Staff 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
- Practice #3: Device Maintenance
- Practice #4: Backing Up Data
- Practice #5: Be Informed about Phishing, 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

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 expose the university and your online identity to cybersecurity incidents such as ransomware.

Practice #3: Device Maintenance

- By keeping a device up-to-date:
    - It increases the security of the device.
    - Limits accessibility of bad actors exploiting vulnerabilities and unpatched software.

    Most applications are not automatically updated. Please thoroughly check to ensure that those are up-to-date.

- Returning unused UofL Equipment:
    - This allows for inventory to be up-to-date and decreases the chance of lost devices.
    - By keeping the surplus cycle running and theft of a device is less likely to occur.

STAY SAFE BY

UPDATING YOUR SOFTWARE

Update Software for Safety - YouTube

- Most individual apps are not automatically updated, so you must ensure those are up-to-date.
    - For example: Notepad ++
    - Remember that the OS updates are done automatically; anything else is your responsibility to update.

- The Workstation and Computing Devices policy also deals with automated OS patching: "All operating systems and other software should be kept-up-to-date by installing all available security updates and patches on a regular schedule but not less often than every 30 days. Automated update capabilities must be turned on."

Practice #4: Backing up Data

UofL storage should **NOT** be used to back up personal files.

- We have seen old data and personal generating incidents like worms and viruses. This occurred because UofL document storage solutions were used to backup, or simply be used as the primary storage option for user
- To backup data from workstations, please use:
  - OneDrive/SharePoint
  - CardBox

Note: Network drives may be used, but the future is moving towards Software-as-a-Service (SaaS) like the ones listed above

- Per the Backup of Data policy, "Backups are an ***essential*** part of disaster recovery and business continuity planning."
- "Files containing valuable information must be backed up."
- Another related policy is ISO-002 Business Continuity and Disaster Recovery
- In case we need to wipe your device, all your locally saved data on disk will be removed

Note: *This is not your get out of jail card. The goal is to prevent security incidents in the first place.*

Practice #5: Be Informed about Phishing

Phishing

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

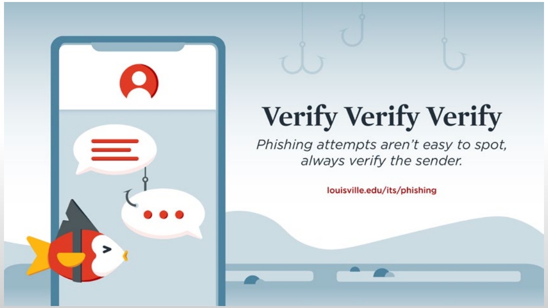
Smishing

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

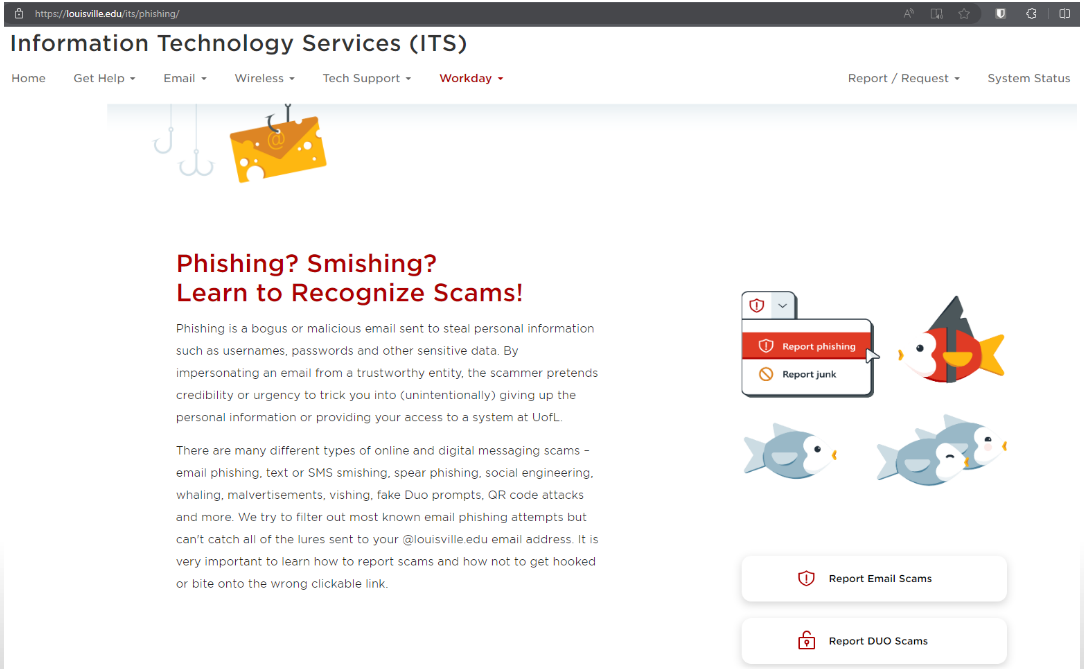
Phishing isn't just an email...
Watchout for fraudulent text messages, emails, and phone calls.
louisville.edu/its/phishing

