants attacker full cloud access via OAuth token

Google Form Phishing

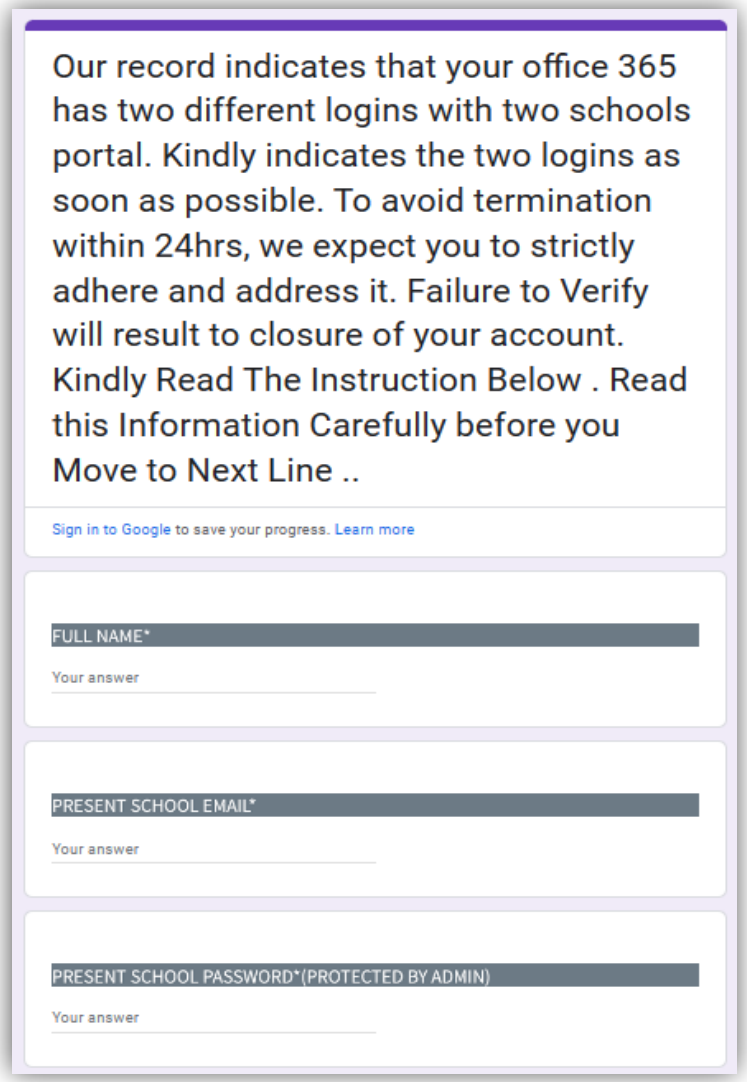
- Successive phishing waves using compromised internal accounts
- Lures claim job offers or account deactivation
- Victims directed to Google Forms requesting credentials and personal info

