Faculty Senate Presentation

Cybersecurity Awareness Month – Security Best Practices

UofL - ITS Security Operations

What we will cover

- Why is cybersecurity important?
- Practice #1: University Email Account
- Practice #2: University Devices
  - Special Topic: Personal Cellphones
- Practice #3: Software and Plugins
  - Special Topic: Software Purchases
- Practice #4: Be Informed about Phishing
  - Special topics: Listservs and UL2FCTR/DUO attacks

All policies listed and mentioned are ***University*** policies and ***University*** requirements.

Why is Cybersecurity important?

- ISO-001 Information Security Responsibility
  - "Each member of the university community is responsible for the security and protection of information resources over which they have control."
  - UofL employees are **entrusted** with **protecting**, **storing**, and **processing** university information
    - "**Participate** in general security awareness program and regulatory specific training as required per job responsibilities."
    - "**Acknowledge** acceptance of security responsibilities."
- There has been an increase in security incidents
- We could face hefty fines along with regulatory violations potentially disrupting UofL's business
- If not monetary penalties, the university's reputation and goodwill are on the line
- Information Security policies and standards help us have common ground and they're designed to keep UofL secured

It's Everyone's Responsibility!

Practice #1 - University Email Account

- UofL email accounts should **NOT** be used for personal use. A UofL email account is for university business **ONLY**
- Some personal use is inevitably expected, but you'll be welcoming more risk to the university and your personal data
- The best practice is to keep your finances in your personal account
- Security incidents:
  - Malicious URL clicks
  - Business Email Compromise (BEC) = disable of accounts, or password reset, and massive spam being sent internally to continue credential harvesting
  - Adversary-in-the-Middle (AitM) and Man-in-the-Middle (MitM) = wiping of machine and password reset.
  - Future incidents of impersonation, information gathering, and spear phishing that bad actors can use to target UofL

Practice #2 - University Devices

- UofL provisioned devices are **NOT** users' personal devices

- Several policies refer to how UofL provisioned devices and computing accounts shall be used:
  - Be used in a prudent manner. Is it prudent to use it for your personal needs and wants?
  - "Computing accounts and facilities must not be used in any manner which could be disruptive, degrade the performance of, or cause damage to university computing infrastructure, resources, or data and/or other users." A security incident is an example of this

- ISO-014 Protection from Malicious Software
  - "Removable media (flash drives, CDs, external drives, etc.) from unknown or untrusted sources must be scanned for viruses and malware." Please ask your Tier One for guidance

When both worlds collide, you are exposing the university and your online identity to cybersecurity incidents such as ransomware.

Special Topic: Personal Cellphones

- The use of personal devices such as your cellphone is not prohibited, but if it will have University sensitive information stored and transmitted, **encryption is required**. Further, the university can use the personal device such as with other apps like Workday and Teams
  - For compliance and regulations, UofL can reserve the right to wipe **Office365 data** on personal mobile devices
  - UofL does not have the ability to wipe personal mobile devices

Practice #3 Software & Plugins

Software & browser extensions should **ONLY** be used for conducting university business functions and **NOT** for personal use

- Consult with your Tier One technical support team as to what other software you must have:
    - For example, using the Rakuten browser extension. What's the merit on using this to the university? Have you seen their privacy policy to see all the data that's given to it?

- Use common sense:
    - Does this software support your work-related tasks? If so, ask your Tier One to check it out. In this case, it's best to ask for permission rather than ask for forgiveness
    - If it does not, then do not install it
    - Again, ask yourself if this is prudent

- Software and Browser extensions can hide malicious software & activity, such as viruses, worms, trojans, Remote Access Trojans, and ransomware

Special Topic: Software Purchases

- Who can help with software purchase?
  - Tier Ones are your technology support team. Software should be:
    - Installed by your team
    - Approved by your unit before installing

- The Information Security Office has requested to see all software purchases and renewals. This is to ensure:
  - That nothing has changed from the use and data perspective as well as regulation since the initial review
  - Confirmation on controls from the vendor or an updated review of controls (e.g., a control review that is 3 years old is likely out of date)

- Purchasing of software between departments and a vendor is referred to as "Department Agreements"
  - Bookmark the Department Agreements web page for complete information
  - Instructions on how to submit Department Agreements.
  - Instructions on how to request software purchase.

