COMMONWEALTH
OFFICE OF
TECHNOLOGY

COT Security Alert – DocHub Phishing Email

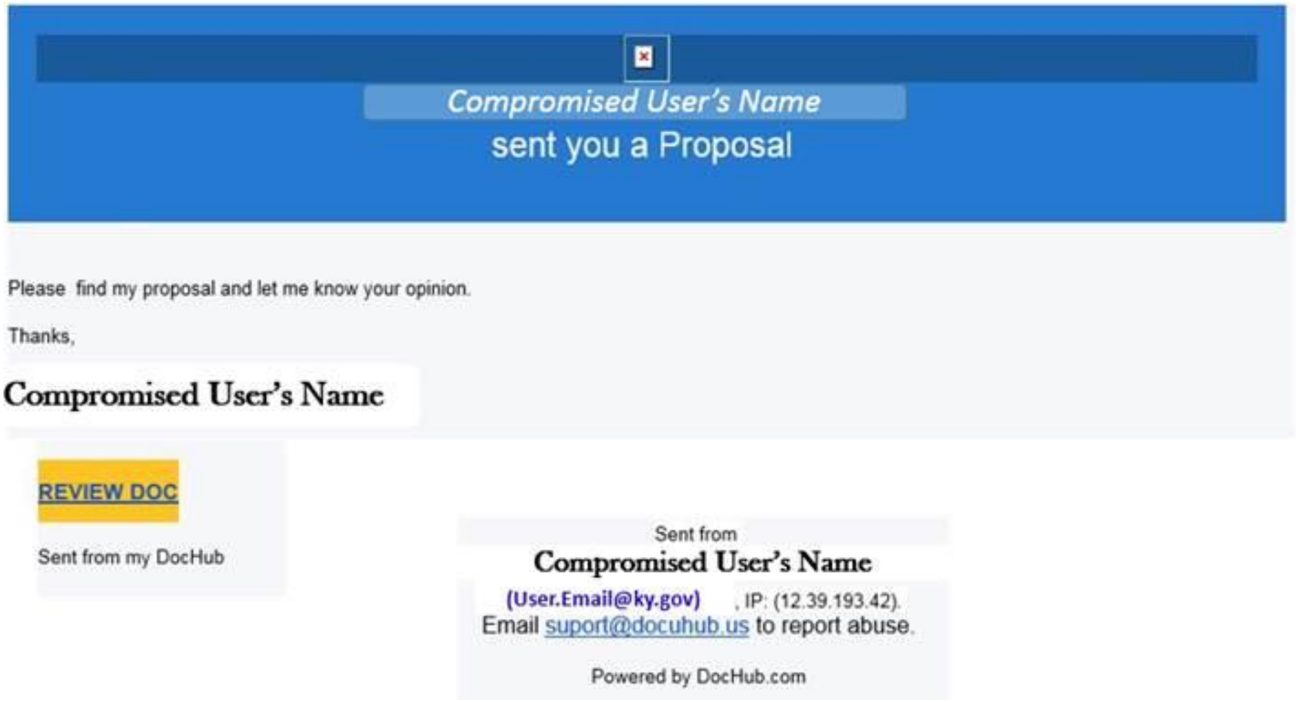
State inboxes are receiving phishing emails that present themselves as containing a DocHub document link from a valid state employee. If a user responds to this email, their account is compromised and used to send out more phishing emails resulting in more compromised email accounts.

COT security and technical staff are aware of this phishing attack and are taking measures to mitigate its effectiveness on our network, but all email users must be diligent. **User's should not respond to this email in any way. If received, this email should be deleted from the Inbox and then deleted from the Deleted Items mailbox immediately.**

The emails from this attack have these characteristics.

1. They will be from a state employee whose account is compromised and whose name is used throughout the email.
2. The email subject may be something like "*State User* Sent you a Proposal via DocHub FYI" (name redacted).
3. The email contains some misspellings and spelling inconsistencies.
4. This is an **unexpected email**.

This is a redacted sample:



Compromised User's Name
sent you a Proposal

Please find my proposal and let me know your opinion.

Thanks,

Compromised User's Name

Sent from my DocHub

Sent from
Compromised User's Name
(User.Email@ky.gov) , IP: (12.39.193.42).
Email suport@docuhub.us to report abuse.

Powered by DocHub.com

Users should be aware that changes to this email may be implemented by the phisher at any time in order to continue the phishing campaign. Caution in opening and responding to email should be practiced at all times.

Always use these guidelines when reviewing email:

- Remember the **appearance** of an email or website is **no indicator** of its legitimacy.

- **Never** click on a link in an unexpected or unusual email, even if it is from someone you know. The apparent sender’s account could be compromised.
- If you receive an unexpected or unusual email and believe it may be legitimate, verify by contacting the sender directly (preferably by phone or in person), but **never** by replying to the email or using contact information it contains.
- **Never** respond to an email in any way with logon credentials. Credentials should be entered only as credentials to directly access their own applications or devices.

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
Frankfort, KY 40601
http://technology.ky.gov/CISO/