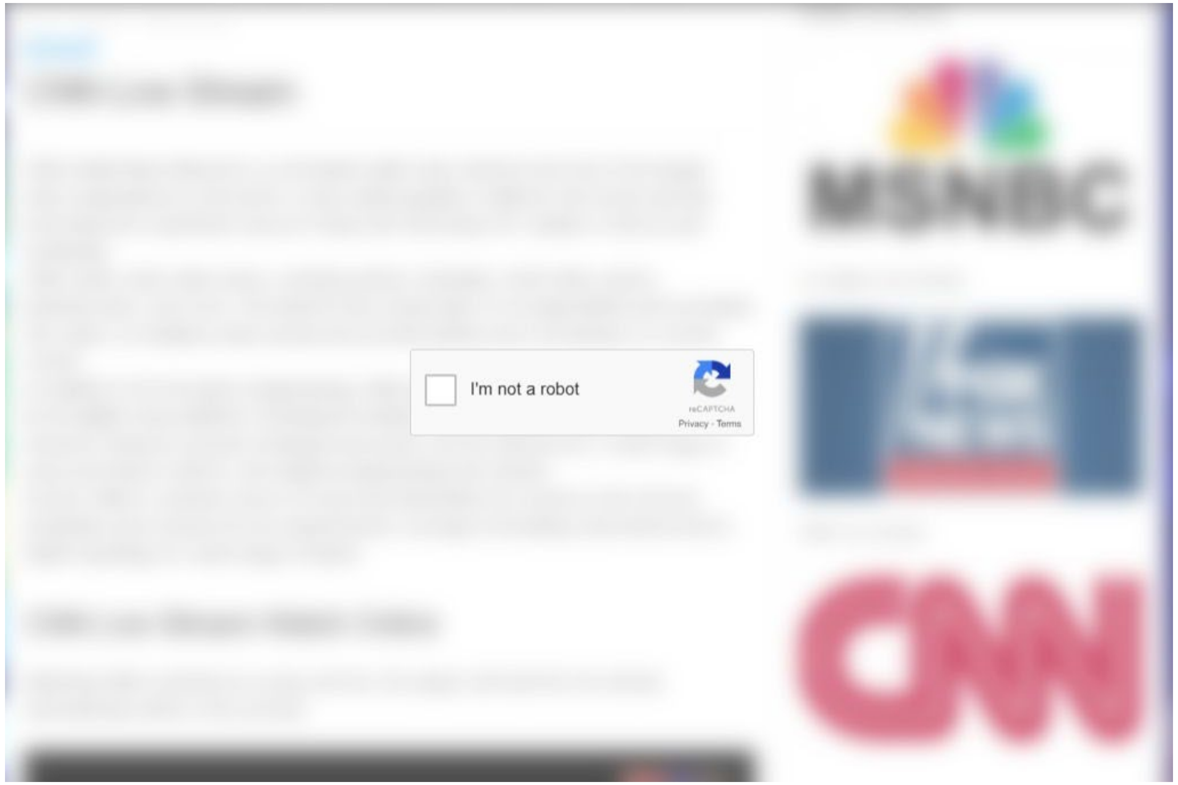
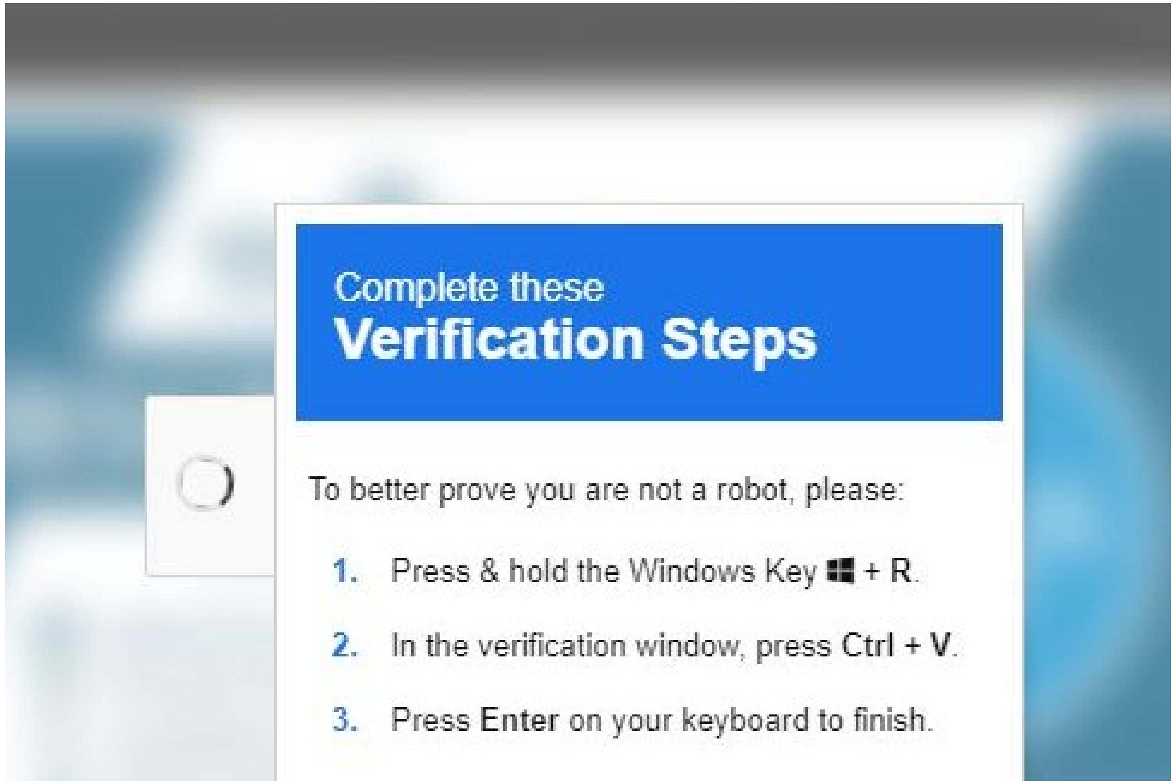
Fake Re-Captchas – Don’t fall for it

