



FEDERAL MINISTRY OF
COMMUNICATIONS AND
DIGITAL ECONOMY, NIGERIA



CERRT.NG

PHISHING ATTACK BEING USED TO STEAL MICROSOFT 365 USER CREDENTIALS



NCA-030423-01

Overview

A phishing campaign has been targeted towards Microsoft 365 users. In this campaign, cyber criminals send malicious email to users with malicious attachment embedded in it, with the intention of harvesting user credentials. The attachment tends to have 2 extensions (.pdf and .html).


Impact

When a user opens one of these malicious HTML files, a phishing page masquerading as Microsoft 365 is displayed that prompts users to input their login credentials. Once the victim inputs their credentials, they get sent to the attacker who harvests them for malicious purposes. There is a high possibility that the hijacked account belongs to a corporate user because Microsoft 365 is widely used by businesses. As a result, if the attacker gets their hands on these credentials, they may be able to get their hands on sensitive information.

Preventive Measures

- Verify the sender's email address to ensure it matches the official domain it claims to be from.
- Pay attention to spelling and grammar mistakes, as well as poor formatting.
- Before clicking on links on emails, hover your mouse cursor over the links to see the actual URL. If the link's destination looks suspicious, do not click on it.
- Beware of emails that claim your account is at risk or that require urgent verification of personal information. Any statement meant to create a sense of urgency should be suspicious.
- Never click on links or download file attachment from unknown senders.

For further enquiries, please
contact **CERRT.NG** through
the following channels:

 cerrt@nitda.gov.ng

 +234 817 877 4580

 www.cerrt.ng