

****ALERT****

NEVER GIVE OUT your passwords or your Microsoft Authenticator App codes to ANYONE, especially if they are claiming to be IT Support or Blackboard Support!

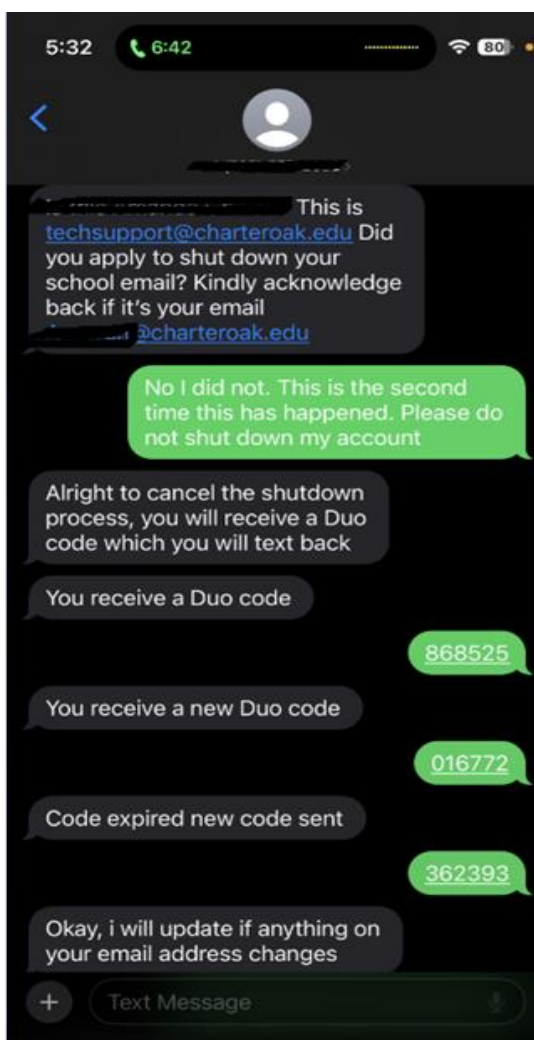
It happened to one of our users whose account was compromised by a malicious actor who used a phish email posing as Charter Oak Tech Support to obtain phone number and password from that user. Once the malicious actor got their passwords, sprayed thousands of other phishing emails both within and outside the COSC email system.

Here are the examples of the incident:

The screenshot shows a phishing email from Charter Oak State College. The email body contains a form titled 'Charter Oak State College| Microsoft365 Validation'. The form asks for the following information:

- Full Name *
- Phone Number *
- myCOSC User Email address *
- myCOSC Passphrase (Protected by Admin) *
- Email Of Former University/College You Once Attended *

A 'Sign in to continue' pop-up is displayed over the form, asking the user to sign in to fill out the form. The pop-up also includes a 'Report Abuse' link and a 'SIGN IN' button.



Please **call Blackboard Support at 844-889-9725** if you get this and they will help you to prevent from happening. Thank you!