

HUMAN NATURE:

# HOW ATTACKERS TARGET PEOPLE THROUGH MICROSOFT OFFICE 365



Today's attacks target people, not just infrastructure. As organizations migrate to the cloud, attackers are finding new ways to target them. Malicious URLs sent to Office 365 users have become an increasingly effective method of attack.

## 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 make 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 makes unmasking the URL even trickier.



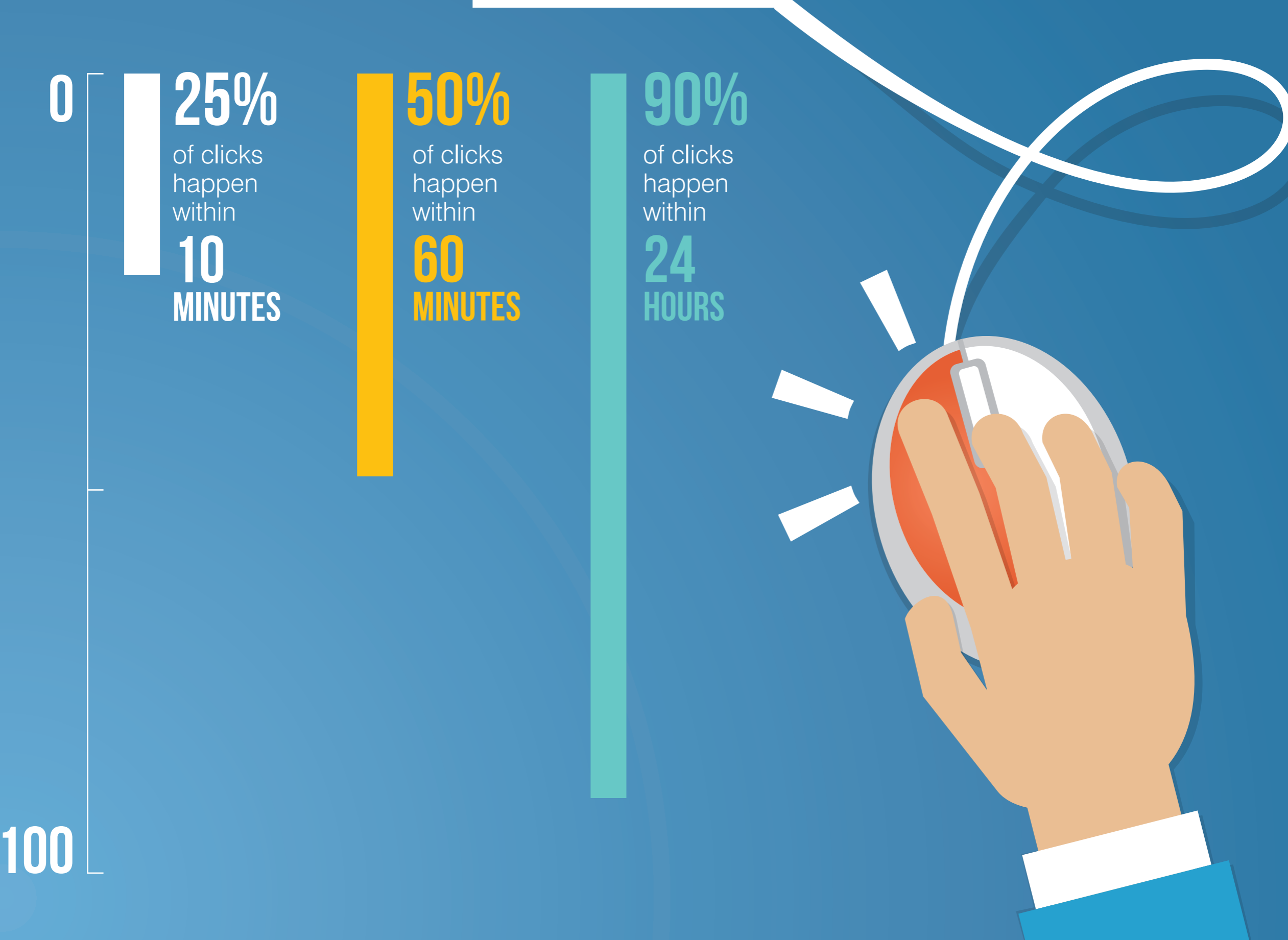
URLs may be hiding in encrypted attachments.



