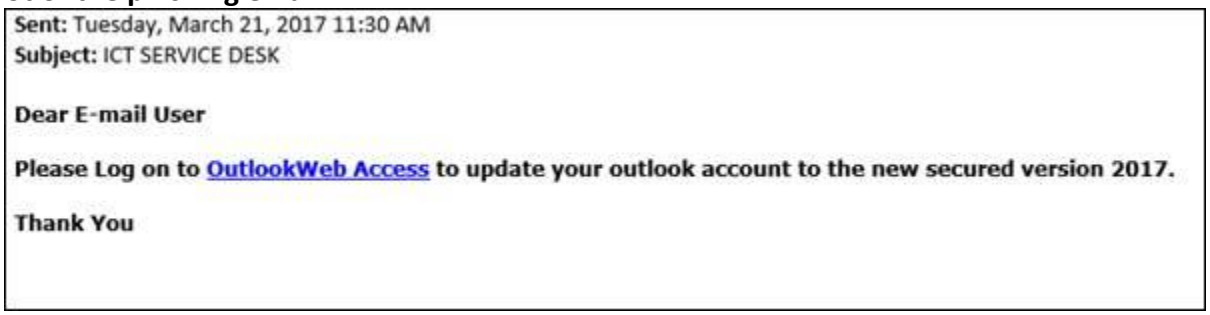
COT Security Alert – Phishing Email with Malicious Link

A number of state government employees have received a suspicious phishing email that looks like it comes from the service desk. **This is not from the Commonwealth Office of Technology.** Do not click on any link in this phishing email as your email account will be compromised and used to conduct further malicious activity.

Screenshot of the phishing email:


Sent: Tuesday, March 21, 2017 11:30 AM
Subject: ICT SERVICE DESK

Dear E-mail User

Please Log on to OutlookWeb Access to update your outlook account to the new secured version 2017.

Thank You

When state employees respond to phishing emails, this puts the entire Commonwealth of Kentucky email system at risk.

All state government email users are reminded of the following:

1. Never open attachments or click on links in unexpected or unusual emails, even if they are from someone you know.
2. Unexpected or unusual emails from known senders should be verified by contacting the sender to see if the email was sent intentionally.
3. Never reply or use information in a suspicious email to verify the sender. Always contact the sender in a separate email or by phone.
4. Hovering over the links in emails will reveal the true destination of the link.
5. COT will **never** ask for a user's credentials using any kind of online form or response to an email. COT does not need that information for any reason.
6. Remember that senders of phishing emails often make changes to the email, such as changing a link destination or subject line, in order to continue their malicious activity.

Notice: COT is providing this information so that you are aware of current security threats, vulnerabilities or preventive actions that may affect state government resources. If you suspect you have become victim to a security threat, please contact CommonwealthServiceDesk@ky.gov.

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