Fake-ReCaptchas – What are they and How Should You Respond?

- They look like the normal captchas, but they appear on websites that are **sketchy**, on a **weird link** you clicked, or a **spoofed website** that looks extremely like the real one
  - Say louisville[.]university[.]com instead of louisville.edu
  - Louisville[.]edu[.]xyz
- The Fake prompt **adds extra steps** for you to do; instead of the normal graphics, **claiming urgency** and trickery
- It asks you to **download a file**, **install a browser extension**, or **hit extra keys** on your keyboard
- By this time, malware was unintentionally downloaded potentially compromising the device and stealing your personal information

Fake Re-Captchas - Examples



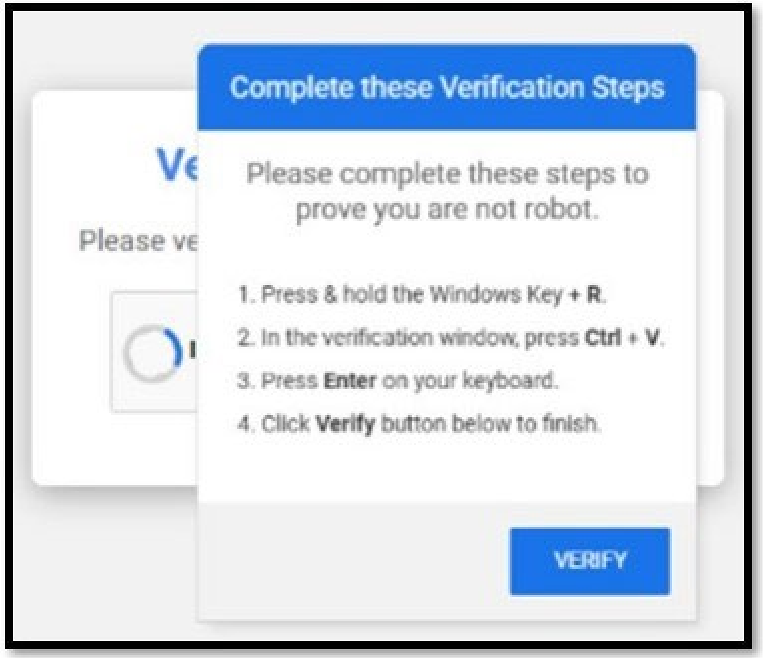


Complete these
Verification Steps

To better prove you are not a robot, please:

1. Press & hold the Windows Key ⊞ + **R**.
2. In the verification window, press **Ctrl** + **V**.
3. Press **Enter** on your keyboard to finish.

Fake Re-Captchas – Examples, contin.