- Controls and review also applies to software that has been used for years, but didn't go through a review process, or where contracts have not been updated with the current language
- 3rd party software needs to be reviewed, and contracts put in place prior to use, according to the Cloud Computing and 3rd Party Vendor Services policy.

Practice #4: Be Informed about Phishing

Phishing

A bogus or malicious message sent to try and steal: Usernames, Passwords, Personal Information, & other Sensitive Data.

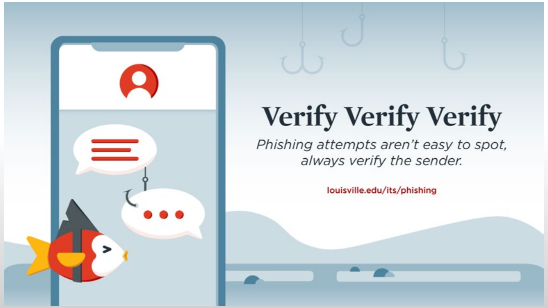
Smishing

A combination of "**SMS**" and "**phishing**" where scammers will send text messages disguised as trustworthy communications from businesses like Amazon, FedEx, or USPS.

Vishing

Uses fraudulent phone calls to trick victims into providing sensitive information, like login credentials, credit card numbers, or bank details.

If you are not sure of a url or link,
please DO NOT click the link. It may be phishy bait.
louisville.edu/its/phishing


Verify Verify Verify
Phishing attempts aren't easy to spot, always verify the sender.
louisville.edu/its/phishing

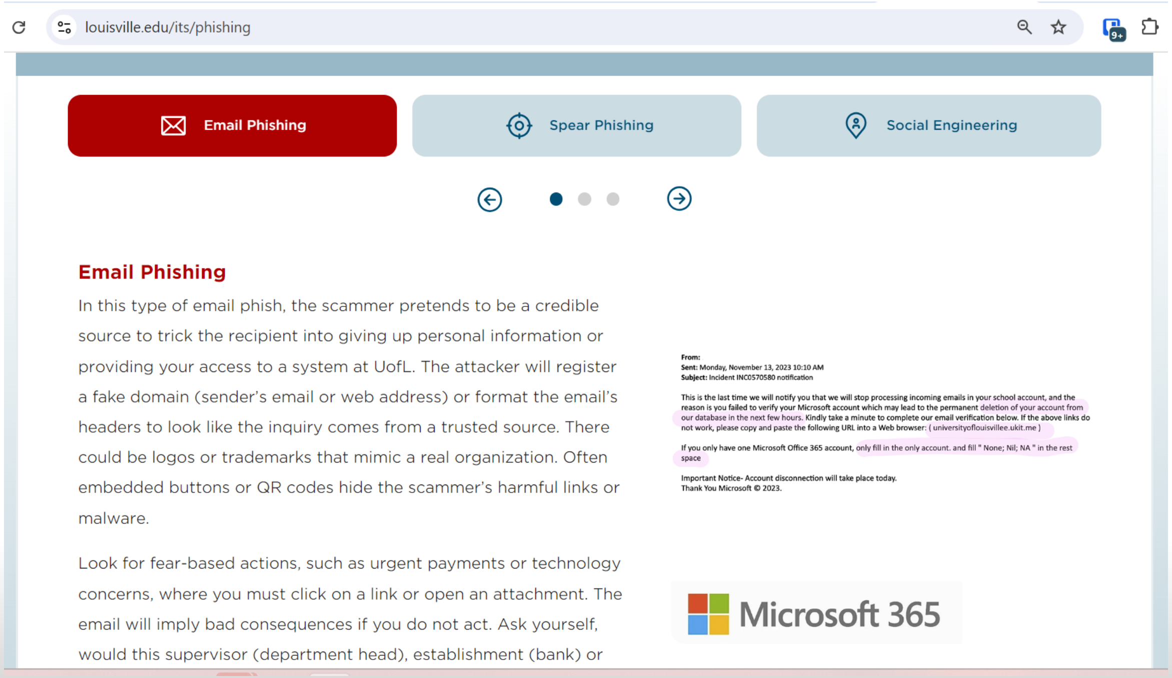
Phishing isn't just an email...
Watchout for fraudulent text messages, emails, and phone calls.
louisville.edu/its/phishing

Bookmark: Louisville.edu/its/phishing

You will learn about other types of phishing attacks and common examples on what to watch out for.

