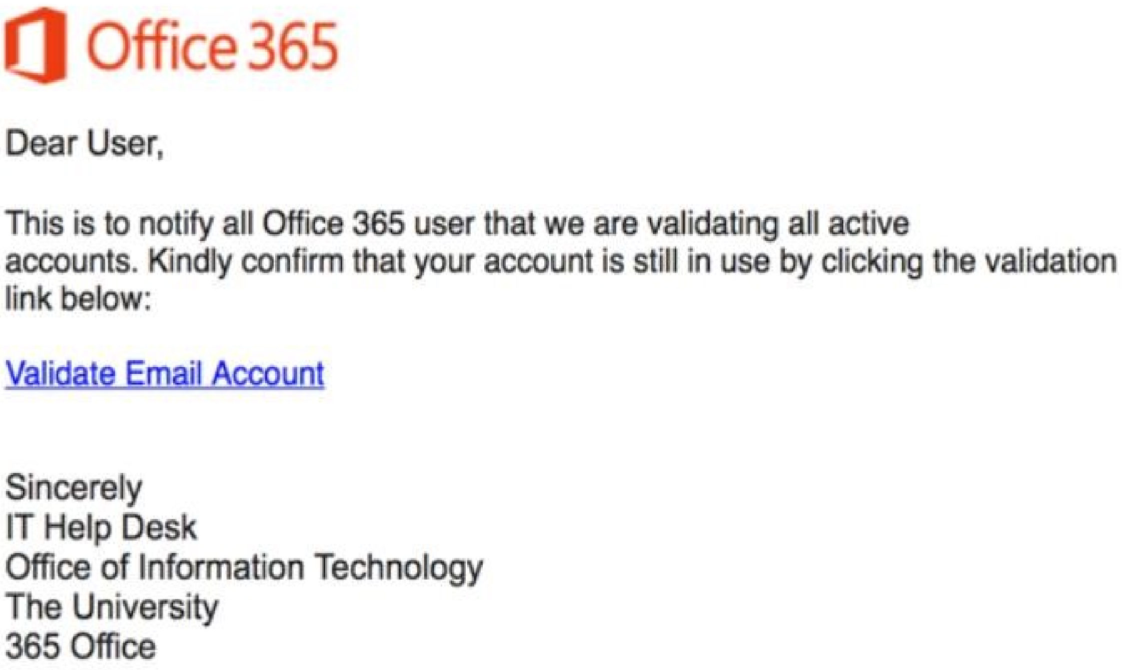
Cyber Security Awareness

SLC CYBER Security: timely information, you need to know …

Each year, the College receives hundreds of phishing attempts. Many of these are blocked, but some still sneak through. Below is a copy of a recent phishing attempt here at the College. Also below, is a list of things to look for to identify the phishing before you are lured in! Another thing to keep in mind here at the College, we will not send you requests for your information unless you email us first. And Microsoft should not be emailing you for account details either. Please keep an eye open for these types of emails. They are on the rise, and we want you to be protected!

CYBER Security: Phishing: a Recent Example



Office 365

Dear User,

This is to notify all Office 365 user that we are validating all active accounts. Kindly confirm that your account is still in use by clicking the validation link below:

Validate Email Account

Sincerely
IT Help Desk
Office of Information Technology
The University
365 Office

CYBER Security: Ways to identify the lure before you’re caught

1) **Pay attention to the spelling**

Often there are spelling mistakes with phishing lures. At first glance, it may seem ok but after rereading the email, they start to pop out at you. If you are having difficulty with an email you suspect could be a phishing attempt, copy and paste the text into a word document. Spell check will help identify many issues.

2) **Look for grammar mistakes**

Look again at the email above. Did you notice that it references “user” not “users” in the body of the email? The correct grammar and proper tense of words is another simple way to identify possible phishing lures. Again, you can use Microsoft Word to identify many of these errors.

3) **The signature gives away more than it should!**

How we sign every email tends to be the same, if we are using the signature feature in your email account. Here at the College we use them all the time. However, take a look at the example above, notice the issue? Microsoft would not be sending any account information emails from “The University”. In the future, read the signature just as carefully as the body of the email.

4) **Hover on the link**

Now this one is a little trickier. Not everyone will recognize a web address. If it is an address completely unrelated to the topic of the email, it may be a fake. Many links have the name of the company or an abbreviation for the company name in the address.

Now that you’re an expert in phishing lures … REACH OUT TO US! Let us know your top tips by tweeting us or mentioning us on FB!

For more topics on e-security click here.

Got a great idea for next month’s **SLC CYBER Security –** timely information, you need to know. Share it! Let us know here or tweet us using #SLCE-security.