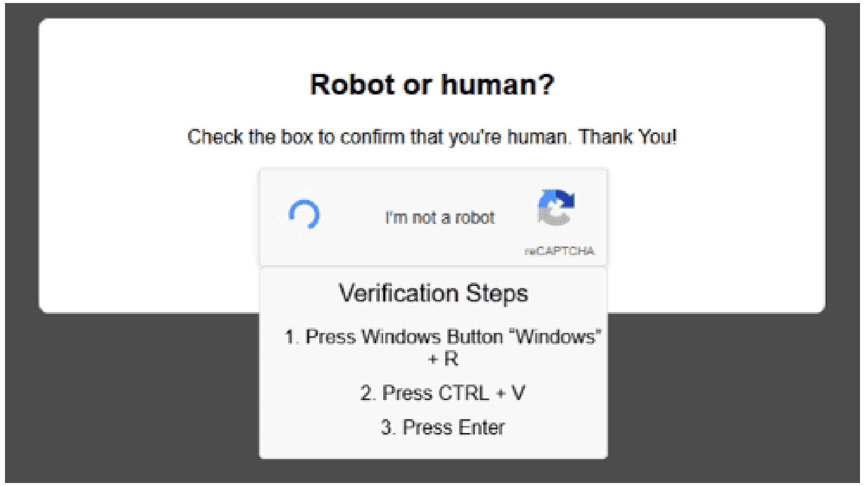
Ve

Please ve

Complete these Verification Steps

Please complete these steps to prove you are not robot.

1. Press & hold the Windows Key + **R**.
2. In the verification window, press **Ctrl** + **V**.
3. Press **Enter** on your keyboard.
4. Click **Verify** button below to finish.



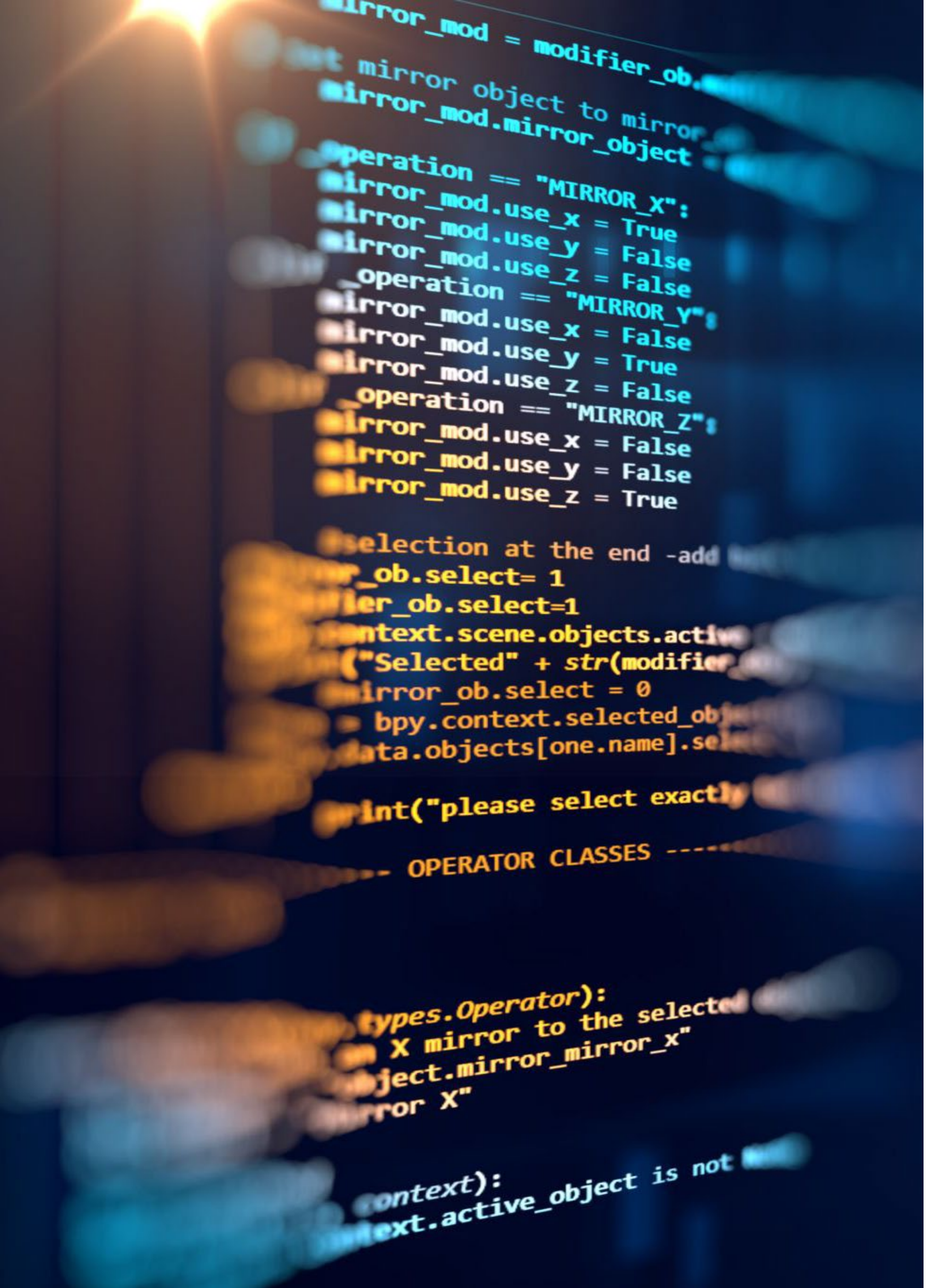
Robot or human?

