


## Phishing Example Superintendent/President Shared a File

**From:** Ms. Katrina Shantell Foster <[no-reply@sharepointonline.com](mailto:no-reply@sharepointonline.com)>  
**Sent:** Wednesday, August 19, 2020 7:59 AM  
**To:** <lots of us>  
**Cc:** Ms. Katrina Shantell Foster <[ksfoster@albertus.edu](mailto:ksfoster@albertus.edu)>  
**Subject:** Ms. Katrina Shantell Foster shared "Faculty.Doc" with you.

**Always Question Non-SWC Email**




**Ms. Katrina Shantell Foster shared a file with you**


**Inconsistent Sharing Name**

Kindred Murillo has share a file with you

**Typo**

 [Faculty.Doc](#)

**These Links Would Get Your Password!**

 This link will work for anyone.

[Open](#)

In the example above, there are a few things that don't look quite right:

1. The email is from a non-SWC email address – that's always a red flag when receiving these kinds of email.
2. There are inconsistent names being used as the person who shared the file – did Katrina share it or Kindred?
3. There is a typo on a supposed system-generated email; tech companies do not make typos like that!

If the person who received this email clicked on one of the links, he/she would've been asked to enter a username and password. Nothing would've happened after that, except for the username and password silently being saved on the back-end of the form.

**Be smart – do not fall for it!**