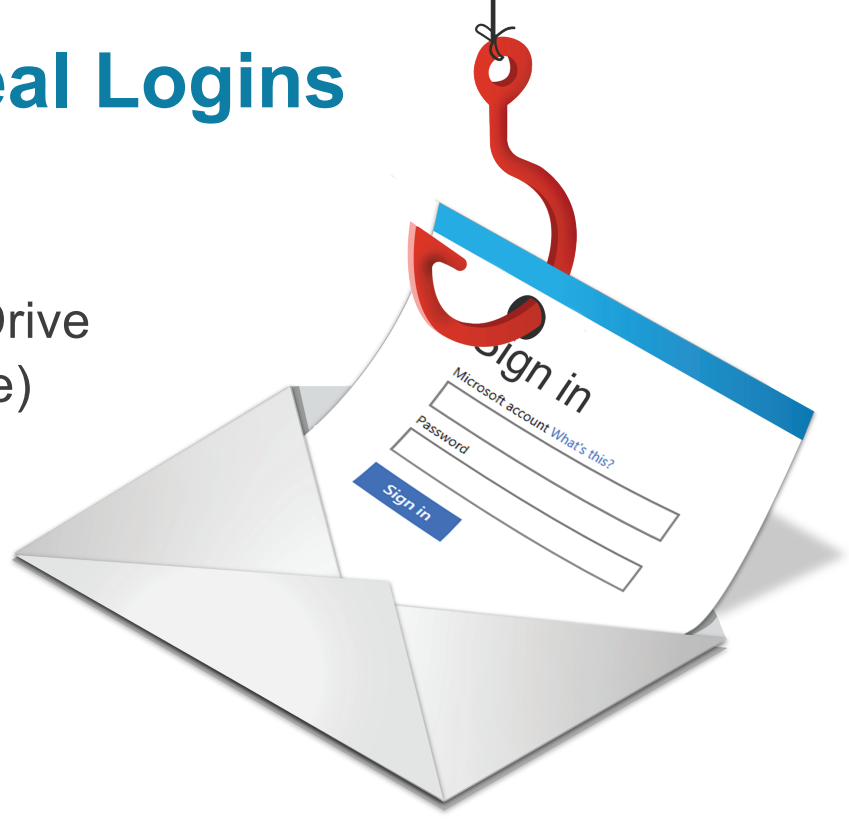
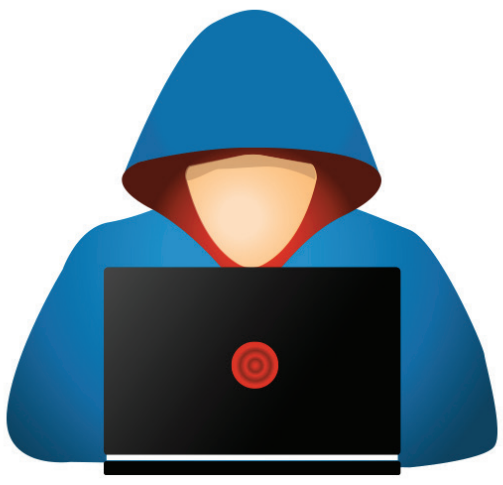
AttackSpotlight

Fake OneDrive Emails Steal Logins



OneDrive Users Remain At Risk

Attackers are sending fraudulent Microsoft OneDrive emails with links to an authentic-looking (but fake) OneDrive login page designed to steal your credentials. Once attackers have your OneDrive username and password, they can do real harm to you or your organization.



They might try to:

Reuse your password to access other accounts.

Collect sensitive data about you or your company.

Use your account to trick others into giving up sensitive information.

What do I look for?

There are multiple variations of this phish.
Here is one example.

DS

Dr. Stacy Jones <noreply@onedrive.onlinedocshare.com> ❶
Dr. Stacy Jones has shared a document with you.
Friday, January 11, 2019 at 1:25

OneDrive for Business

Hello,

❷ You have a file shared tagged “Paper Work” sent from Dr. Stacy Jones.

Kindly review the document asap and let me know if you have any questions.

View Document

Warm Regards,

Dr. Stacy Jones

https://www.onlinedocshare.com ❸

❶ Examine the Sender

The sender’s address includes the word ‘onedrive’ to fool you.

But look closer. The email is really from onlinedocshare.com, not OneDrive.

Don’t be fooled by domains that include brand names.

❷ Content in Context

Is this expected? Be careful with unexpected invitations to view or download documents, even when they look legitimate.

Scammers often research to find businesses and people familiar to you.

❸ Examine the Link

Examine the link. While the url uses a secure connection **(https://)**, this doesn’t mean the site is legitimate.

Examine the URL in the hover text. This link sends you to onlinedocshare.com, not OneDrive.

How do I protect myself?

If you receive an invitation to open or download a OneDrive file:

Don’t immediately interact with the email.

Take your time to evaluate it.

Decide on an action to take:

Looks legitimate: Verify it with the sender. Don’t reply directly to the email. Use another means of communication.

Looks suspicious: Report it to the appropriate team in your organization.

proofpoint
Security Awareness Training