Security Awareness

- How can you be cybersafe? -

UofL - ITS Enterprise Security

What we will cover

- Why is Cybersecurity Important?
- Phishing & Scams
- Multi-factor Authentication (MFA) Attacks
- How to Report Emails
- Security Best Practices
- Takeaways

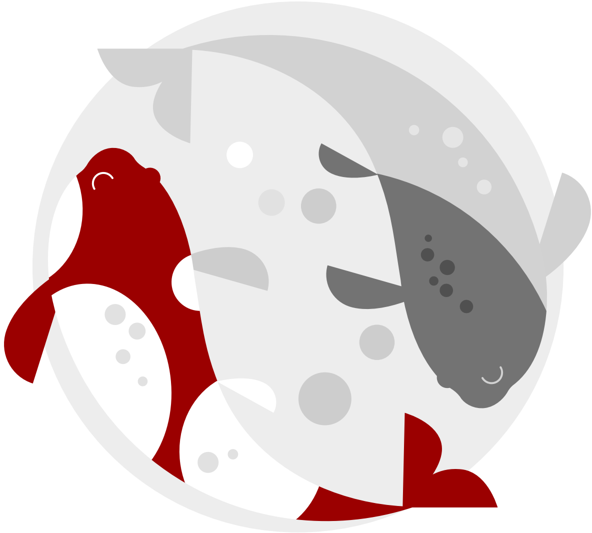
All policies listed and mentioned are ***University*** policies and ***University*** requirements.

Why is Cybersecurity important?

Cybersecurity is the art of protecting networks, devices and data from unauthorized access or criminal use and the practice of ensuring confidentiality, integrity, and availability of information.

- 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."

- Information Security policies and standards help us have a common ground. They are designed to keep UofL and its members secured.



Phishing & Scams

What is Phishing?

Phishing is a bogus or malicious message sent to try and steal:

Usernames, Passwords, Personal Information, & other Sensitive Data

Email Phishing

Bad actor pretends to be a credible source to trick an individual into giving up personal information or providing credentials to your UofL account(s).

Spear Phishing

Bad actor targets a specific individual by gathering information (online) and uses the data to their advantage.

Malware Phishing

Bad actors will insert an attachment (like a bank statement or resume) in an email that contains malware. They will make the attachment look like it came from a trustworthy source.

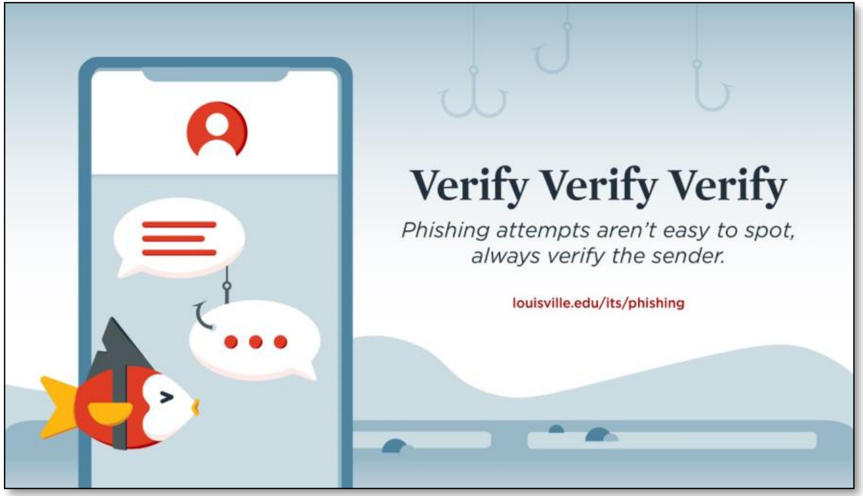
Smishing

Smishing is a combination "**SMS**" and "**phishing**" where bad actors will send text messages disguised as trustworthy communications from businesses like Amazon, FedEx, or USPS.

Scammers will try steal personal information, money, passwords, and more from users.