Look back at this site when in doubt!

https://louisville.edu/its/phishing



Email Phishing

In this type of email phish, the scammer pretends to be a credible source to trick the recipient into giving up personal information or providing your access to a system at UofL. The attacker will register a fake domain (sender's email or web address) or format the email's headers to look like the inquiry comes from a trusted source. There could be logos or trademarks that mimic a real organization. Often embedded buttons or QR codes hide the scammer's harmful links or malware.

Look for fear-based actions, such as urgent payments or technology concerns, where you must click on a link or open an attachment. The email will imply bad consequences if you do not act. Ask yourself, would this supervisor (department head), establishment (bank) or

From:
Sent: Monday, November 13, 2023 10:10 AM
Subject: Incident INC0570580 notification

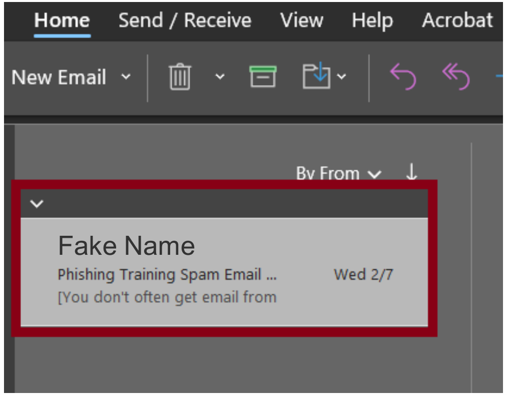
This is the last time we will notify you that we will stop processing incoming emails in your school account, and the reason is you failed to verify your Microsoft account which may lead to the permanent deletion of your account from our database in the next few hours. Kindly take a minute to complete our email verification below. If the above links do not work, please copy and paste the following URL into a Web browser: (universityoflouisvillee.ukit.me)

If you only have one Microsoft Office 365 account, only fill in the only account. and fill " None; Nil; NA " in the rest space

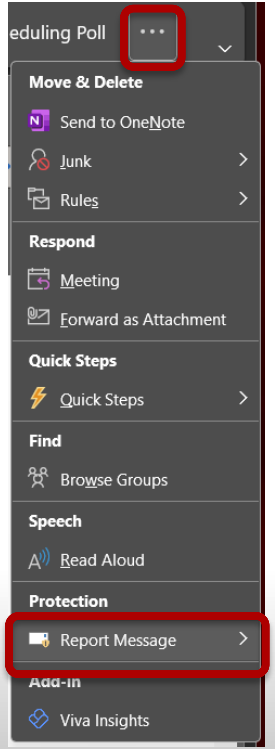
Important Notice- Account disconnection will take place today.
Thank You Microsoft © 2023.

Reporting Example in Outlook Desktop (older version)

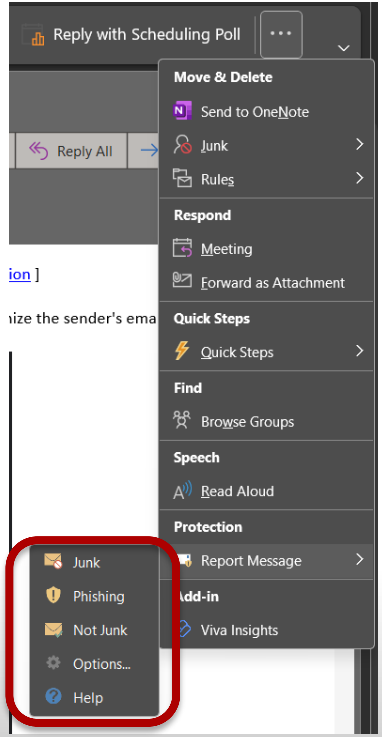
Step 1:



