GRAMBLING
STATE UNIVERSITY®

Grambling State University Faculty and Staff:
Subject: Phishing

Dear Gram Fam,

As October is Cybersecurity Awareness Month, we want to take a moment to share some important tips to help keep you safe online. In today's digital world, cybercriminals are constantly finding new ways to deceive and manipulate users into sharing sensitive information. One of the most common and dangerous methods they use is phishing—sending fake emails designed to steal personal or company data.

If you receive an email you believe to be a phishing, report it to the IT Department by clicking on the "report phishing" button. Never click a link directly that is received in an email, but rather, navigate to a new Internet Browser window to search the site's address. Each of you is an essential part of keeping our digital environment secure. Together, we can prevent cyber threats and ensure a safe, productive workspace.

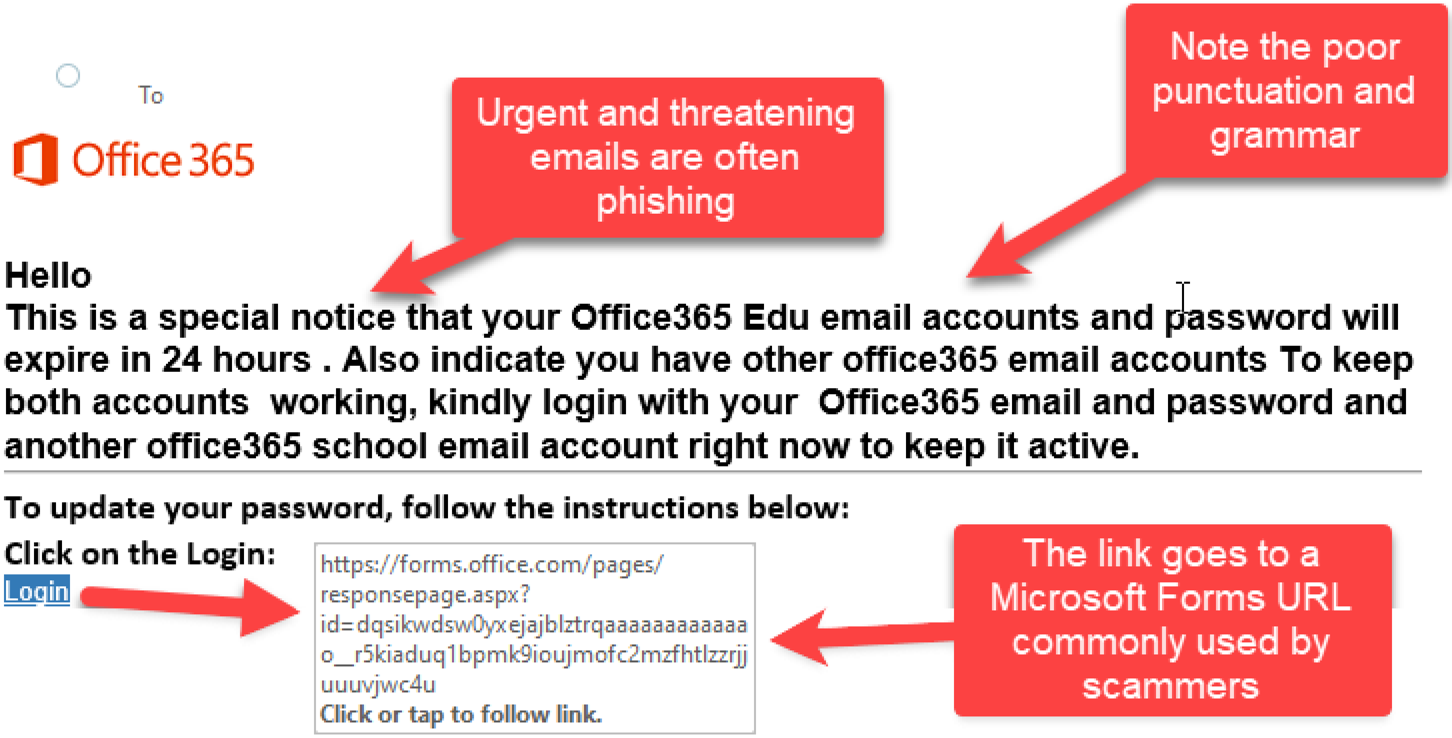
-Information Technology Dept

Here are some simple but effective **tips to help you spot and avoid phishing** attempts:

- **Hover Before You Click:** Before clicking any link in an email, hover your mouse over it to see the actual URL. If the URL looks suspicious or doesn't match the sender's domain, don't click on it.
- **Watch Out for Lookalike Domains:** Attackers often create fake domains that are very similar to legitimate ones, with slight changes like missing letters or altered characters (e.g., replacing an "l" with a "1"). Always double-check the URL for these subtle differences.
- **Beware of Out-of-Character Messages:** If you receive an email that asks you to do something unusual or unexpected, think twice before acting. It may be an attempt to trick you.
- **Sense of Urgency:** Phishing emails often try to create a sense of urgency or panic by claiming your account is about to expire, that you'll lose access to something, or that a package is undelivered. These tactics are designed to make you act quickly without thinking.
- **Know the Sender:** Just because an email appears to come from someone you know doesn't mean it's legitimate. Cybercriminals can spoof addresses or use compromised accounts to send malicious messages. Always verify any unusual requests, even if the email appears to come from a familiar name.
- **Change of Venue:** Be cautious of messages that ask you to switch the conversation to text messages. These are often scams. It might start with "Are you free?" and appear to come from someone you know, but once they move the conversation to text, it's easier for them to avoid our security measures. If in doubt, verify directly with the person through a trusted method.