How to spot smishing:

- Check for improper grammar and punctuation
- Look out for bad actors trying to request you to copy and paste links into your browser
- Do you recognize the sender? Were you expecting this message?


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

Vishing

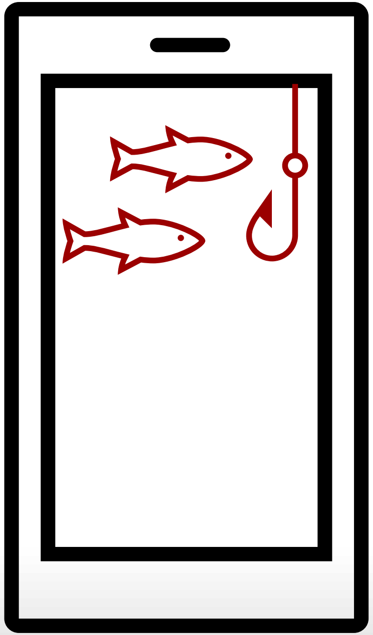
Vishing uses fraudulent phone calls to trick victims into providing **sensitive information**, like **login credentials**, **credit card numbers**, or **bank details.**

Voice Cloning

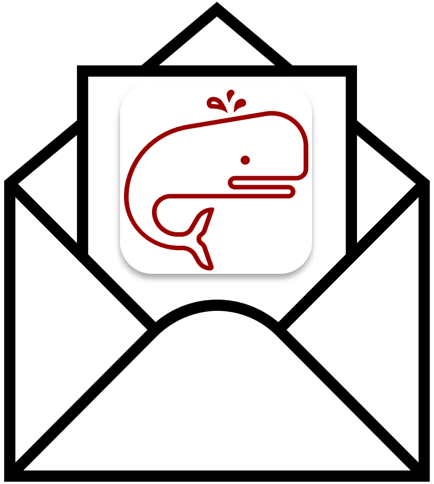
- Voice cloning technologies use **artificial intelligence** to create realistic voice recordings that copy loved one's or even your boss's voice. Spoofing phone numbers.

Tech Support Vishing

- Scammers will imitate tech support warning the user that suspicious activity has been found on their device or through their accounts. Fake offering of a solution to install remote access tools to steal information or install malware.



Business Email Compromise



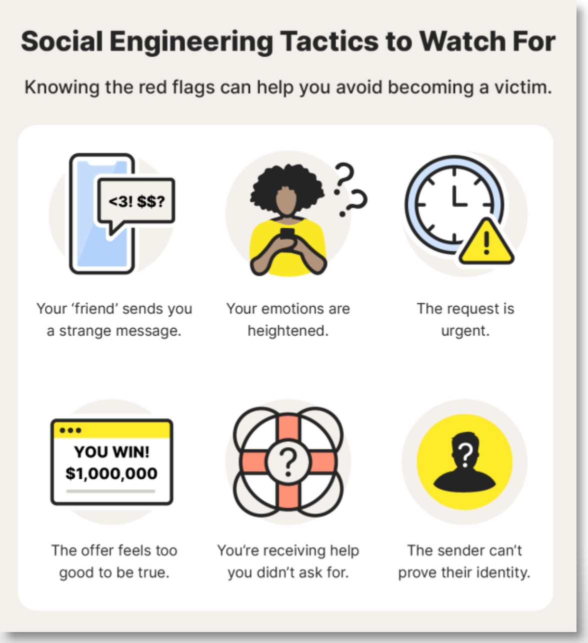
BEC (Business Email Compromise) occurs when a bad actor impersonates an individual higher up in a company. They trick the employee into sending money or data.

Bad actors will send out mass phishing emails to try and get the most amount of numbers. BEC scammers use spear phishing to target specific users. They may try to gain access into accounts by sending deceiving request or target executives directly (also called "whaling") to exploit trust.

