UNISPHERE SOLUTIONS
info@unisphere.co.nz
www.unisphere.co.nz

CYBER GUIDANCE ISSUE 00033

PHISING FOR MICROSOFT CREDENTIALS

DATE ISSUED: 6th September 2020

	LOW	MEDIUM	HIGH
IMPACT			✓
EASE OF EXPLOIT		MEDIUM	HIGH

OVERVIEW

Attackers seeking to steal Microsoft Outlook credentials have launched a new phishing campaign that uses overlay screen tactics to lure in victims under the guise of legitimate sites.

BREAKDOWN

Leveraging email quarantine policies and internal company support, emails imitating the technical team were circulated to staff claiming the recipients were required to take action in the subject line. Claims that they were from the email security service and were holding emails in a quarantine and preventing them from reaching the users inbox, suggesting that the user should review and retrieve them as necessary, otherwise they would be deleted after three days. Should a user click on the email, they were prompted with an overlay screen and a request to log in, sending their credentials to the attacker. The link supplied appeared suspiciously long and once clicked, utilises specific parameters to determine which web page to pull and place their overlay on top of. The attacks were also noticeably targeted towards each organization as the link also populates the address of the original email recipient.

REMEDIATION STEPS

- Practice caution when dealing with links and attachments – particularly ones that ask you to log in
- Educate all users on how to spot a phishing email
- Use URL filtering to restrict access to known malicious sites.

REFERENCES & RESOURCES

Threatpost: https://threatpost.com/attackers-steal-outlook-credentials-overlay-screens/158969/