Step 2:

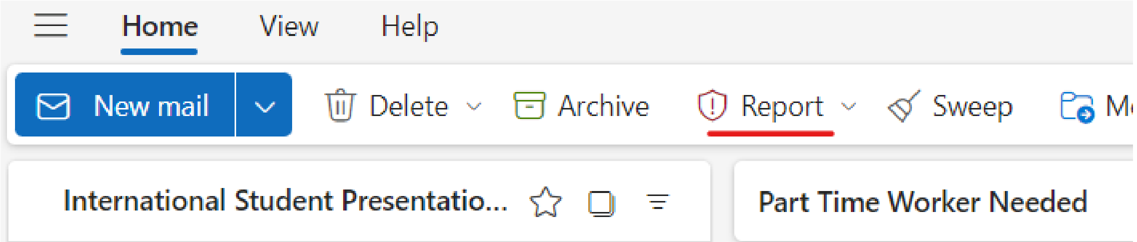


Step 3:

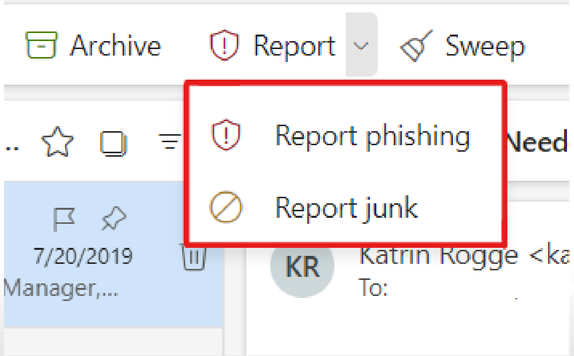


Reporting Example in Outlook Web Application (Browser) & Desktop (newest version)

Step 2:

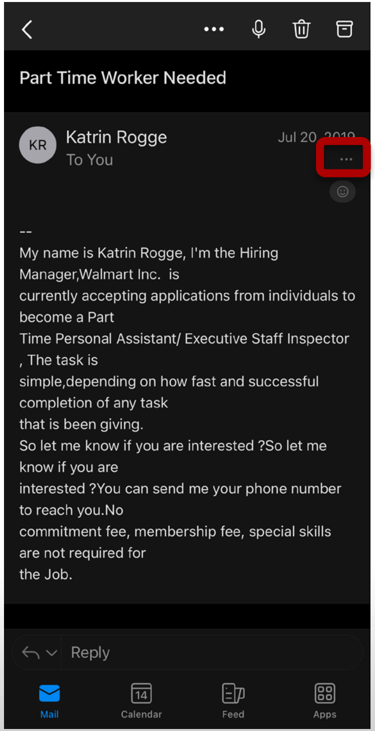


Step 3:



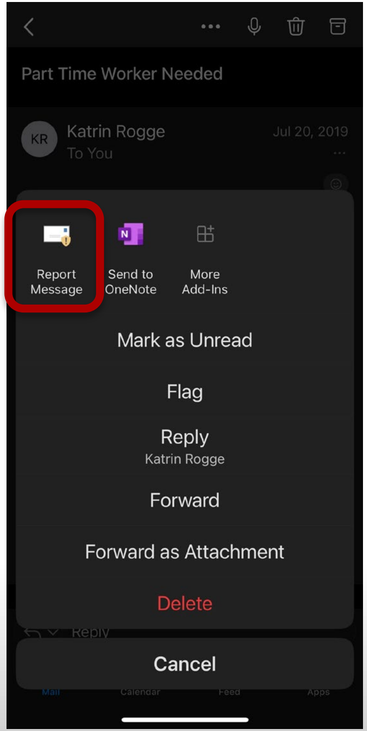
Reporting Example in Outlook Mobile App

Step 1:

