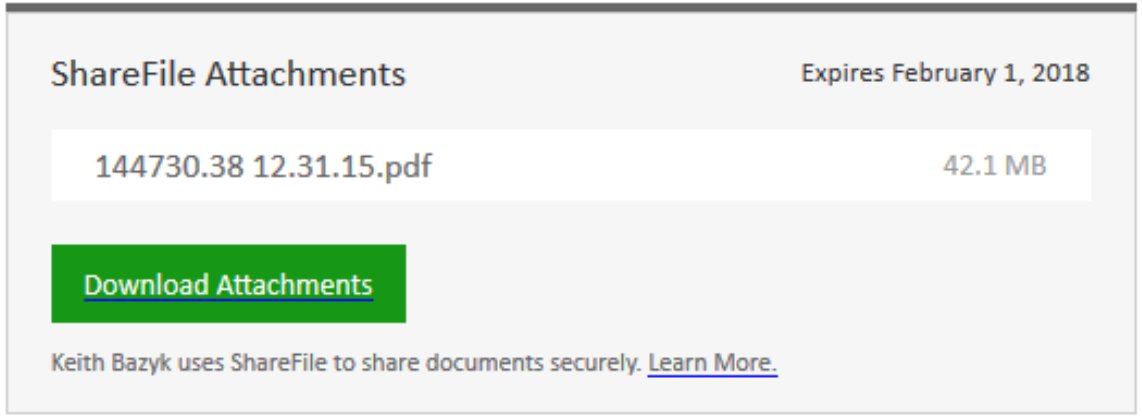
A Lesson on Phishing

- The following reviews the details of a most recent phishing attempt that targeted our domain

The message

From: Keith Bazyk [mailto:keith@genrub.com]
Sent: Thursday, January 18, 2018 10:41 AM
Subject: Document - (Invoice&Payment2.Pdf)



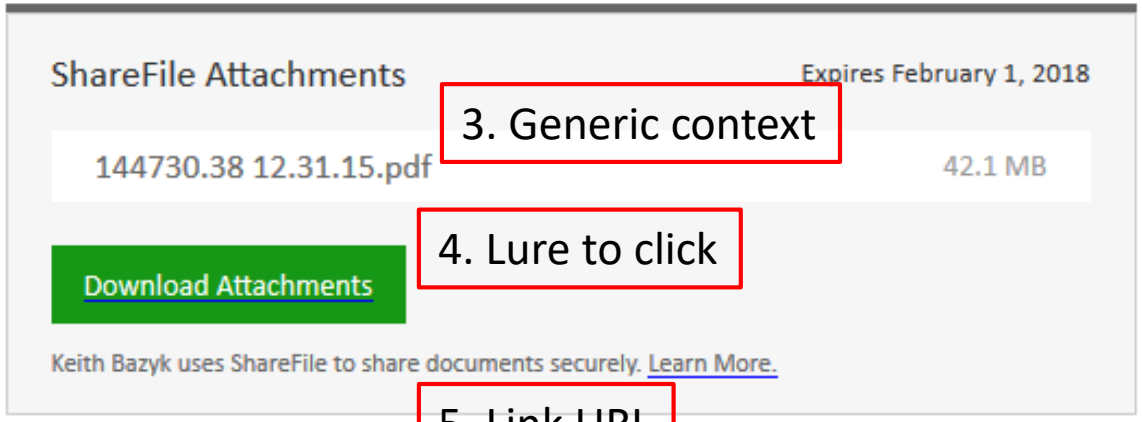
Keith A. Bazyk
General Rubber & Plastics
Bristol, TN
423-764-7126 office
423-383-4415 cell

The message: red flags

1. Don’t assume a trustworthy the sender

From: Keith Bazyk [mailto:keith@genrub.com]
Sent: Thursday, January 18, 2018 10:41 AM
Subject: Document - (Invoice&Payment2.Pdf)