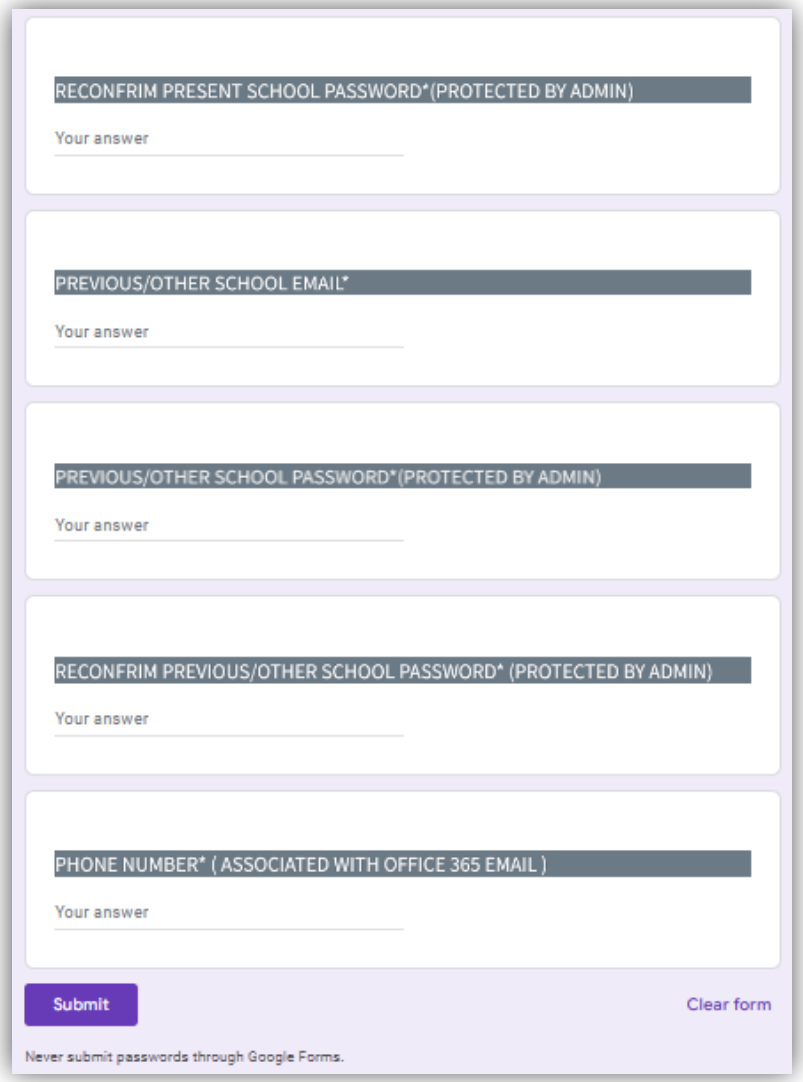


Dear Students and Staff,
Work at your convenience and earn $450 weekly. It's a Flexible part-time job.
All the tasks are work from home/on campus job, you don't need to travel somewhere and also you don't need to have a car to get started.
To know more about the position, apply below.

CLICK HERE TO APPLY (https://forms.gle/NdkeDxhEUg1h5FY17) will be received, and you will get a response between 2- 24 hours
Regards,
Office of Student Financial Aid
University of Kentucky
Academy Career Opportunity.

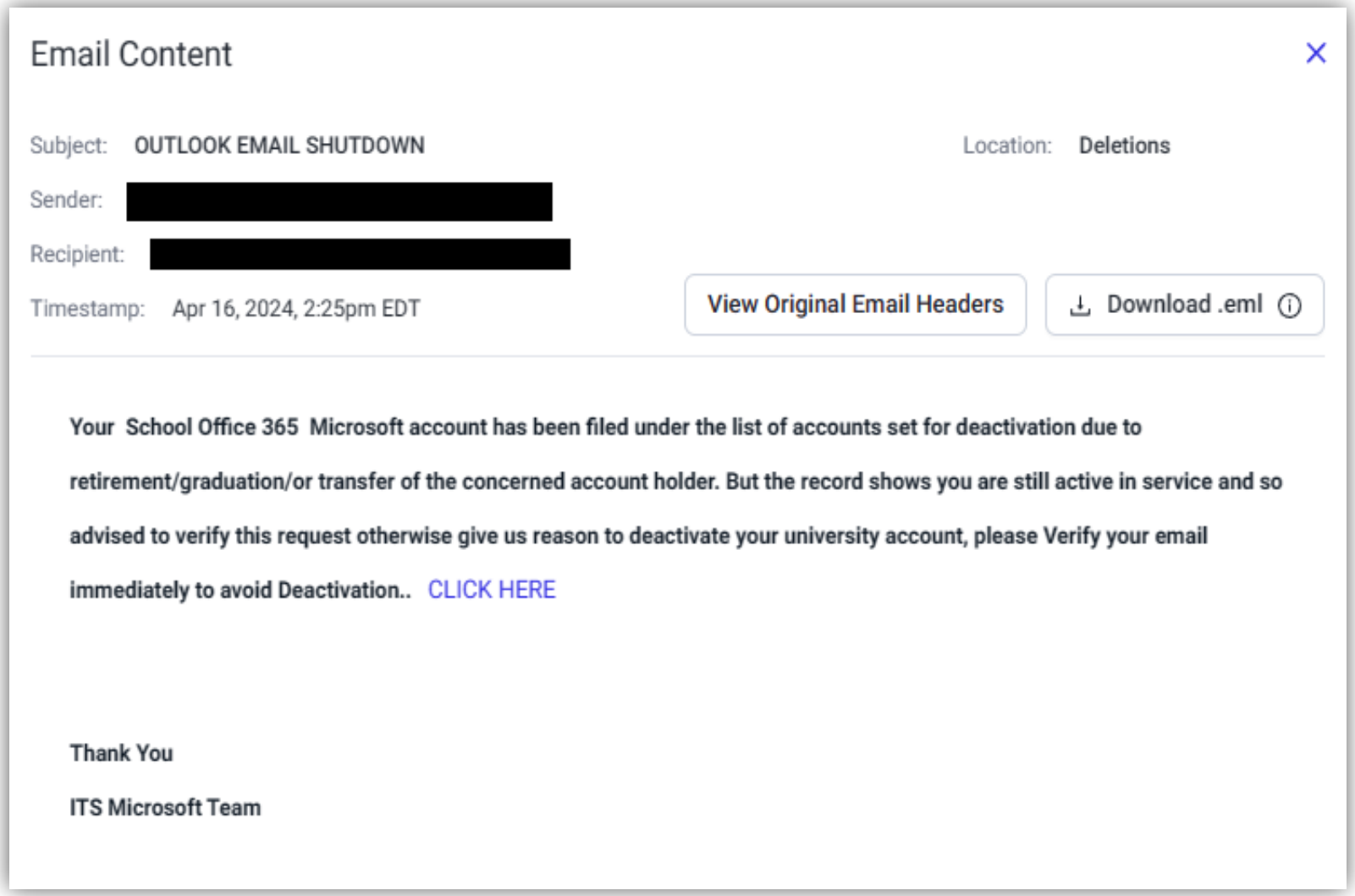
Form Collection





cbmi
COLLEGE BUSINESS MANAGEMENT INSTITUTE

Phishing



Email Content

Subject: OUTLOOK EMAIL SHUTDOWN

Location: Deletions

Sender: [redacted]