Check the box to confirm that you're human. Thank You!

Verification Steps

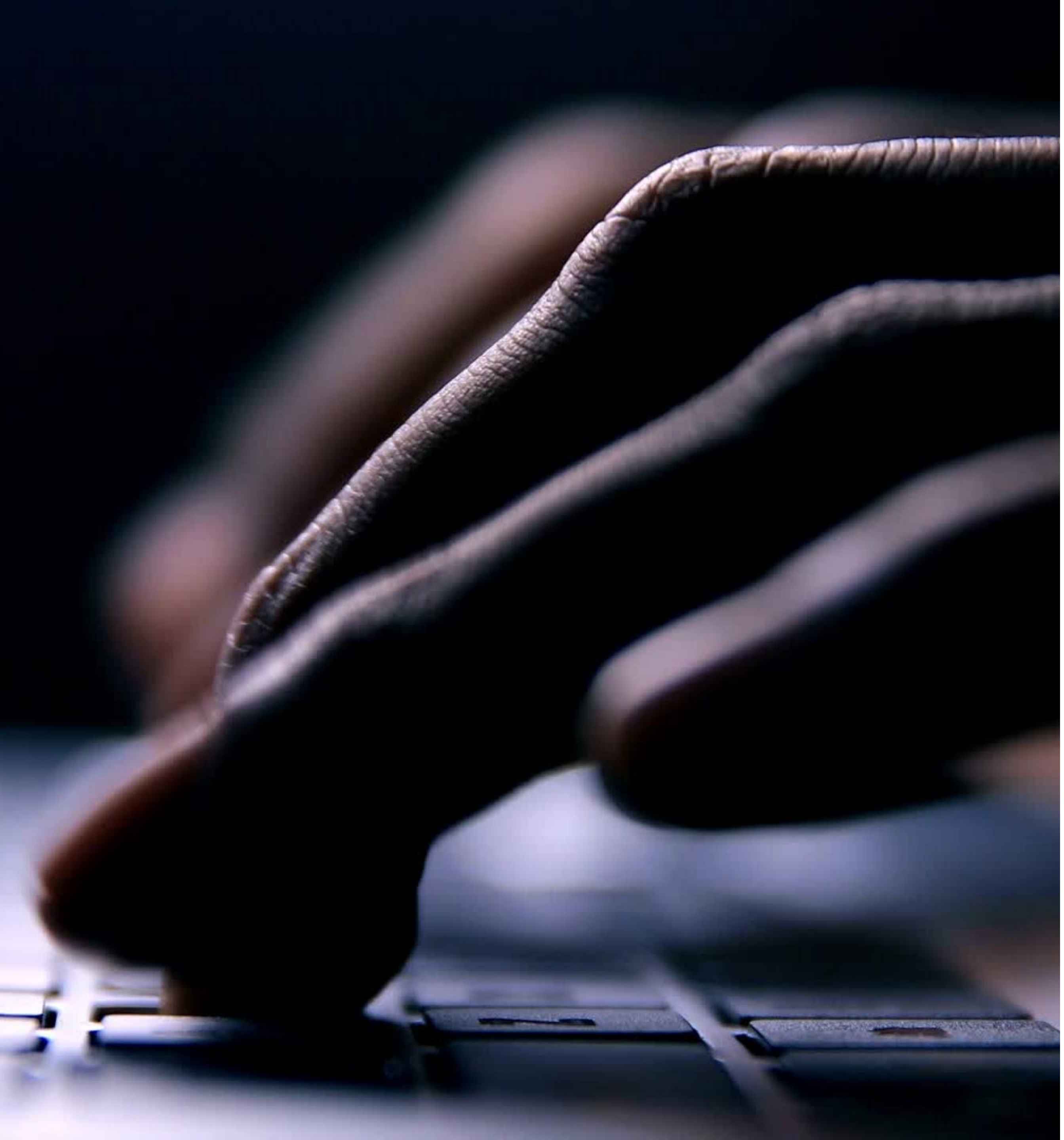
1. Press Windows Button "Windows" + R
2. Press CTRL + V
3. Press Enter