GRAMBLING
STATE UNIVERSITY®

An example of a Phishing email:



○ To

Office 365

Hello

This is a special notice that your Office365 Edu email accounts and password will expire in 24 hours . Also indicate you have other office365 email accounts To keep both accounts working, kindly login with your Office365 email and password and another office365 school email account right now to keep it active.

To update your password, follow the instructions below:

Click on the Login:

Login

https://forms.office.com/pages/responsepage.aspx?id=dqsikwdsw0yxejajblztrqaaaaaaaaaaaao__r5kiaduq1bpmk9ioujmofc2mzfhtlzzrjjuuuvjwc4u
Click or tap to follow link.

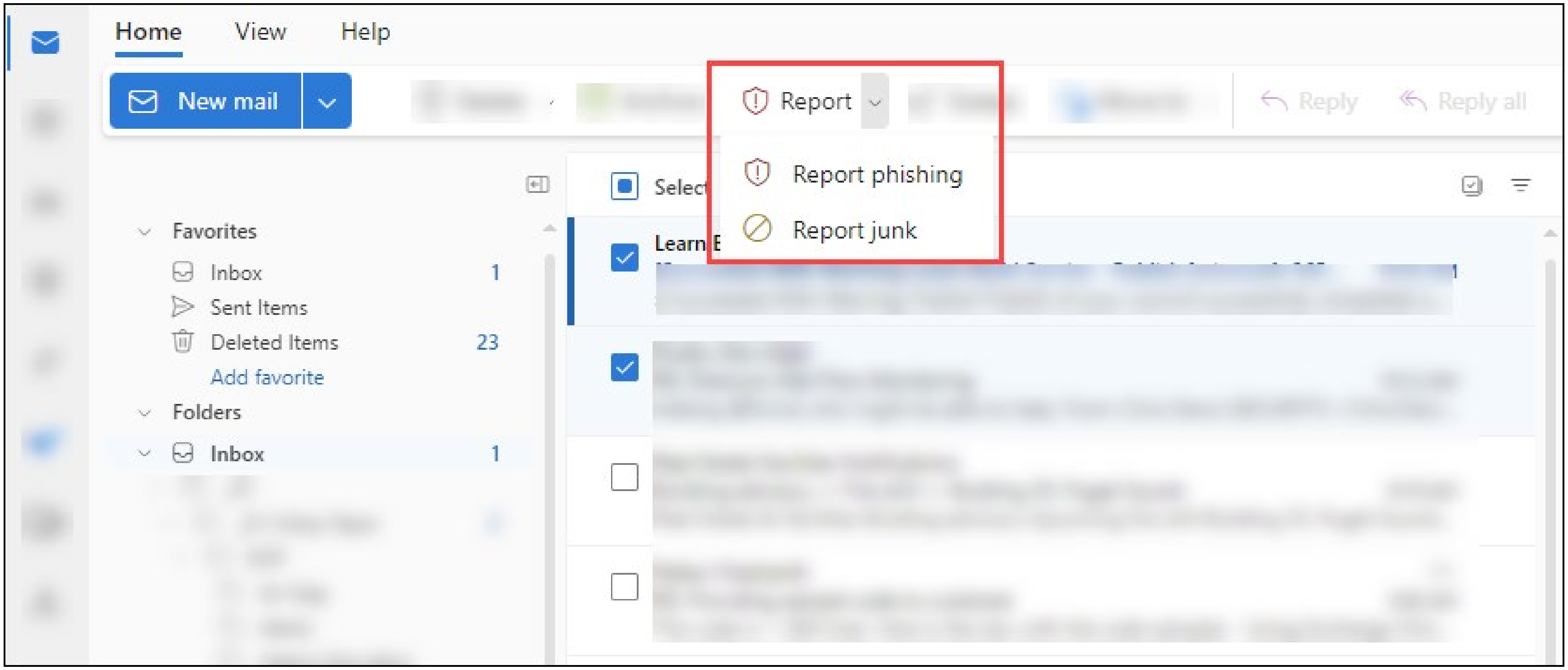
Urgent and threatening emails are often phishing

Note the poor punctuation and grammar

The link goes to a Microsoft Forms URL commonly used by scammers

GRAMBLING
STATE UNIVERSITY®

How to Report Phishing in Outlook:



Home
View
Help
New mail
Report
Report phishing
Report junk
Reply
Reply all
Select
Favorites
Inbox 1
Sent Items
Deleted Items 23
Add favorite
Folders
Inbox 1
Learn