Recipient: [redacted]

Timestamp: Apr 16, 2024, 2:25pm EDT

View Original Email Headers

Download .eml

Your School Office 365 Microsoft account has been filed under the list of accounts set for deactivation due to retirement/graduation/or transfer of the concerned account holder. But the record shows you are still active in service and so advised to verify this request otherwise give us reason to deactivate your university account, please Verify your email immediately to avoid Deactivation.. CLICK HERE

Thank You

ITS Microsoft Team

cbmi

COLLEGE BUSINESS MANAGEMENT INSTITUTE

Another Example

Subject: EMAIL ACCOUNT SHUTDOWN NOTICE Location: Junk Email

Sender: [redacted]

Recipient: [redacted]

Reply-to: [redacted]

To: [redacted]

Timestamp: Apr 23, 2024, 2:18pm EDT View Original Email Headers Download .eml

You don't often get email from jayla.atkinson@uky.edu. Learn why this is important

Your Office 365 Email Microsoft account has been filed under the list of accounts set for deactivation due to retirement/graduation/or transfer of the concerned account holder. But the record shows you are still active in service and so advised to verify this request otherwise give us reason to deactivate your university account, please Verify your email immediately to avoid Deactivation...

PLEASE COPY AND PASTE THE LINK TO YOUR ADDRESS BAR OR TO YOUR BROSWER TO VERIFY YOUR ACCOUNT AND STOP THE SHUTDOWN PROCESS.. (tinyurl.com/5t4c467f)

tinyurl.com/5t4c467f

THANKS

ADMIN

Our record indicates that your office 365 has two different logins with two schools portal. Kindly indicates the two logins as soon as possible. To avoid termination within 24hrs, we expect you to strictly adhere and address it. Failure to Verify will result to closure of your account. Kindly Read The Instruction Below . Read this Information Carefully before you Move to Next Line...

FULL NAME*

PRESENT SCHOOL EMAIL*

PRESENT SCHOOL PASSWORD*(PROTECTED BY ADMIN)

RECONFRIM PRESENT SCHOOL PASSWORD*(PROTECTED BY ADMIN)

PREVIOUS/OTHER SCHOOL EMAIL*

PREVIOUS/OTHER SCHOOL PASSWORD*(PROTECTED BY ADMIN)

RECONFRIM PREVIOUS/OTHER SCHOOL PASSWORD* (PROTECTED BY ADMIN)

PHONE NUMBER (ASSOCIATED WITH OFFICE 365 EMAIL)

PERSONAL PHONE NUMBER*

Submit

Never submit passwords through QuestionScout forms!

cbmi

COLLEGE BUSINESS MANAGEMENT INSTITUTE

User Engagement

THIS IS LEGITIMATE,YOU NEED TO FILL THE FORM TO KEEP YOUR ACCOUNT ACTIVE AND SECURED

From: [redacted]
Sent: Thursday, April 18, 2024 8:08 PM
To: [redacted]
Subject: Re: OFFICE EMAIL SHUTDOWN
I need some sort of verification that this is legit. I do not want to do something and risk my accounts. Someone that is supposed to be on a professional level should not be using all caps in emails. They should also be a little more professional in how they ask things. Greetings, endings, things like that. If I do not get some verification that this is legit I am reporting this email.
[redacted]

From: [redacted]
Sent: Thursday, April 18, 2024 10:07:08 PM
To: [redacted]
Subject: Re: OFFICE EMAIL SHUTDOWN
YES FILL THE FORM TO KEEP YOUR ACCOUNT ACTIVE AND SECURED

From: [redacted]
Sent: Thursday, April 18, 2024 8:05 PM
To: [redacted]
Subject: Re: OFFICE EMAIL SHUTDOWN
The verification is asking for passwords to my accounts. At the end of the survey it says not to share passwords on it. I am cautious and confused on why I am having to do this well over a year into both my job and school career.
[redacted]

From: [redacted]
Sent: Thursday, April 18, 2024 10:04:35 PM
To: [redacted]
Subject: Re: OFFICE EMAIL SHUTDOWN
FILL THE VERIFICATION FORM TO KEEP YOUR ACCOUNT ACTIVE AND SECURED

