Hiding in Plain Sight

You can train people to be skeptical before they click, but sophisticated social engineering techniques can snare even savvy users. URLs in emails are easily masked, and the sites they link to can change over time. Here’s what makes URLs so hard to unmask:

- 42% of clicks on malicious URLs come from mobile devices, where the full URL can be hard to make out.
- URL shorteners such as bit.ly make unmasking the URL even trickier.
- URLs may be hiding in encrypted attachments.
- URLs to pages often contain malware, sometimes after delivery.

The clicks keep on coming

The longer a malicious URL sits in the inbox, the more likely it will be clicked. Document-sharing lures are consistently effective. URLs often link to malicious /files in Google Drive, Adobe Creative Cloud, and Dropbox. Top click rates include:

- OneDrive
- Phishing: 11%
- Microsoft Excel Online Phishing: 2.8%
- Microsoft OWA Phishing: 13%
- SharePoint Online: 14%
- Adobe Creative Cloud: 26%
- Dropbox: 2.8%
- Top click rates happen within 25% of clicks happen within 90%

Sharing is Scaring

Document-sharing lures are among the most effective attacks. Office 365 users often receive emails from untrusted sources that look like legitimate office documents or files. Top click rates:

- Click-thru rate: 10%
- Click-thru rate: 60%

Connect with Confidence

Take a proactive, real-time, multilayered approach to unveil and stop attacks before they reach your Office 365 users. Respond effectively with actionable insight. Proofpoint protects across email, OneDrive for Business, SharePoint Online, Skype, and even SaaS applications beyond Office 365.

To learn more, visit www.proofpoint.com/office365