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



Information Technology Services (ITS)

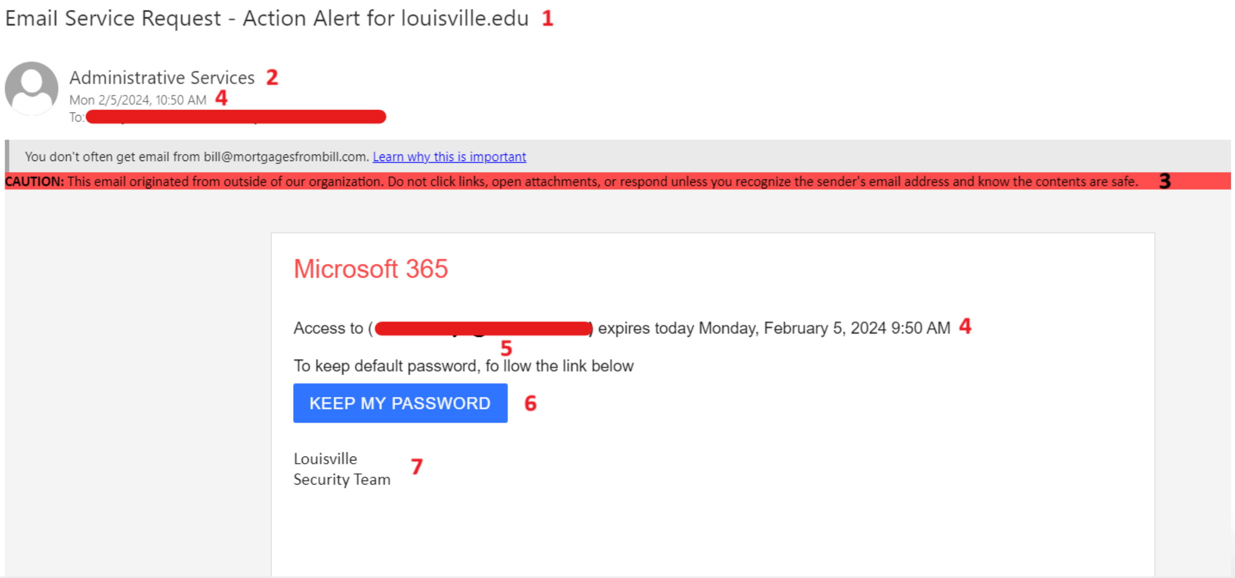
Phishing? Smishing?
Learn to Recognize Scams!

Phishing is a bogus or malicious email sent to steal personal information such as usernames, passwords and other sensitive data. By impersonating an email from a trustworthy entity, the scammer pretends credibility or urgency to trick you into (unintentionally) giving up the personal information or providing your access to a system at UofL.

There are many different types of online and digital messaging scams – email phishing, text or SMS smishing, spear phishing, social engineering, whaling, malvertisements, vishing, fake Duo prompts, QR code attacks and more. We try to filter out most known email phishing attempts but can't catch all of the lures sent to your @louisville.edu email address. It is very important to learn how to report scams and how not to get hooked or bite onto the wrong clickable link.

Phishing Email Example: Password

1. Header & Subject Line
2. Who did this come from?
3. Red Banner
4. Email time & context
5. Improper Grammar
6. KEEP MY PASSWORD
7. Signature



Email Service Request - Action Alert for louisville.edu

Administrative Services
Mon 2/5/2024, 10:50 AM
To: [redacted]

You don't often get email from bill@mortgagesfrombill.com. Learn why this is important

CAUTION: This email originated from outside of our organization. Do not click links, open attachments, or respond unless you recognize the sender's email address and know the contents are safe.

