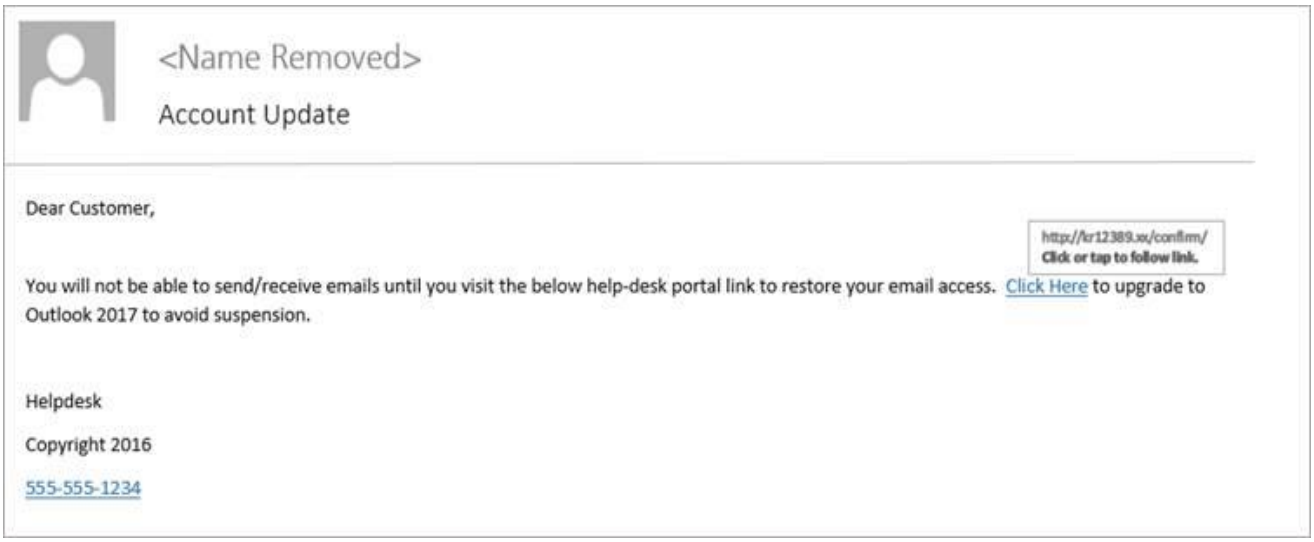
COT Security Alert – Phishing Emails, Diligence Needed

Continued diligence is needed from all users on the state email system so that falling victim to phishing emails is avoided. **Phishing** emails are emails that *appear* to be from a trusted source but which are *actually* sent by a malicious source for the purpose of gaining **personal** or **confidential** information, including user names and passwords.

Responding to a phishing email brings a significant negative impact and consequences to the responder, to their agency, to the email system, and to all state government business. This type of attack is popular among criminals because the malicious emails are often able to bypass technical security measures. Once the phishing email arrives in user inboxes, a response by a user is all that is needed to give the criminal success.

Example of a Phishing Email:



Phishing emails may have any or all of these characteristics:

- They may have misspellings and/or a generic greeting.
- They often use graphics, language, names or signatures of believable or legitimate business or government entities.
- They usually include a sense of urgency, such as making false claims about disappearing accounts or mailboxes.
- They usually appeal to human tendencies such as helpfulness, duty, or greed.

- They are **unexpected** and they direct the user to take an action against better judgment (click a link or attachment, complete a form with confidential information).

State government email users are reminded of the following:

1. Remember that the **appearance** of an email or website is **no indicator** of its legitimacy.
2. **Never** open attachments or click on links in unexpected or unusual emails, even if they are from someone you know.
3. Unexpected or unusual emails from known senders should be verified by contacting the sender to see if the email was sent intentionally, but **never** reply, forward or use information in the unexpected email. Always contact using information from other sources.
4. Hover over the links in emails to see the true destination.
5. **Remember** your password is **yours alone**. Enter your state credentials to gain access to state-managed services **only**.
6. Remember that senders of phishing emails may change elements of the email, such as link destinations or subject lines, to avoid updated filters and continue their malicious activity.
7. Remember that since the arrival of a phishing email cannot be predicted, these guidelines must be a continual practice.

Office of the CISO
Commonwealth Office of Technology
669 Chamberlin Ave., Frankfort, KY 40601
http://technology.ky.gov/CISO/