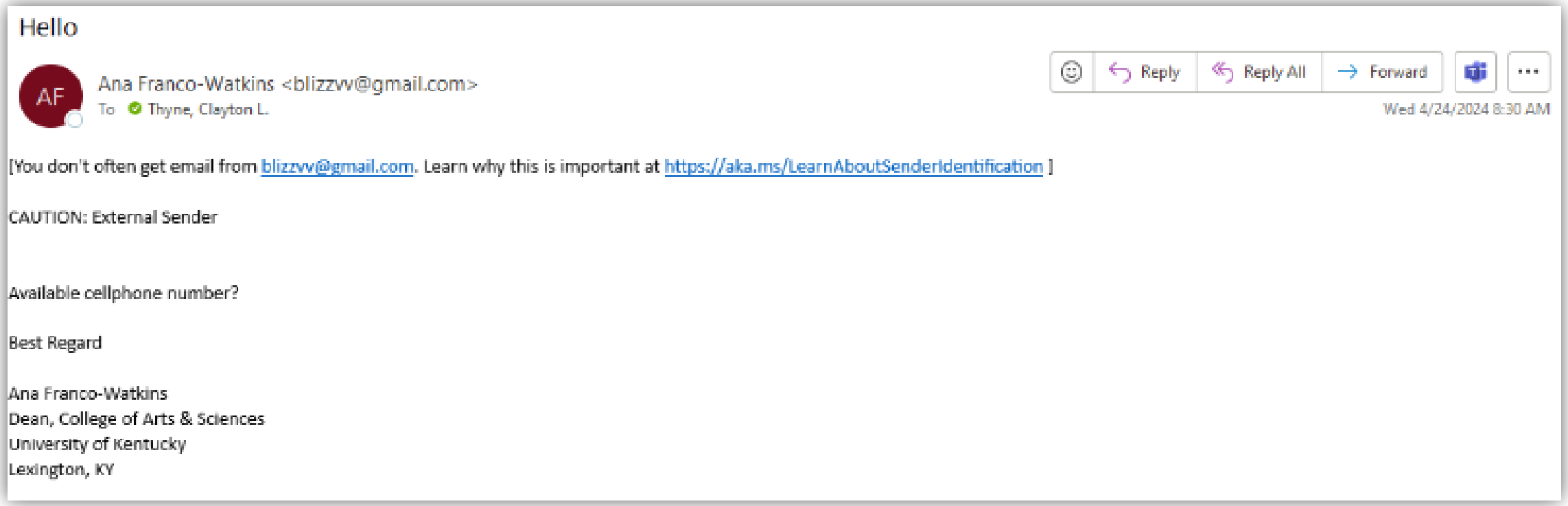
From: [redacted]
Sent: Thursday, April 18, 2024 8:03 PM
To: [redacted]
Subject: Re: OFFICE EMAIL SHUTDOWN
I have two emails through school portals. I have my student email, through UK and I have my work email, that has a school email ending. I work at Campbellsville University. Both accounts are needed. I am no where near graduation so I would like to understand why my account is being deactivated.
[redacted]

From: [redacted]
Sent: Thursday, April 18, 2024 10:00:29 PM
Subject: OFFICE EMAIL SHUTDOWN
Your Office 365 Email Microsoft account has been filed under the list of accounts set for deactivation due to retirement/graduation/or transfer of the concerned account holder. But the record shows you are still active in service and so advised to verify this request otherwise give us reason to deactivate your university account, please Verify your email immediately to avoid Deactivation VERIFY HERE

Thank You
ITS Microsoft Team

cbmi
COLLEGE BUSINESS MANAGEMENT INSTITUTE

Out of Band Communication



Hello

AF

Ana Franco-Watkins <blizzvv@gmail.com>

To Thyne, Clayton L.

Reply | Reply All | Forward

Wed 4/24/2024 8:30 AM

[You don't often get email from blizzvv@gmail.com. Learn why this is important at https://aka.ms/LearnAboutSenderIdentification]

