



proofpoint.

HOW TO STOP YOUR MICROSOFT OFFICE 365 USERS FROM GETTING HOOKED BY **CREDENTIAL PHISHING**

Today's attacks target people, not just infrastructure. As more people work through Office 365 and the cloud, credential phishing is an effective way to target them. These attacks don't use malware, and are hard to block with traditional defenses.

DEADLIEST CATCH

Credential phishing is effective.



95%

of the time, attackers use email to connect with their targets.¹



80%

of breaches involve compromised or weak passwords.²

GETTING GOOD BAIT

Thanks to open sharing on social media, trawling for personal data online is easy. Convincing lures and shortened URLs can trick even well-trained employees.



REELING THEM IN



Nearly **50%** of users open e-mails and click on phishing links within an hour of receiving them.³



Many people blindly authorize third party apps with access to their Office 365 environment.

PROTECTING YOUR PEOPLE

You need a security solution to stop phishing lures before they reach your Office 365 inboxes and a way to protect your cloud assets in Office 365 and beyond.

Look for a solution that:

Has proven capabilities to block phishing emails using predictive URL sandboxing and webpage analysis to keep your end-users safe

Informs a user's risk profile if exposed to phishing or malware

Automates response actions, such as step-up authentication, to protect data in Office 365 and other SaaS apps



See what your defenses are missing – learn more at www.proofpoint.com/office365

¹ Verizon. "Data Breach Digest." April, 2017

² Verizon. "2016 Data Breach Investigations Report." April 2016.

³ Proofpoint. "The Human Factor 2017." May 2017

proofpoint.