Microsoft 365

Access to ([redacted]) expires today Monday, February 5, 2024 9:50 AM

To keep default password, fo llow the link below

KEEP MY PASSWORD

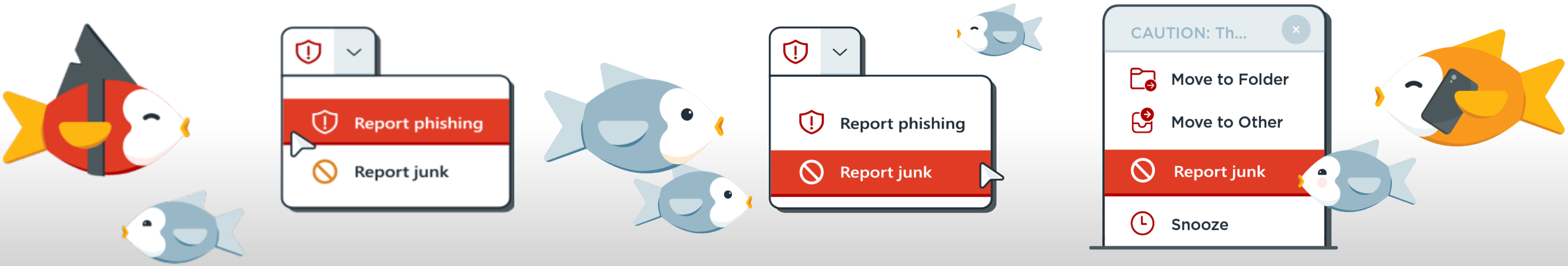
Louisville
Security Team

How to Report Emails

Always remember to **not click on any links** until you are certain that the email is legitimate. If the email does not seem legitimate, please follow these steps to report the email:

You have 2 options on how to report emails:

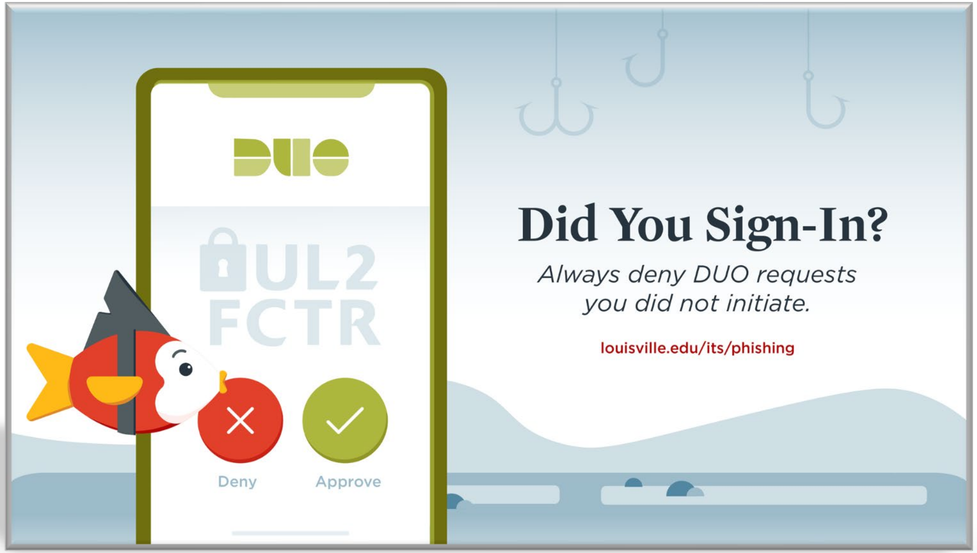
1. Report Phishing
   - Select the email > Report > Report Phishing
2. Report Junk
   - Select the email > Report > Report Junk



Phishing — Information Technology Services (ITS) (louisville.edu)

UL2FCTR/DUO attacks

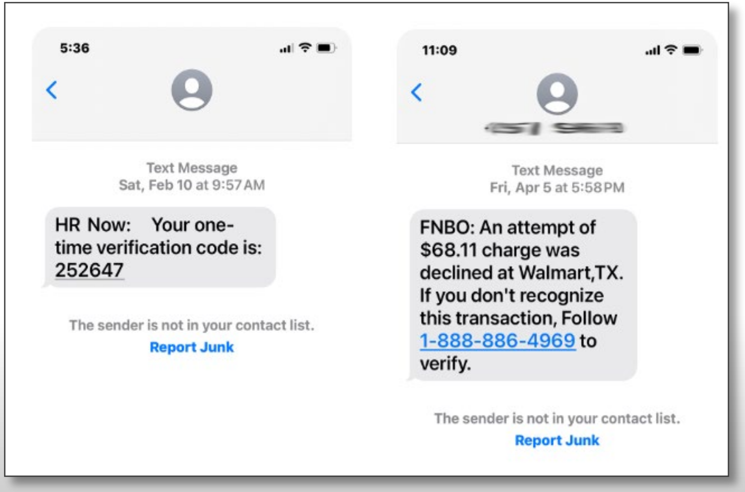
Bad actors obtain credentials to UofL accounts through phishing emails. Once they have access to credentials, they will attempt fraudulent DUO notifications to add malicious DUO device to the user's profile, thereby gaining full access to UL2FCTR computing accounts.