- How to protect yourself:
  - Be careful with the information you share online
  - Do not click on anything in an unsolicited email or text message
  - Review the email sender. Make sure you know who they are or if you were expecting an email from them
  - Be careful what you download
  - Setup two-factor authentication

For more information, please visit: What is Business Email Compromise (BEC)? | Microsoft Security

Social Engineering



Social Engineering Tactics to Watch For

Knowing the red flags can help you avoid becoming a victim.

- Your 'friend' sends you a strange message.
- Your emotions are heightened.
- The request is urgent.
- The offer feels too good to be true.
- You're receiving help you didn't ask for.
- The sender can't prove their identity.

Norton – What is social engineering?

What is a social engineering attack?

- A scammer will use social skills to obtain or compromise information about the organization or to gain access into the network
- They will try to seem inconspicuous and innocent by pretending to be a new employee, tech support, or more
  - Example:
    - The MGM hotel & casino was hacked due to social engineering which led to a ransomware attack
- We have seen and heard from other sources that scammers like to target employees that work and have access to:
  - Payment Management Services
  - Sensitive Information

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

QR Code Scams

A scammer’s QR code could take you to a spoofed site that looks legitimate. And if you log in to the spoofed site, the scammers could steal any information entered. The QR code could also install malware that steals your information before you realize it

What to lookout for:

- **DO NOT** scan a QR code in an unexpected place
- Inspect the URL before you open it
- **DO NOT** scan QR codes in text messages or emails
  - Especially if you are not expecting it or it urges you to act immediately

Scammers hide harmful links in QR codes to steal personal information

- Inspect the URL before clicking
- Keep your phone’s OS up to date
- Use strong passwords and multi-factor authentication

FEDERAL TRADE COMMISSION

Scammers hide harmful links in QR codes to steal your information | Consumer Advice (ftc.gov)

How to Spot Phishing

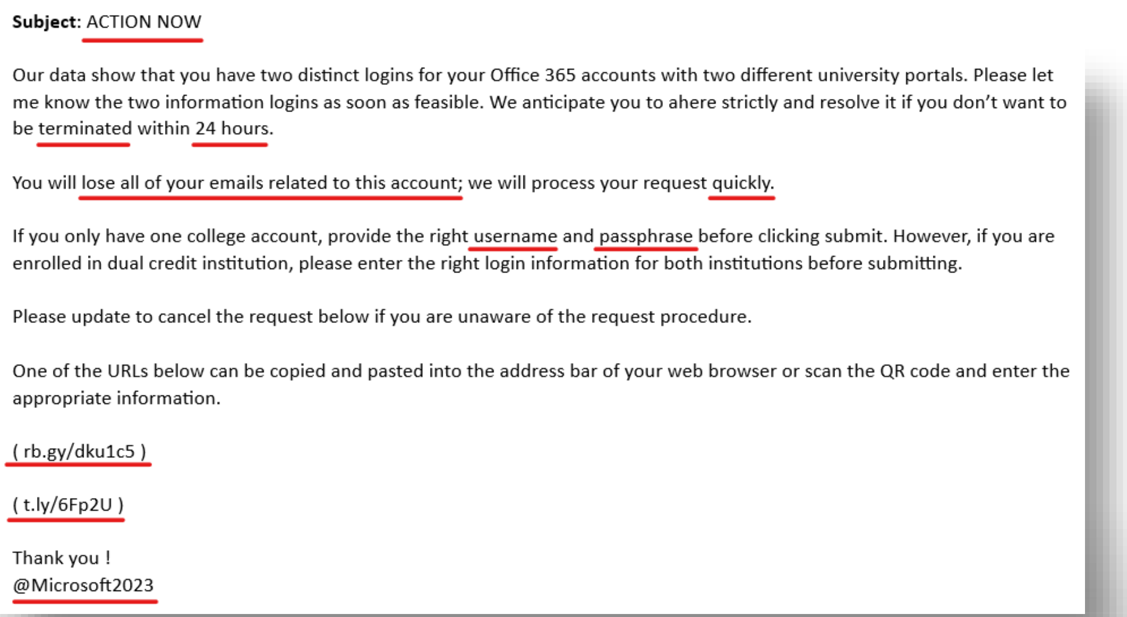
Phishing Email Example: Copy and Paste

Phishing Activity:

- Sense of urgency, “ACTION NOW” & “quickly”
- A short time limit. “24 hours”
- Has you copy and paste the URLs into the browser

The University will **not** ask you for your login information or your login information for another account.

