



Scamming for Education - IT&C 266 Final -

Samuel Jensen, Jonah Abbott, Ethan Fisher,
Vigo Miller



Our Project:

- Phishing is a problem.
- Everyone seems to know about it, yet everyone is still vulnerable
- So we designed a harmless demo using something we're all familiar with



Quick Overview

- Phishing: Fraudulent communication designed to dishonestly obtain information or money, or to convince victims to install malware.
- Phishing relies heavily on cognitive biases and logical fallacies
- This was all covered in class already, so we'll get to the good stuff...
- BYU housing email jumpscare warning

BYU Emails and Sign-in Pages!

to me ▾

Dear Student,

You have received a new message from BYU Campus Accommodations. please [sign in](#) to the housing website to read it.

With sincerest regard,

BYU Campus

Phone: 801-422-2611

Toll Free: 877-403-0040

Email: housing@buu.edu

reslife.byu.edu



BYU Emails and Sign-in Pages!

BYU Login

cas-byu-edu.org

BYU

BRIGHAM YOUNG
UNIVERSITY

By signing in, you agree to BYU Account [Terms of Use](#).

Sign in with Church Account

Sign in with another institution ▾

OR

Net ID

Password

Need help logging in?

Sign In



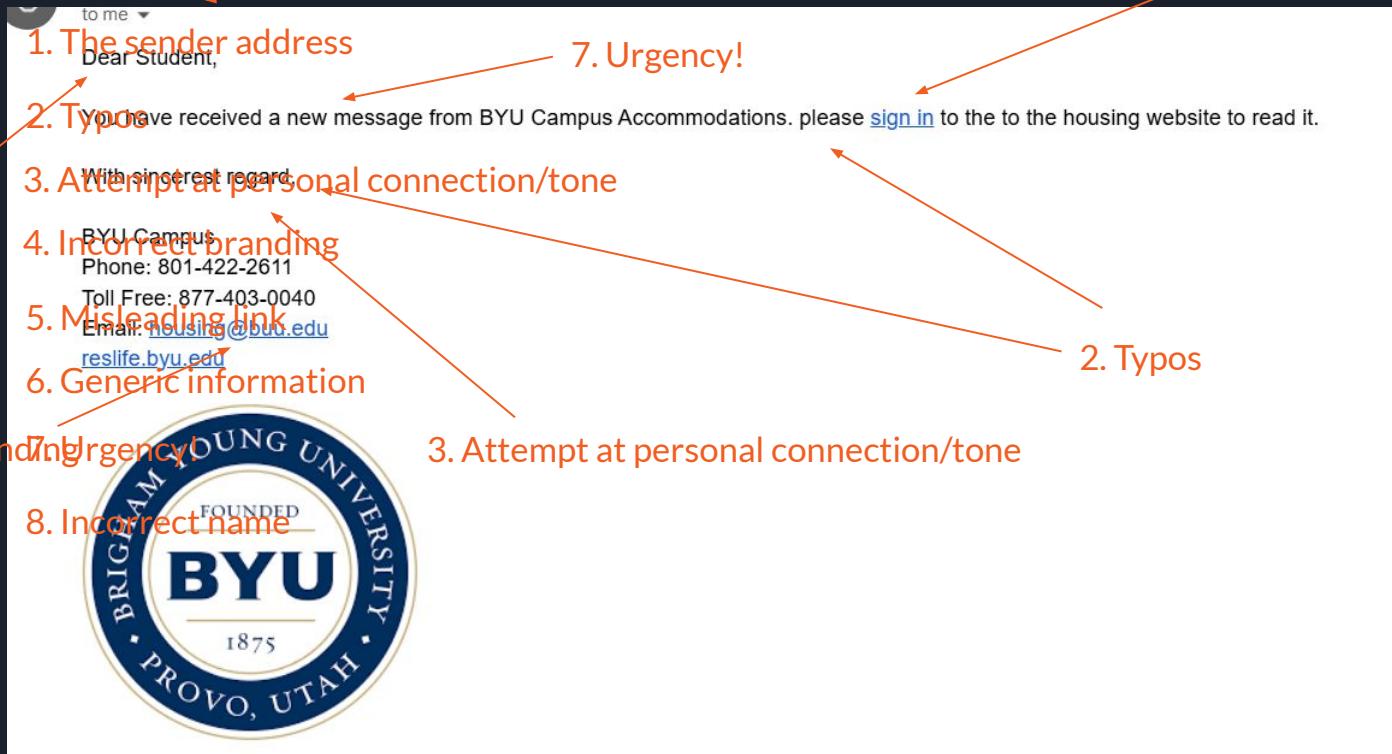
We love multi-factor authentication and fee reminders!

- Neither of those were real
- They were both (harmless) phishing attacks!
- In our demo, we hid several indicators of this within them for you to find



Demo Time!

1. The Email



2. The Website

The image shows a web browser window with a dark blue header. In the header, there is a 'BYU' logo and a 'Login' button. The main content area displays a Brigham Young University login page. The page has a dark blue background with white text. At the top, it says 'BYU' and 'BRIGHAM YOUNG UNIVERSITY'. Below that, it says 'By signing in, you agree to BYU Account [Terms of Use](#)'. There are two main input fields: 'Net ID' and 'Password'. Above these fields, there are two options: 'Sign in with Church Account' (with a key icon) and 'Sign in with another institution' (with a dropdown arrow). Below the input fields, there is a link 'Need help logging in?'. At the bottom, there is a blue 'Sign In' button. A large red box highlights the URL bar at the top of the browser, which is currently empty.

1. Incorrect (but close) URL

2. Lacking website functionality

3. Website is hosted in Iowa according to whatismyipaddress.com. Expected to be in SLC area, right?

4. Browser cache doesn't recognize this site, so passwords won't get filled in automatically.

1. Incorrect (but close) URL

2. Lacking website functionality

3. Website is hosted in Iowa...

4. Browser cache doesn't recognize



Application

- No phishing attempt is perfect, but some can be really good
- The tips we listed for identifying a scam are useful, but not comprehensive
- So, keep the following in mind...



If:

- Are any of the logical fallacies and cognitive biases we've learned about in class being exploited in a communication you're unsure about?
- Does this sender usually send communications like this?
- What does the sender want? Does that seem strange?
- Does * anything * seem unusual?



Then:

- Examine the communication before acting. Reach out to the sender through another means if it's important but you're unsure about if it's real
- Report the message as spam or phishing to your organization or email handler
- Avoid attachments and links
- If the malicious communication seems to have your name or other personal information, consider how they got it.



Questions?