Keep yourself protected from Fake Re-Captchas



Avoid anything suspicious

- The run dialog, which is activated by hitting the keys Windows Key + R at the same time, shouldn’t be used often and legitimate websites don’t ask for this
- Validate the company’s website via a search engine and then manually type in the URL to visit the website. Scammers use slight differences to trick your eye and gain your trust
- Avoid sites with unusual domains



When browsing online, please strive to keep your personal and work lives separated

- In all of instances of these types of malware at the university, the leading cause of infections has been users from the university community using UofL devices to conduct their personal non-work Internet searches
- Applicable university policies:
  - ISO User Accounts and Acceptable Use
  - ISO Protection from Malicious Software

Ask permission before installing software

- It’s best practice to ensure you are not downloading software that the university already has, and you can use, or worse yet, getting your work computer compromised
- Contact your TierOne support staff if the software you need is approved by your department for use

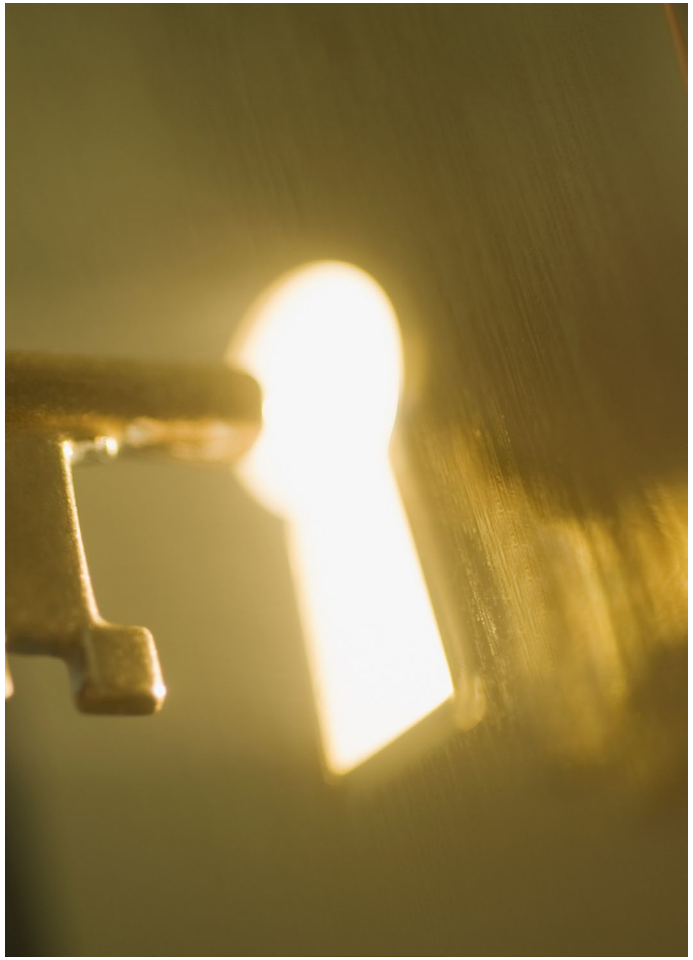
Avoid Pop-Ups

- Don’t click on pop-ups
- It’s best to err on the side of caution if your Spidey senses tell you something is off
- Close your computer and contact your TierOne support staff

Use university's approved antivirus software

- Ask your TierOne support staff what your options are and whether your computer is protected
- The University of Louisville employs Microsoft Detection for Endpoint for an antivirus tool and is automatically added to all workstations properly onboarded in our domain

Remove unnecessary privileges to your computer account



Does the account you use to login to your computer have local administrator privileges? If so:

Get with your TierOne support team and ask if you absolutely need this permission

Together, you and your department TierOne would be able to make that determination. Mutual understanding of the risks associated with maintaining local administrator access in your computer account should be established

Report suspicious activity

- If you encounter the Fake Re-Captchas, please contact the ITS Help Desk via phone at 502-852-7997, live Chat, walk-ins, or in our LiveChat
- Send an email to secureit@louisville.edu

Takeaways

- Please conduct your non-work related tasks at your personal computer
  - If you are using your personal computer to do UofL work, please send us an email at secureit@louisville.edu
- You have control. Follow the guidelines here to stay safe while browsing