2. Generic subject



3. Generic context

4. Lure to click

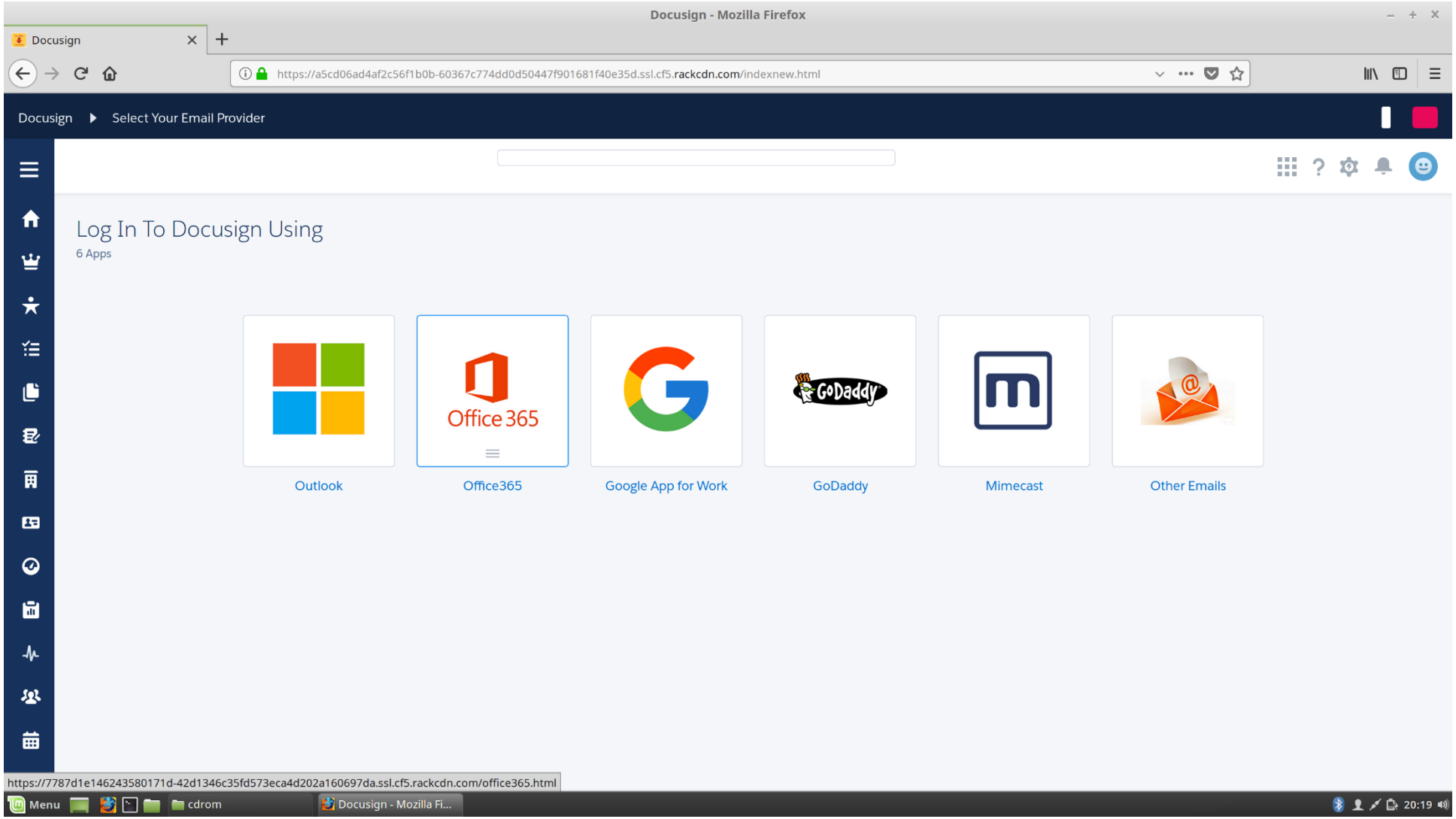
5. Link URL

https://a5cd06ad4af2c56f1b0b-60367c774dd0d50447f901681f40e35d.ssl.cf5.rackcdn.com/indexnew.html