DUO
UL2
FCTR
Deny
Approve
Did You Sign-In?
Always deny DUO requests you did not initiate.
louisville.edu/its/phishing

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]

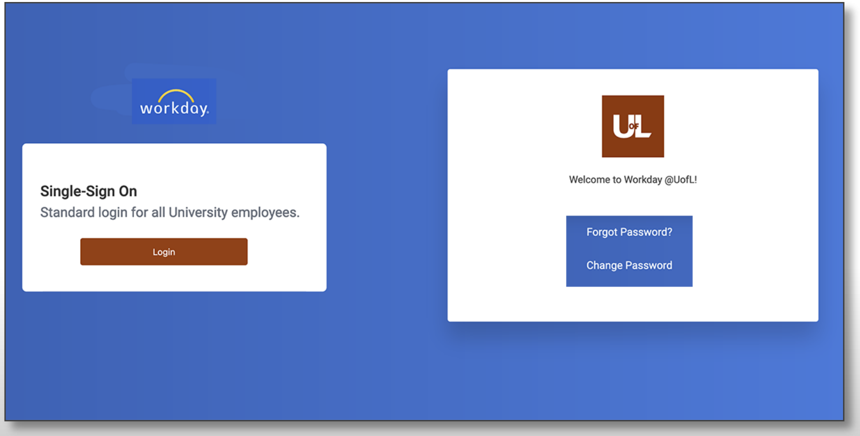
Text Message
Fri, Apr 5 at 5:58 PM

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.



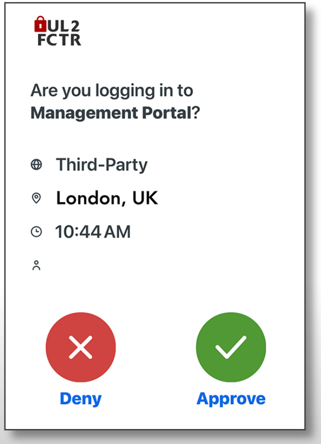
Single-Sign On
Standard login for all University employees.

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.

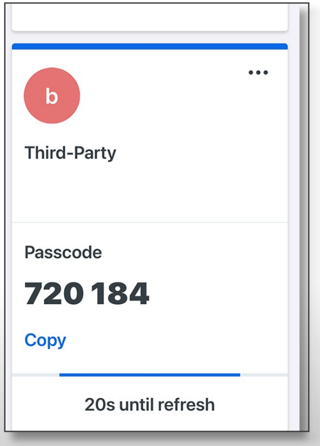


Are you logging in to **Management Portal?**

Third-Party

London, UK

10:44 AM



Third-Party

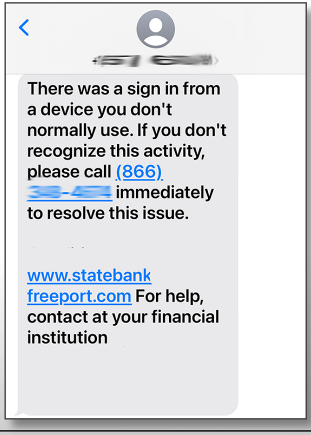
Passcode

720 184

20s until refresh

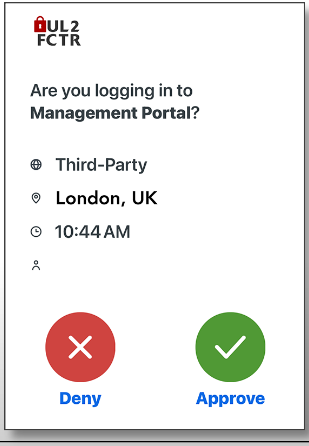
Exhaustion Phish Attack

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

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
- The policy here talks about what you can expect from privacy and potential disclosure:
    - It’s not guaranteed or expected
    - Logs, access, and other metadata are maintained
- 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 Computer Purchase Program
    - For any questions about the computer purchase program, please contact Human Resources at 852-6258 or askhr@louisville.edu.

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!

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

Staff Senate Feedback

Thank you for attending!

Do you have any questions?