Do not copy and paste suspicious URLs into your browser (or click on them) and **do not** scan QR codes from untrusted sources.



Subject: ACTION NOW

Our data show that you have two distinct logins for your Office 365 accounts with two different university portals. Please let me know the two information logins as soon as feasible. We anticipate you to ahere strictly and resolve it if you don’t want to be terminated within 24 hours.

You will lose all of your emails related to this account; we will process your request quickly.

If you only have one college account, provide the right username and passphrase before clicking submit. However, if you are enrolled in dual credit institution, please enter the right login information for both institutions before submitting.

Please update to cancel the request below if you are unaware of the request procedure.

One of the URLs below can be copied and pasted into the address bar of your web browser or scan the QR code and enter the appropriate information.

(rb.gy/dku1c5)

(t.ly/6Fp2U)

Thank you !
@Microsoft2023

S.L.A.M

- **S**top
  - Examine the sender
  - The **Red Banner and CAUTION message** at the top of emails is a helpful tool to alert you of external senders.
- **L**inks
  - Be very vigilant about links
  - Bad actors can make links look legitimate to try and get you to click on them.
- **A**ttachments
  - Bad actors will attach attachments within the email disguised as PDFs, documents, etc. In doing so, they could possibly download malicious software/virus on a computer if opened/downloaded.
- **M**essage
  - Check for grammatical errors, missing/improperly placed punctuation, and strange text/wording. Bad actors will use everyday greetings to throw users off as well. Like “Are you available?” Please thoroughly read the message/context. Bad actors will also push that “Action Now” and try to create that sense of urgency and panic.

*If you feel uncomfortable about an email, a text message or a phone call, **DO NOT** respond and report. It's better to be safe than sorry.*

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

Multi-Factor Authentication Attacks

DUO Two-factor Authentication

What is two factor authentication?

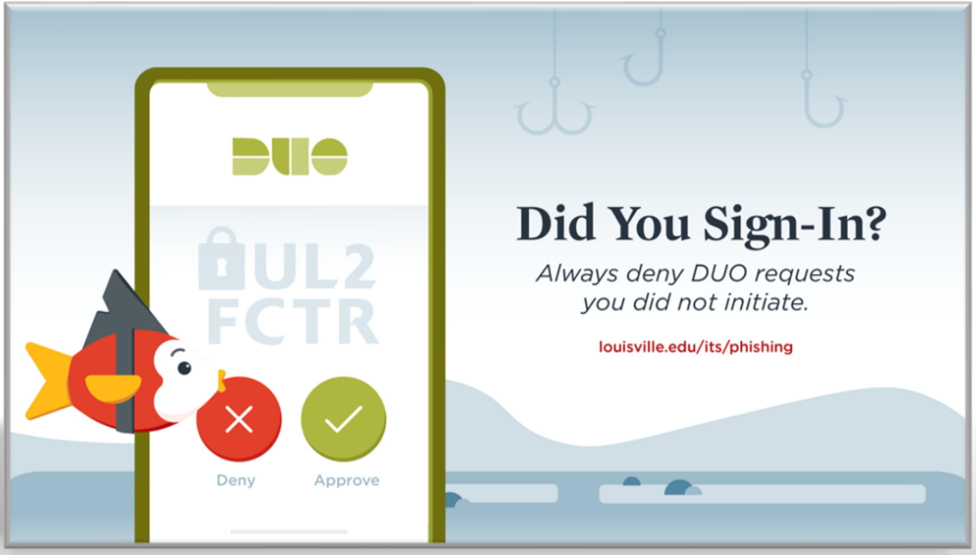
- Two-factor authentication adds a second layer of security to your online accounts by requiring a second piece of information before you can log into a system.