URLs to pages often contain malware, sometimes after delivery.<sup>1</sup>

## THE CLICKS KEEP ON COMING

The longer a malicious URL sits in the inbox, the more likely it will be clicked.



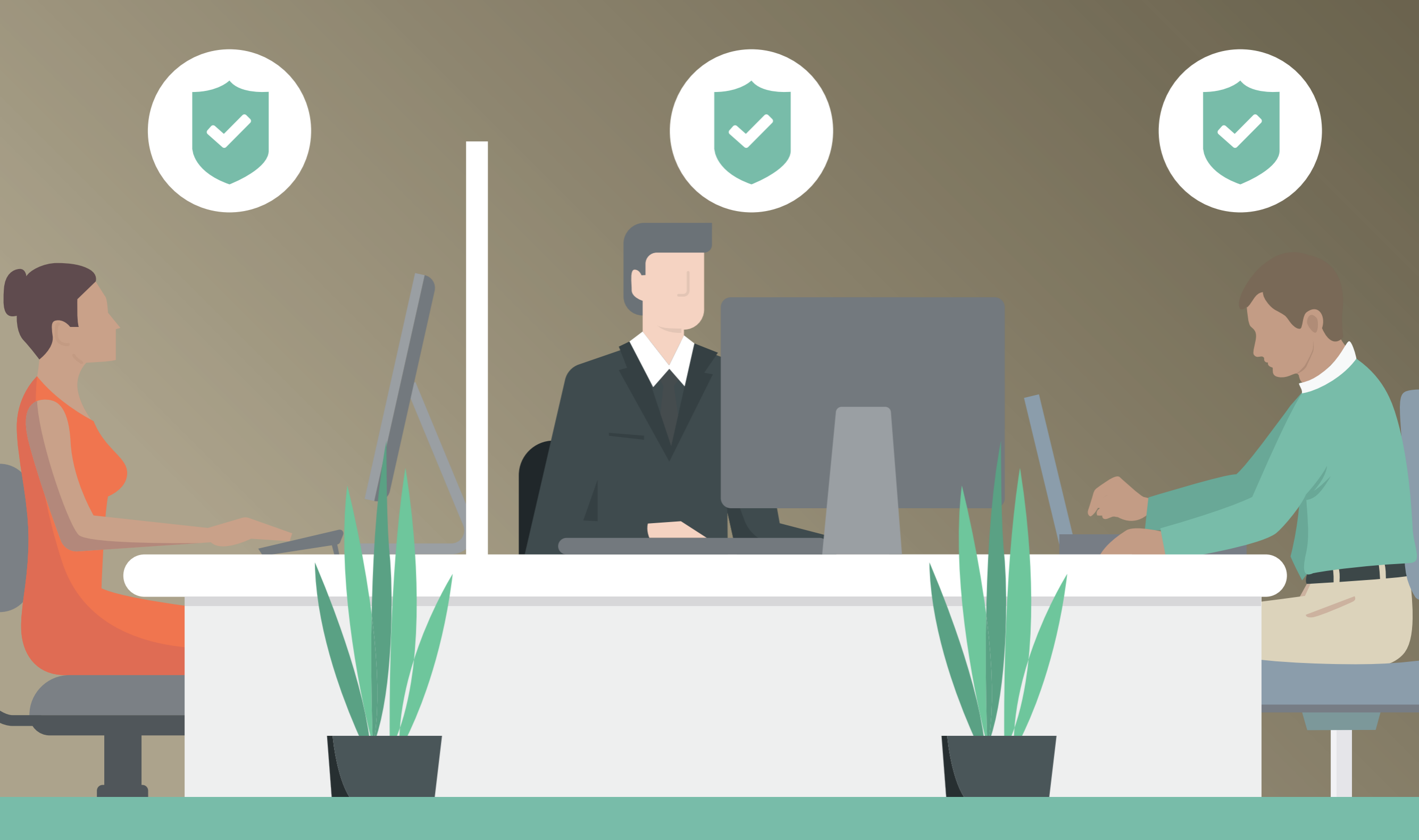
## SHARING IS SCARING

Document-sharing lures are consistently effective. URLs often link to malicious files in Google Drive, Adobe Creative Cloud, and Dropbox. Top click rates include:



## 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, Yammer, and even SaaS applications beyond Office 365.



To learn more, visit [www.proofpoint.com/office365](http://www.proofpoint.com/office365)

<sup>1</sup> Proofpoint. "Magnitude Actor Adds a Social Engineering Scheme for Windows 10." March, 2017.