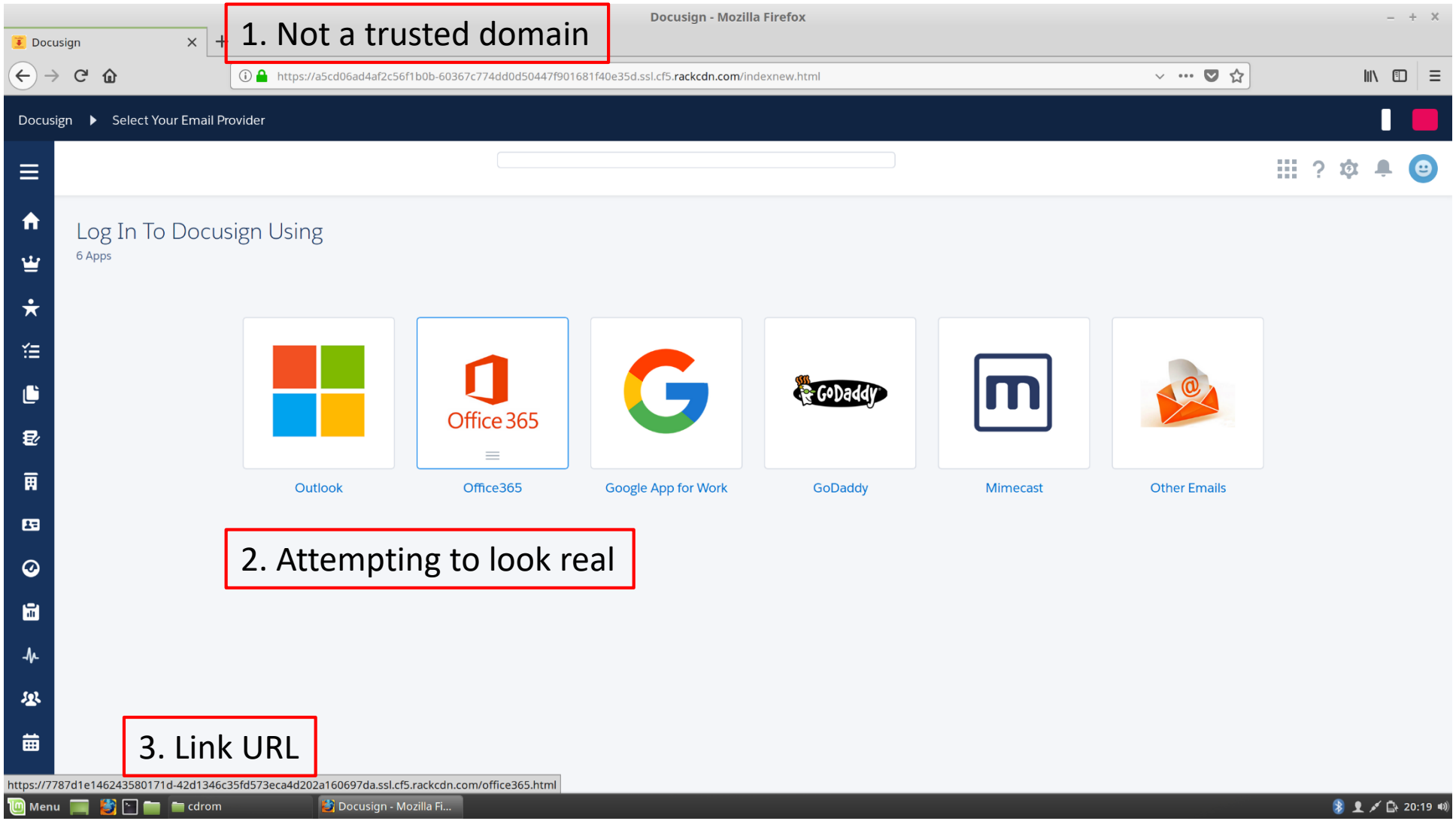
Keith A. Bazyk
General Rubber & Plastics
Bristol, TN
423-764-7126 office
423-383-4415 cell