Why do I need UL2FCTR / Duo?

- Two-factor authentication keeps your account secure even if your password is compromised.
- Our two-factor authentication system is a Duo application specific to UofL named UL2FCTR.
- With UL2FCTR or Duo, you'll be alerted right away (on your phone) if someone is trying to log in as you.

What is a multifactor attack?

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

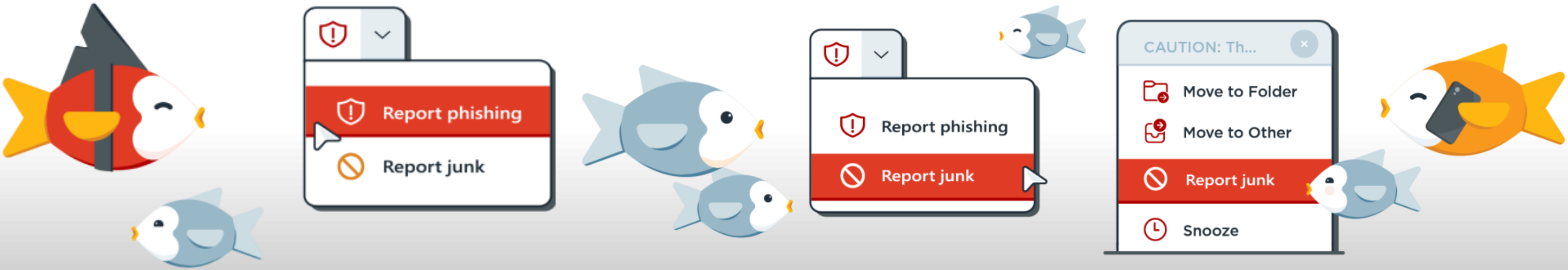
How to Report Emails

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:

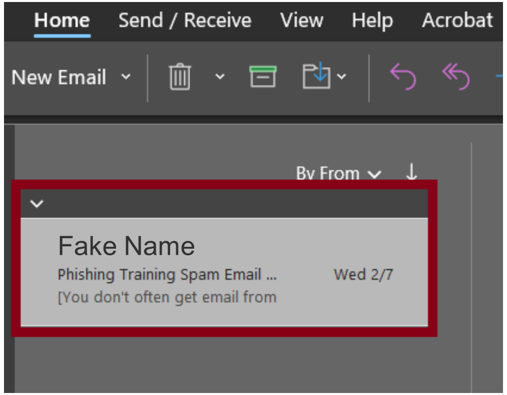
You have 2 options on how to report emails:

1. Report Phishing
2. Report Junk



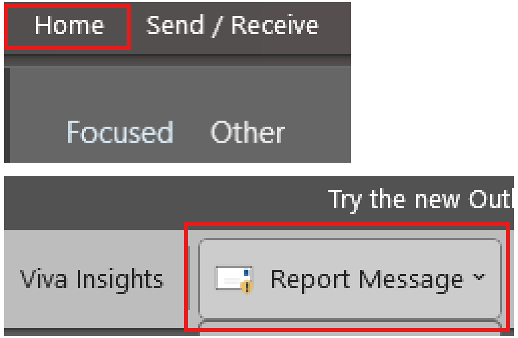
Reporting Example in Desktop Outlook (classic)

Step 1:

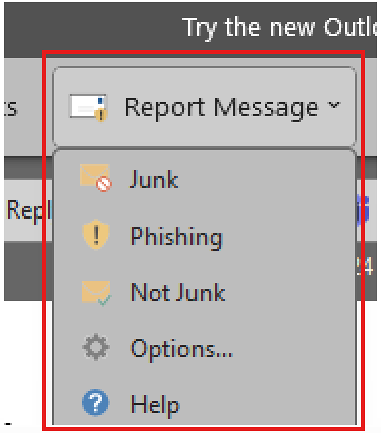


Fake Name
Phishing Training Spam Email ... Wed 2/7
[You don't often get email from

Step 2:

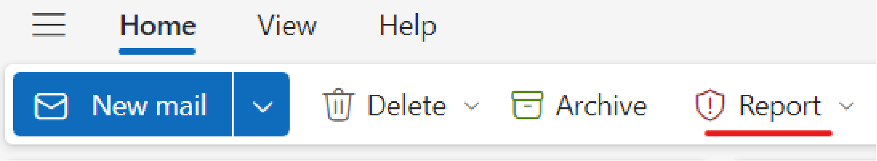


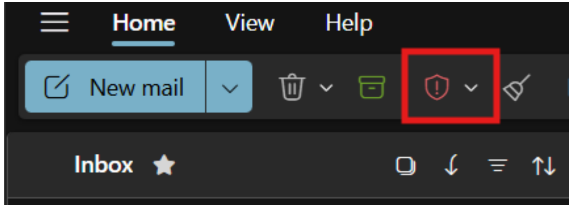
Step 3:



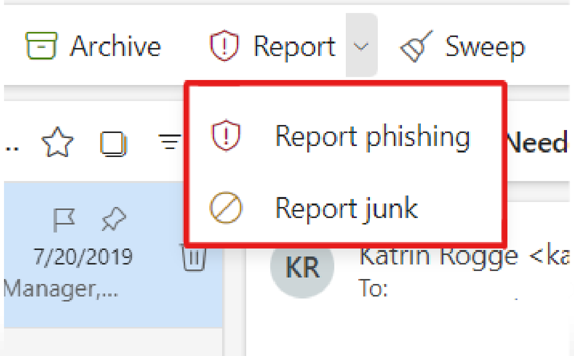
Reporting Example in Outlook Web Application (Browser) & Desktop

Step 2:



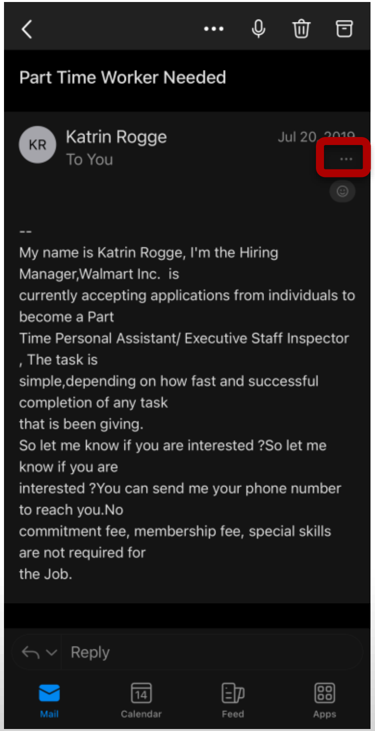


Step 3:



Reporting Example in Outlook Mobile App

Step 1:

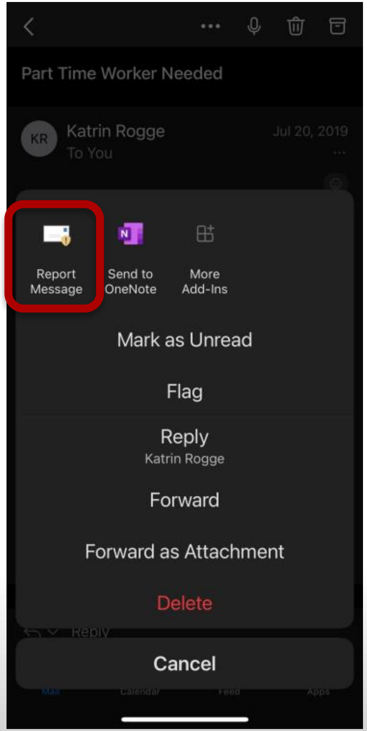


Part Time Worker Needed

Katrin Rogge
To You
Jul 20, 2019

--
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.