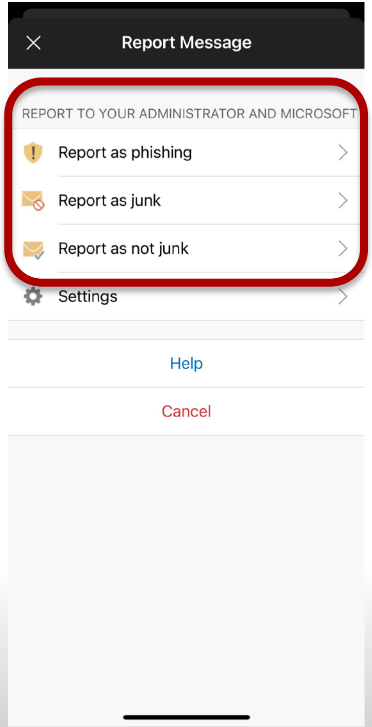


--
My name is Katrin Rogge, I'm the Hiring Manager,Walmart Inc. is
currently accepting applications from individuals to become a Part
Time Personal Assistant/ Executive Staff Inspector , The task is
simple,depending on how fast and successful completion of any task
that is been giving.
So let me know if you are interested ?So let me know if you are
interested ?You can send me your phone number to reach you.No
commitment fee, membership fee, special skills are not required for
the Job.

Step 2:

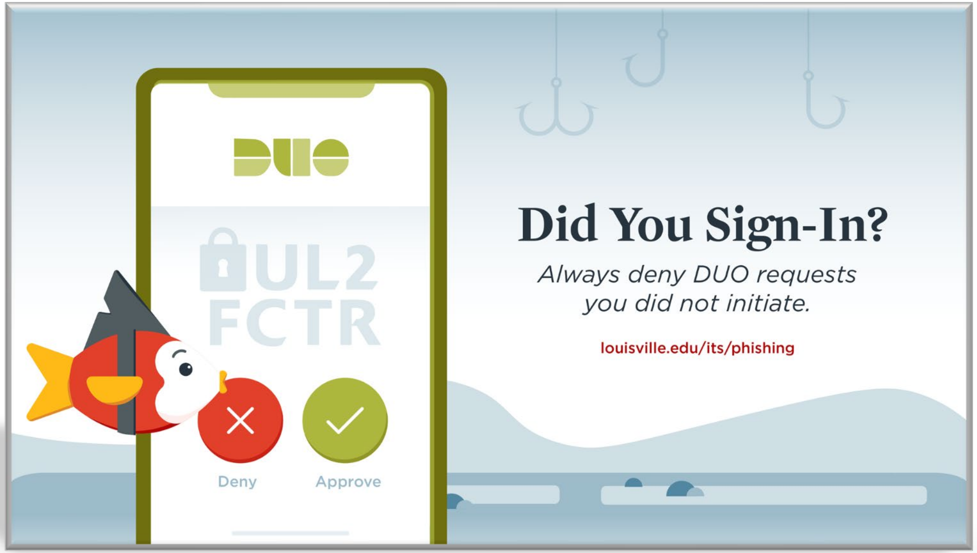


Step 3:



Special Topic: UL2FCTR/DUO attacks

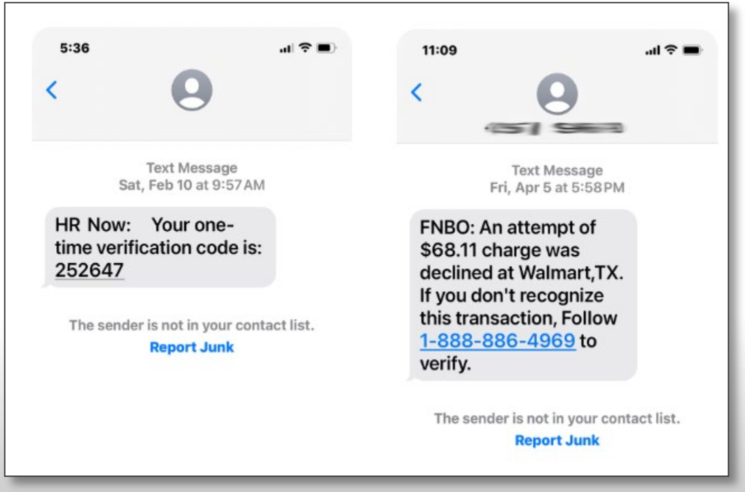
Bad actors obtain credentials to UofL accounts through phishing emails. Once they have access to credentials, they will attempt fraudulent DUO notifications to add malicious DUO device to the user's profile, thereby gaining full access to UL2FCTR computing accounts.