CAUTION: External Sender

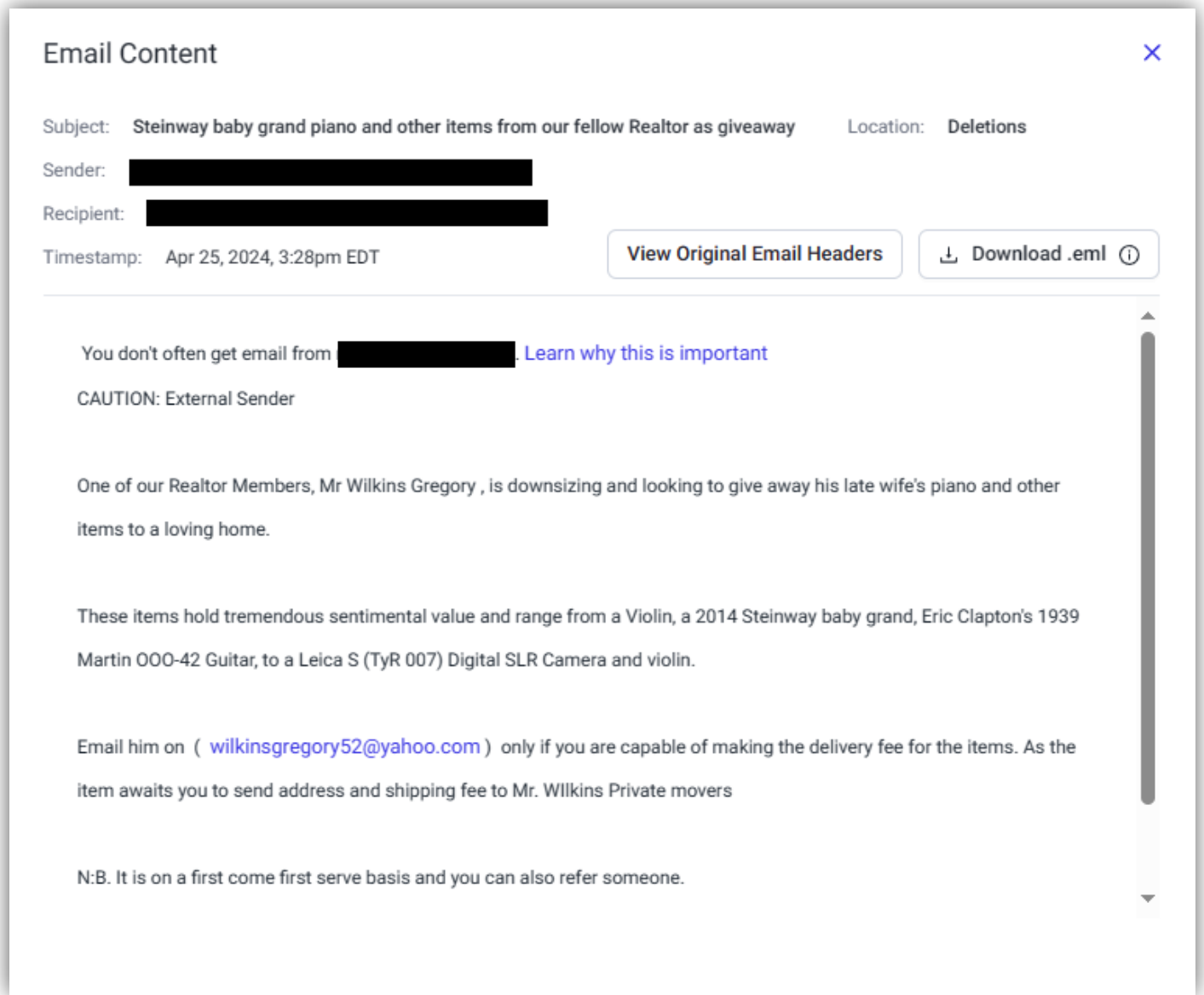
Available cellphone number?

Best Regard

Ana Franco-Watkins
Dean, College of Arts & Sciences
University of Kentucky
Lexington, KY

cbmi
COLLEGE BUSINESS MANAGEMENT INSTITUTE

Out of Band Communication



Email Content

Subject: **Steinway baby grand piano and other items from our fellow Realtor as giveaway** Location: **Deletions**

Sender: [redacted]

Recipient: [redacted]

Timestamp: Apr 25, 2024, 3:28pm EDT

View Original Email Headers | Download .eml

You don't often get email from [redacted]. Learn why this is important

CAUTION: External Sender

One of our Realtor Members, Mr Wilkins Gregory , is downsizing and looking to give away his late wife's piano and other items to a loving home.

These items hold tremendous sentimental value and range from a Violin, a 2014 Steinway baby grand, Eric Clapton's 1939 Martin OOO-42 Guitar, to a Leica S (TyR 007) Digital SLR Camera and violin.

Email him on (wilkinsgregory52@yahoo.com) only if you are capable of making the delivery fee for the items. As the item awaits you to send address and shipping fee to Mr. WIlkins Private movers

N:B. It is on a first come first serve basis and you can also refer someone.

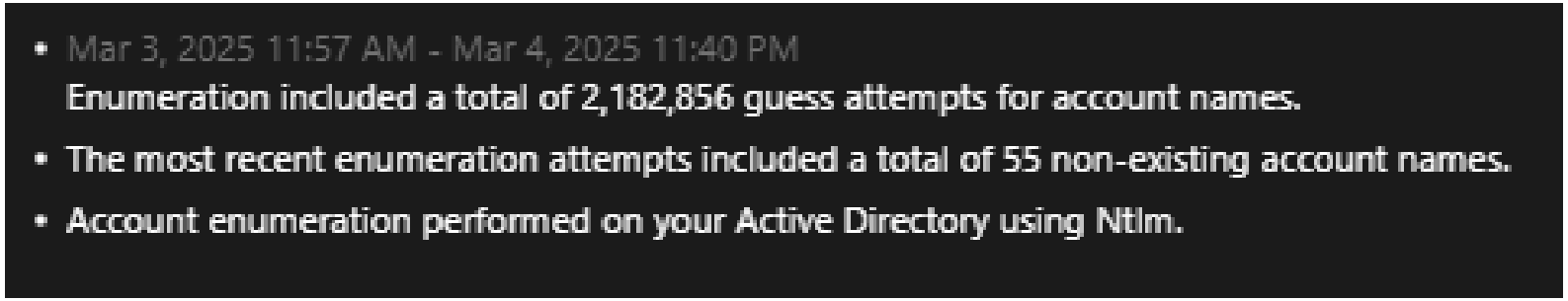
cbmi
COLLEGE BUSINESS MANAGEMENT INSTITUTE

