Keystone
TECHNOLOGY CONSULTANTS

Cybersecurity Tips and Reminders

This Month's Focus- O365 Credential Phishing!

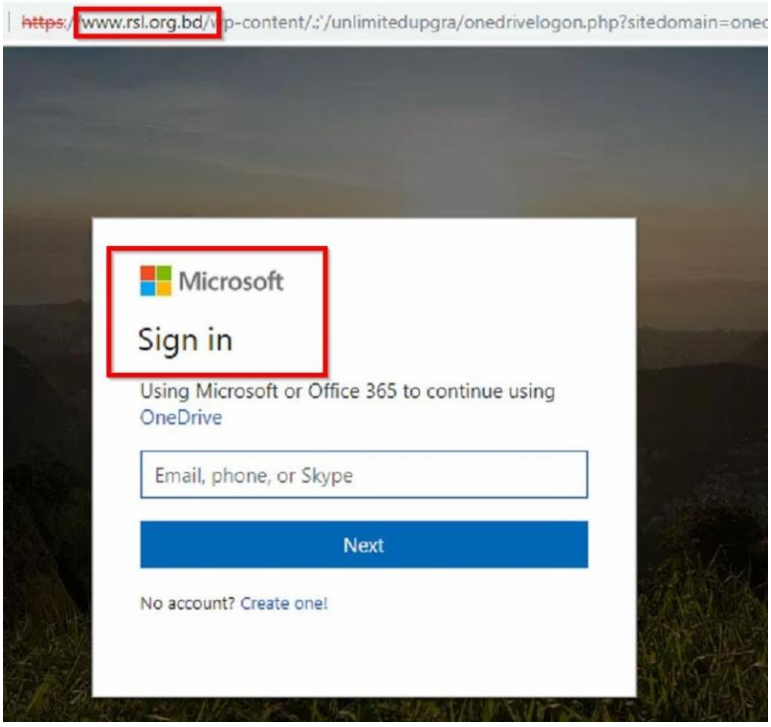
Hackers will often send spam messages that are phishing for user's Office 365 username and password. The email may come in many forms asking you to sign into your account online. It may say your account is going to expire, it may say you have a message waiting for you, it may say there is suspicious activity on your account. It provides a link that takes you to a website that looks almost identical to the Office 365 sign in page. Above is an example going to web address hxxps://www.rsl.org.bd which is definitely not a Microsoft website. The sign in page for Office 365 is **https://login.microsoftonline.com**.

If a phishing victim were to enter their email address and Office 365 password on one of these fake Office 365 sign pages, it essentially gives the hackers access to the victim's mailbox.

Send me more info

Be Suspicious. Something is not Right.

They can go online, sign into the victim's mailbox, download all the email, and even create rules to forward any new emails to another email address. All this without the victim knowing.



If you receive one of these emails asking you to go online to sign into your Office 365 account, ask us to review it first. Or if you end up on a page that looks like the Office 365 login page but the web address is **NOT https://login.microsoftonline.com**, close the page and carry on with your day.

Any Questions?
Please respond to this email if you have questions, comments, or desire more information.