DUO Phishing Attacks

DUO Smish Text

Did you get a UL2FCTR/Duo authentication request that you did not initiate? UofL's Duo or second factor service will never email, call or text you asking for a passcode or PIN. We don't send SMS or text notifications without you first signing into a system.



5:36

Text Message
Sat, Feb 10 at 9:57 AM

HR Now: Your one-time verification code is: 252647

The sender is not in your contact list.
Report Junk

11:09

[redacted]

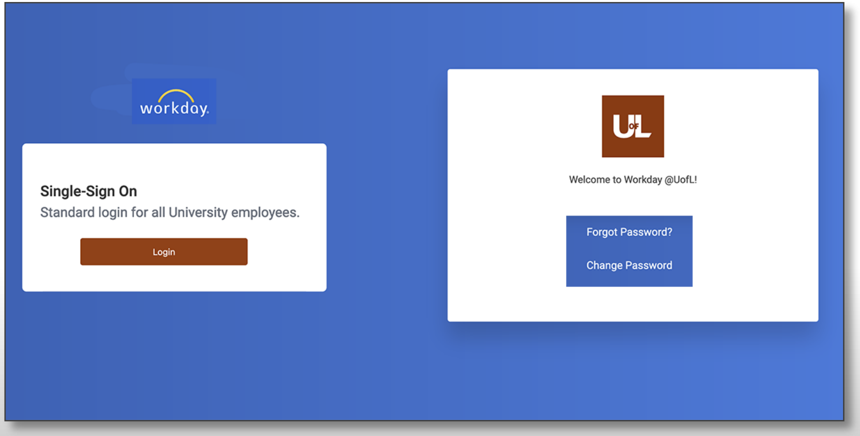
Text Message
Fri, Apr 5 at 5:58 PM

FNBO: An attempt of $68.11 charge was declined at Walmart,TX. If you don't recognize this transaction, Follow 1-888-886-4969 to verify.

The sender is not in your contact list.
Report Junk

Multiple Phish Attack – Asking for DUO Passcodes

Scammers often use more than one method of attack – a phishing email with a nefarious link to a fake webpage that displays a dubious UofL sign in which initiates a Duo-looking message to accept a prompt. Yes, cybercriminals are devious and getting better every day.



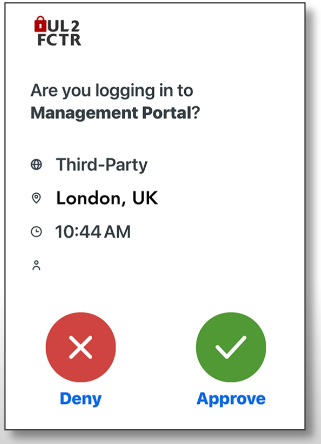
Single-Sign On
Standard login for all University employees.

Welcome to Workday @UofL!

DUO Phishing Attacks

DUO Phish Prompt

Did you get a UL2FCTR/Duo verification prompt request that you did not initiate? UofL's Duo or second factor service will never email, call or text you asking you to verify a separate prompt. We don't push authentication notifications without you first signing into a system.