Drive-by Malware Downloads

- Triggered by visiting low-reputation sites, suspicious links, or email attachments
- Users unknowingly download bundled malicious payloads alongside legitimate software
- Malware executes silently on the device

Brute-Force Attacks & Account Enumeration

- Attackers scan for internet-facing devices and enumerate valid accounts
- Automated tools test millions of usernames to identify real accounts
- Discovered accounts are targeted with brute-force credential attacks



cbmi
COLLEGE BUSINESS MANAGEMENT INSTITUTE

Discussion: *What common social engineering prompts have you observed at your institutions? How can you protect against them?*

Auxiliary Services

SACUBO
SOUTHERN ASSOCIATION OF COLLEGE AND UNIVERSITY BUSINESS OFFICERS

Key Controls

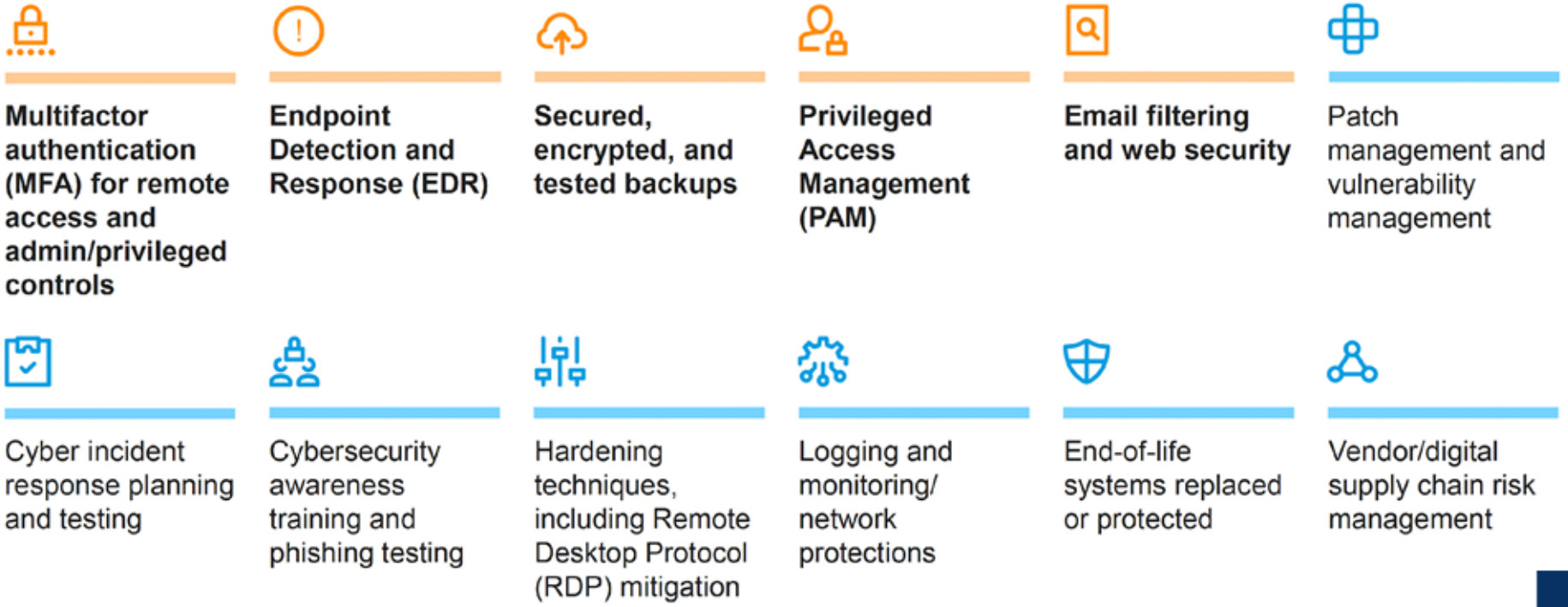
Control types

- Technical controls
- Process and procedure
- Awareness training
- Cybersecurity insurance

cbmi
COLLEGE BUSINESS MANAGEMENT INSTITUTE

Key Controls

Top cybersecurity controls are the key to risk mitigation, resilience, and insurability

