UNISPHERE SOLUTIONS

info@unisphere.co.nz
www.unisphere.co.nz

CYBER GUIDANCE ISSUE 00084

FAX ALERT EMAILS PHISH MICROSOFT OFFICE 365

DATE ISSUED: 21st December 2020

IMPACT	LOW	MEDIUM	[✓ HIGH]
EASE OF EXPLOIT	HARD	MEDIUM	[✓ EASY]

OVERVIEW

Emails sent from legitimate, but compromised accounts to users containing documents that simulate an eFax is the latest phishing campaign effort to steal Microsoft Office 365 credentials

BREAKDOWN

Hundreds of recently compromised accounts in conjunction with novel URLs designed to bypass traditional threat intelligence solutions are being used in a phishing campaign aimed at stealing Microsoft Office 365 user credentials. The emails impersonate a legitimate user using their compromised email account and contain an electronic fax document with a clickable attachment or button containing a malicious link. These emails and landing pages are well crafted to appear authentic and the URLs are hosted on a number of sites including Weebly, Joom and Quip. After clicking, the user is taken to the landing page to enter their credentials for harvesting.

REMEDIATION STEPS

- These emails are difficult to detect so users should proceed with caution, particularly in instances where an eFax is not expected. If in doubt, don't click the link and report to your internal phishing and security team.
- Never enter login credentials when prompted through email links, always type the known URL to the address bar of your browser to log in.

REFERENCES & RESOURCES

Threatpost:	https://threatpost.com/microsoft-office-365-credentials-attack-fax/162232/