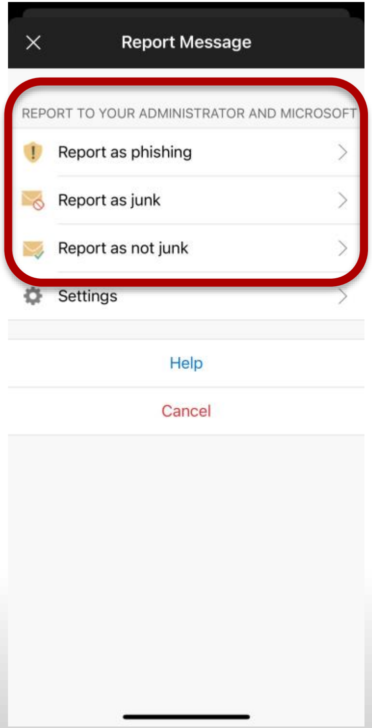
Step 2:



Part Time Worker Needed

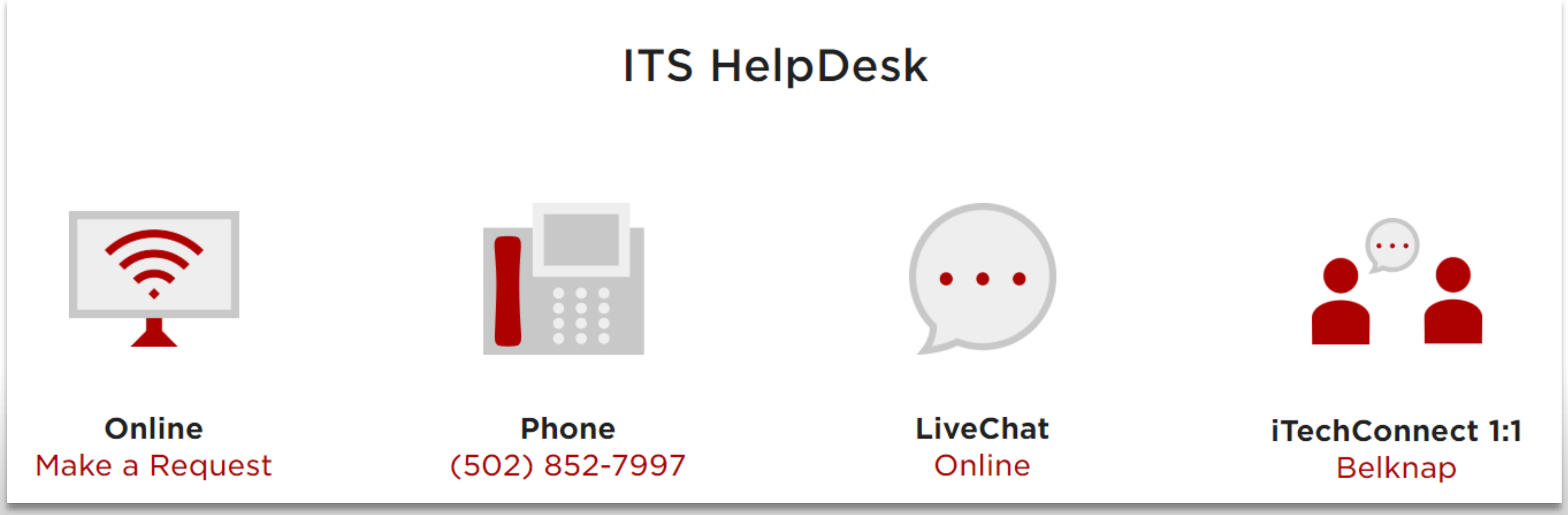
Katrin Rogge
To You
Jul 20, 2019

Step 3:



UofL ITS Helpdesk site

Please visit louisville.edu/its/get-help/its-helpdesk If you need assistance accessing your university accounts (ULink, for example), unlocking your password, or more, we can help.



ITS HelpDesk

Online
Make a Request

Phone
(502) 852-7997

LiveChat
Online

iTechConnect 1:1
Belknap

Security Best Practices

Keeping Device Up-to-Date

- 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

ISO-012 Workstation and Computing Devices

- All computing devices shall: "Have operating systems and other software maintained in the most up-to-date and secure manner reasonably possible."