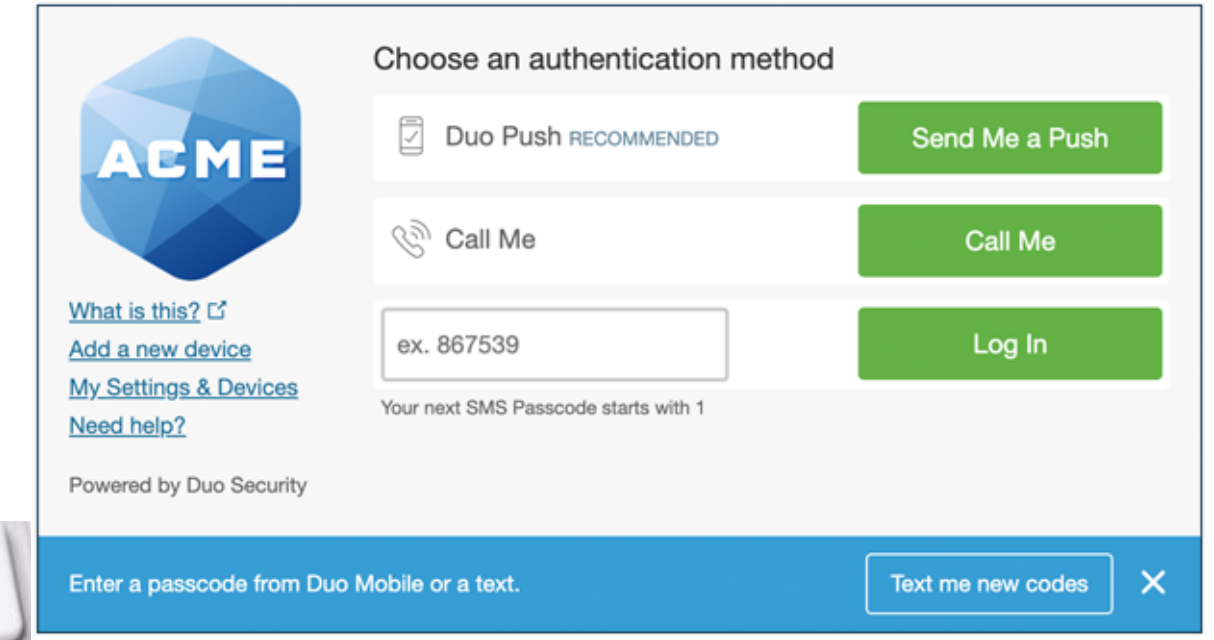


Source: https://www.marsh.com/kz/en/services/cyber-risk/insights/cyber-resilience-twelve-key-controls-to-strengthen-your-security.html

cbmi
COLLEGE BUSINESS MANAGEMENT INSTITUTE

Multifactor Authentication

Priority: ***remote access***, ***admin/privileged accounts***, *and* ***identity management systems***



Source: https://guide.duo.com/tokens

cbmi
COLLEGE BUSINESS MANAGEMENT INSTITUTE

Email & Web Security

- Email filtering
  - Phishing attacks
  - Vendor impersonations
  - Social Engineering
- Link rewriting
- DMARC
  - Domain-based Message Authentication, Reporting & Conformance
  - https://dmarc.org

I need your urgent assistance…
Please text me…

COLLEGE BUSINESS MANAGEMENT INSTITUTE

Backups

- Secure
- Encrypted
- Tested

cbmi
COLLEGE BUSINESS MANAGEMENT INSTITUTE

Privileged Access Management

How do we keep attackers from breaking into mission critical systems?