Best action: delete or mark as spam

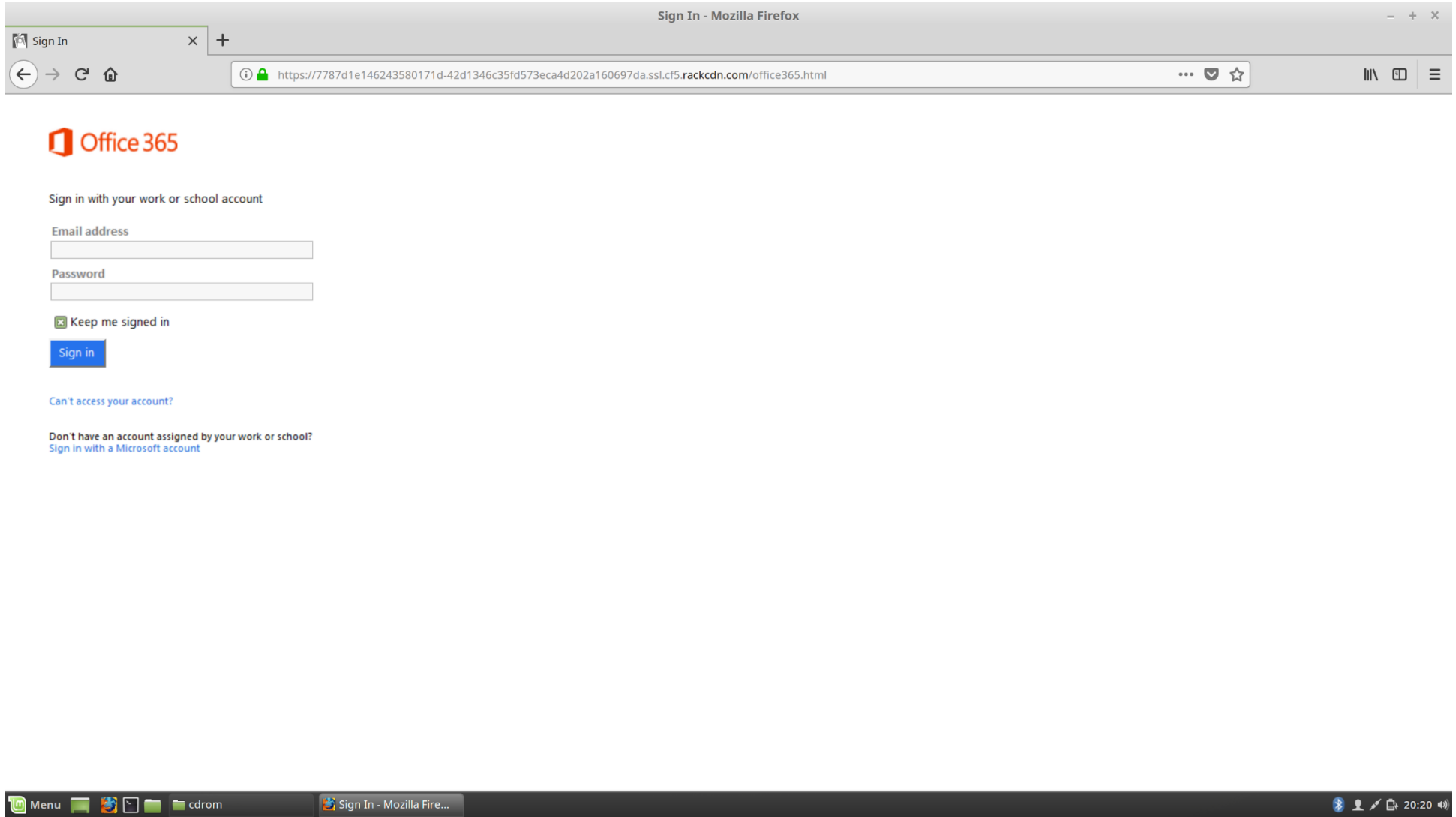
Site: falling for the lure



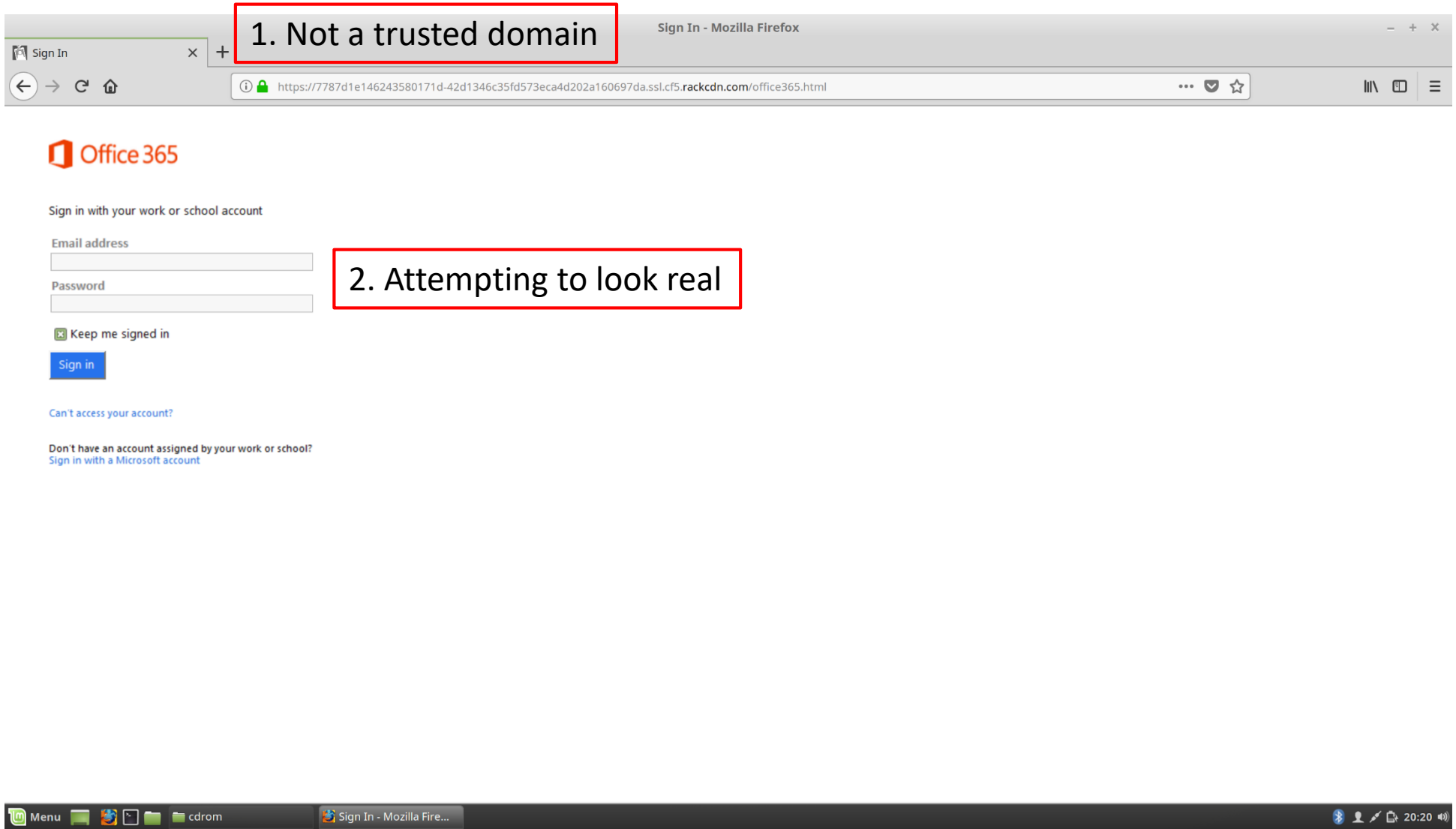
Site: red flags