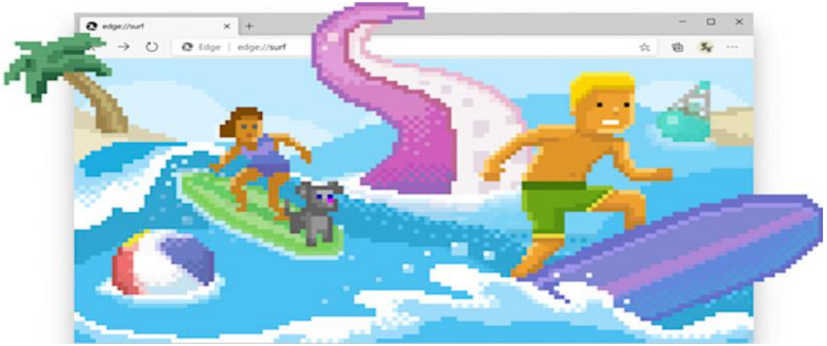
Passwords

ISO-008 Passwords

- Passwords to university accounts and devices must be kept confidential
- To preserve account integrity, the owner of the account must be the **only person** with knowledge of the password
- **No user is required to share a university account password with another individual**; including but not limited to managers, co-workers, or technical staff
- Passwords that have been or suspected to have been compromised must be changed immediately

For more information, please review Pol-Passwords — Policy and Procedure Library (louisville.edu)

Staying Safe while Surfing the Web



ThePhoto by PhotoAuthor is licensed under CCYYSA.

ISO-007 User Accounts and Acceptable Use

"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. Personal use should be kept to a minimum and in no case should a university account be used for non-university business purposes."

What to look out for:

1. Do not use website that being with http://. Use sites that begin with https://. The S after http stands for secure
2. Change your browser preference **to only** allow HTTPS connections
3. Check website URLs for slight misspellings or incorrect domain extensions. For example, **louisville[.]com** compared to **louisville.edu**
4. Check the padlock next to the website's URL to verify that the websites certificate has not expired and comes from a legitimate certificate authority

Enabling MFA

What is Multi-Factor Authentication (MFA)?

- Security enhancement that goes beyond a username + password
- It requires a user to provide a combination of two or more of the following:
  - Biometrics such as FaceID or fingerprint scanners are ways to prove authentication with something you are
  - A hardware token, a cellphone, and a security key provide proof with something you have

Takeaways

UofL Phishing Page

Please visit Phishing — Information Technology Services (ITS) (louisville.edu) to learn more and better protect yourself from Phishing and Scams.

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

Digital Transformation Center
– Cybersecurity Workforce Program –

The Digital Transformation Center presents the Cybersecurity Workforce Program. Designed to equip participants with the skills needed to excel in cybersecurity, this program offers a flexible learning path tailored to different levels of expertise.

This program is the result of a collaborative effort led by the University of Louisville. As part of a national initiative, UofL is spearheading a Coalition of schools to develop a comprehensive cybersecurity curriculum. Each school in this coalition is designated by the National Security Agency (NSA) as a National Center of Academic Excellence (NCAE) in Cyber Defense, contributing their unique expertise and skills in cybersecurity systems.

For more information, please visit: Digital Transformation Cybersecurity Workforce Program | Service Centers

Digital Transformation Center
– Technology Certification Pathways –

Digital Transformation Center presents the Information Technology Certification Pathways (ITCP) — a fully online program designed to help you build technical skills and earn industry-recognized certifications.

Courses available:

- CompTIA Tech+
- CompTIA A+
- Cisco Certified Network Associate (CCNA)
- CompTIA Network+
- CompTIA Security+
- CompTIA Cloud+
- CompTIA Pentest+

For more information, please visit: Digital Transformation IT Certification Pathways | Service Centers

Thank you for your time!

Questions?

2025 Cybersecurity Awareness - Faculty Senate - Feedback Form

ITS Enterprise Security - CISA Presentation - Sign Up Form