- Secure login to systems
- Just-in-time access
- Password rotation

cbmi
COLLEGE BUSINESS MANAGEMENT INSTITUTE

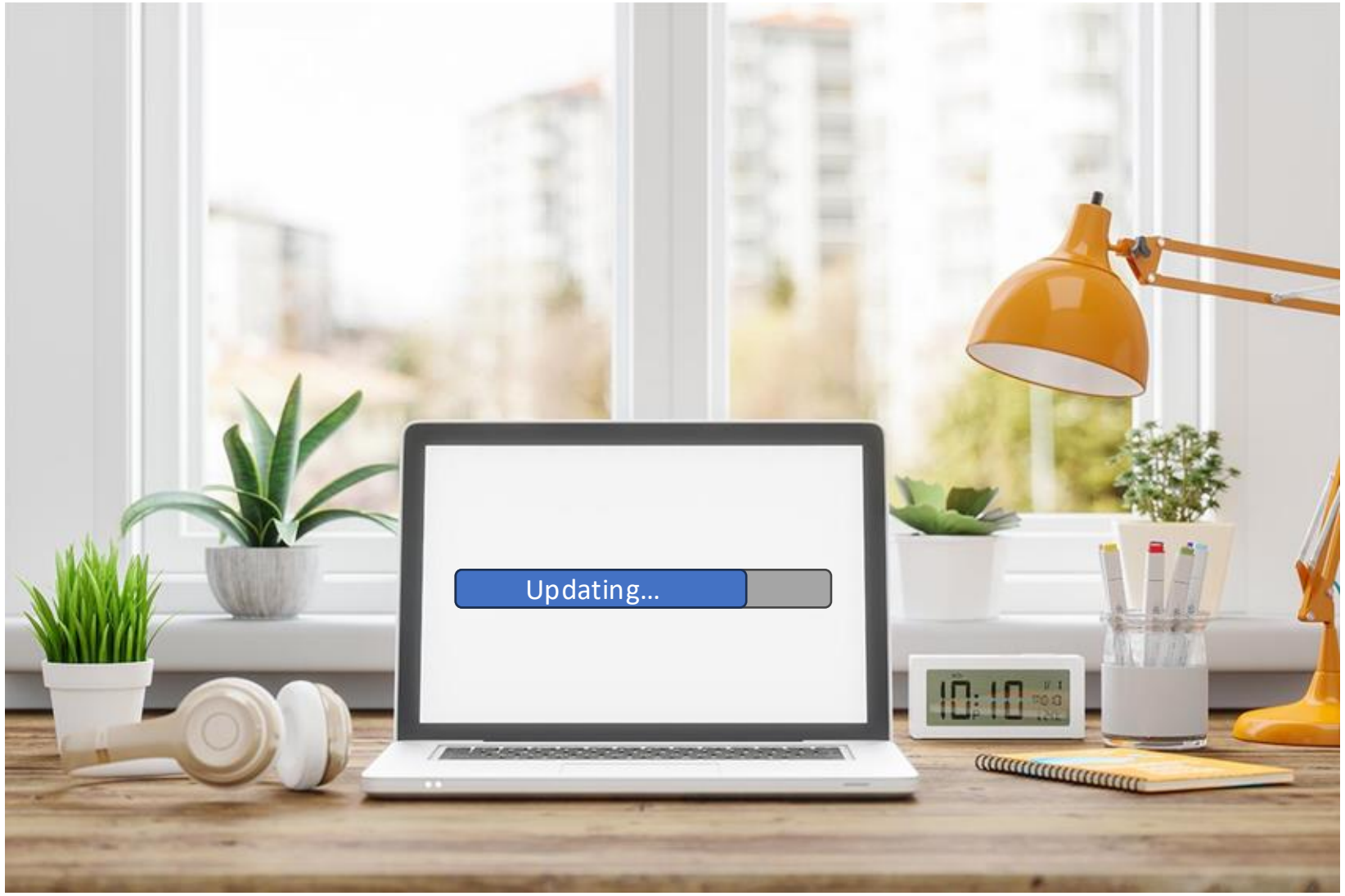
Endpoint Protection

Endpoint detection and response (EDR)

- Virus protection
- Ransomware protection
- Investigations

cbmi
COLLEGE BUSINESS MANAGEMENT INSTITUTE

Patch & Vulnerability Management



- Hardware
- Software
- Devices

cbmi
COLLEGE BUSINESS MANAGEMENT INSTITUTE

Incident Response

Incident Response Plan: Predefined procedures to detect, respond to, and contain cyber attacks

Disaster Recovery Plan: Steps to restore critical systems after major failures or destruction

Business Continuity Plan: How the organization sustains operations during and after disruption

Source: https://csrc.nist.gov/glossary

Cybersecurity Awareness

- Training
  - In-person
  - Virtual
- Phishing simulations
- Newsletters

cbmi
COLLEGE BUSINESS MANAGEMENT INSTITUTE

Remote Access

Remote Access: Users connecting through external, non-institutional networks

- **VPN**: Encrypted tunnel providing secure remote connectivity
- **Multifactor**: Requires multiple authentication factors for access

Source: https://csrc.nist.gov/glossary

Logging & Monitoring

- Log aggregation
- Monitoring
- Search
- Visualization

Source: https://www.splunk.com/en_us/home-page.html

cbmi
COLLEGE BUSINESS MANAGEMENT INSTITUTE

Unsupported Devices

- Hardware
- Software
- Devices

If you can't update it, you can't protect it

cbmi
COLLEGE BUSINESS MANAGEMENT INSTITUTE

Vendor & Supply Chain Risks

How do you protect your institution from third parties?

- Vendor risk assessments
- Higher Education Community Vendor Assessment Toolkit (HECVAT)
- Cybersecurity insurance

Recent examples:

CHANGE HEALTHCARE

National Student Clearinghouse

TIAA

cbmi COLLEGE BUSINESS MANAGEMENT INSTITUTE

Key Partners

- EDUCAUSE Cybersecurity Library — central resource for higher ed cybersecurity
- REN-ISAC
  - Threat sharing and peer assessments for research and education networks
  - Peer assessments
- CISA
  - Federal alerts, training, and vulnerability scanning services
- Peer Institutions — collaborative security through institutional partnerships

cbmi
COLLEGE BUSINESS MANAGEMENT INSTITUTE

Bonus: Personal Cybersecurity

1. Enable multifactor authentication everywhere
2. Never reuse passwords — use a password manager
3. Avoid public Wi-Fi or use a VPN
4. Keep all devices updated
5. Limit personal information shared online
6. Think before you click, text, or call back

cbmi
COLLEGE BUSINESS MANAGEMENT INSTITUTE

cbmi
COLLEGE BUSINESS MANAGEMENT INSTITUTE

Questions? Thank you!

Auxiliary Services

SACUBO
SOUTHERN ASSOCIATION OF COLLEGE AND UNIVERSITY BUSINESS OFFICERS