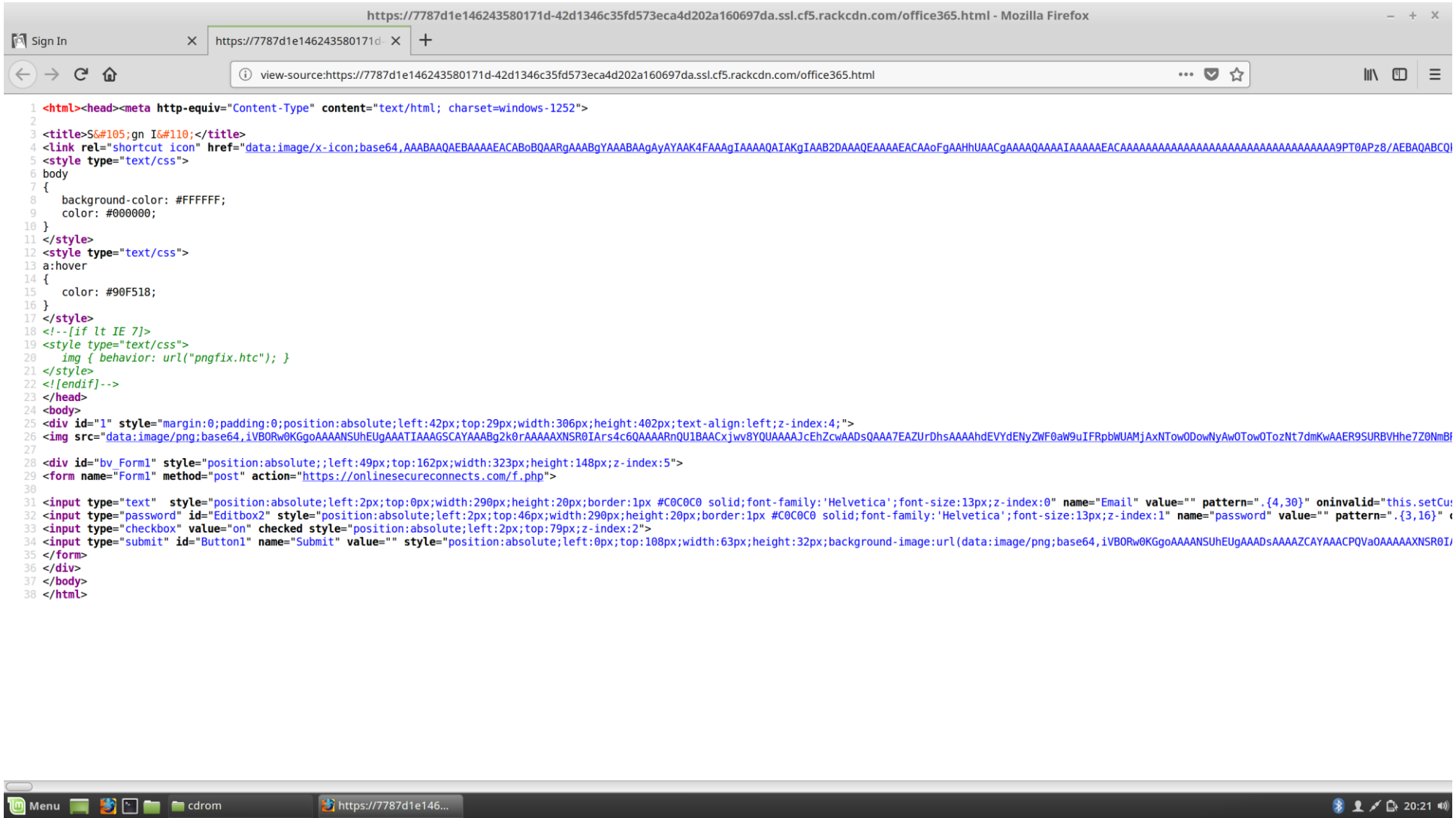
Site: falling deeper in the lure



Site: red flags



Site source code



Site source code: red flag

Takeaways

- If questioning
  - The sender
  - The content
  - Just delete/mark as spam
- Don’t login unless a trusted domain
  - spu.edu
  - office365.com
  - outlook.com