COLUMBUS STATE UNIVERSITY
UNIVERSITY INFORMATION & TECHNOLOGY SERVICES

Phishing Alert - Google Docs Campaign

On 5/3 a phishing campaign designed to trick users into granting access to their Google account was observed.

DATE: 5/4/17

SUBJECT: Google Docs Phishing Campaigns

SUMMARY: On May 3, 2017, several sources reported a Google Docs phishing email campaign. The details of the attack are as follows:

- The affected users received an email that appeared to be from a contact offering to share a Google doc.
- Clicking the link in the attacker's email directed the user to the attacker's application, which falsely claimed to be Google Docs and asked for access to the user's account.
- If the user authorized the application, it accessed the user's contacts for the purpose of sending the same message to those contacts.
- This access only retrieved contacts and sent the message onward—customer data such as the contents of emails and documents were not exposed.

Upon detecting this issue, Google immediately responded with a combination of automatic and manual actions, including removing the fake pages and applications, and pushing updates through Safe Browsing, Gmail, and other anti-abuse systems.

RECOMMENDATIONS: If you received this email, clicked on the link and authorized permissions on your Google account:

1. **Reset your password on a machine that was not infected. Here is Google's guide for creating a strong password.**
2. **Google should have automatically revoked permissions related to this phishing attack. However, the user should still review all permissions at this time. You can do this here.**
3. **As a reminder, do not open suspicious emails or attachments, or follow suspicious links, as they may contain malware.**

Source: Google Docs