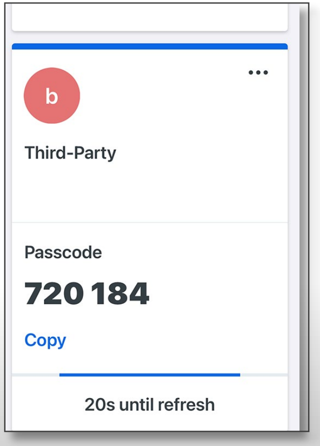


Are you logging in to **Management Portal?**

Third-Party

London, UK

10:44 AM



Third-Party

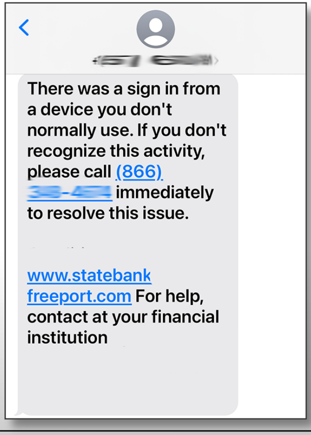
Passcode

720 184

20s until refresh

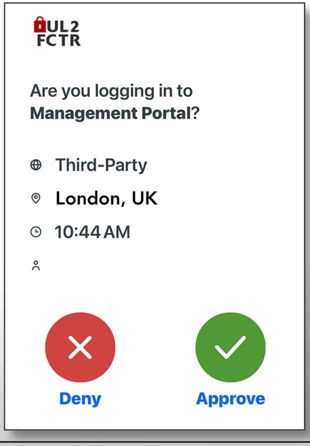
Exhaustion Phish Attack

Two-factor fatigue and email/text bombing are tactics where attackers flood a user with repeated requests to exploit the user's decreasing alertness due to exhaustion. Take time to think about what you are being asked to do and why before you act. Think twice before clicking within text messages or providing sensitive information on unsolicited inquires.


[redacted]

There was a sign in from a device you don't normally use. If you don't recognize this activity, please call (866) [redacted] immediately to resolve this issue.

www.statebankfreeport.com For help, contact at your financial institution



Are you logging in to **Management Portal?**

Third-Party

London, UK

10:44 AM

Special Topic: Listservs

Listservs are email lists that send emails to people associated with the University. However, as the University continues to better communication tools, we suggest Teams as the way to move forward.

- Use it to send important messages such as events
- Anyone can request a listserv.

There are three types of Listservs:

- Interactive – Subscribers to the listserv can send and respond to emails sent to the listserv.
- Moderate – If an email is sent to the listserv, the editor must approve the email before being sent out to all subscribers of the listserv.
- Announcement/Broadcast - Subscribers cannot respond to listserv emails. The editor is the only one that can send messages.

Improper Use of Listservs:

- List owners can decide if something is improper and would take proper penalty actions. If it goes beyond that, then it will need to go to the governing body, for example, student, faculty, or staff affairs.
- All UofL accounts on a UofL Listserv are subject to the Email Archive, User Accounts and Acceptable Use, and all other UofL policies.

Takeaways

- UofL devices and UofL computing accounts are not for personal use
- It's best to ask for permission
- Use common sense
- Clean up your UofL email. Change your contact preferences now and be smart about keeping things separated
- Adopt a security hat mindset and help keep the university safe
- Doing so can save UofL from operational, financial, and infrastructure disruptions
- If you're using your UofL provisioned device as your personal device, you're highly encouraged to cease that activity. UofL Human Resources offers a Computer Purchase Program for employees
    - Find out more at https://louisville.edu/hr/benefits/computer-purchase-program
    - For any questions about the computer purchase program, please contact Human Resources at 852-6258 or askhr@louisville.edu.

Please scan the QR code or click on the link to fill out the feedback form.

Faculty Senate Feedback

Thank you for attending!

Do you have any questions?

Upcoming Events and Resources

- Attend the Learning Café Unlock the Secrets to Cybersecurity to Protect Yourself, October 23rd at noon – Virtual Teams Meeting - Employee Success Center. Register here!

- If you would like to learn more about how to stay Cyber Safe at Work, there is a LinkedIn Learning course that can help you.
  - Length: 1 hour 10 minutes
  - Easy to go through
  - Each section has a quiz and a test at the end
  - Can get a certificate after passing.
  - Access the course here.

- Join UofL ITS and the Cybersecurity & Infrastructure Security Agency (CISA) talk on "Raising Awareness for Cybersecurity – It's Everyone's Responsibility!" happening on October 17th at 4:30 PM at the PNC Horn Auditorium in Frazier Hall. Register here!