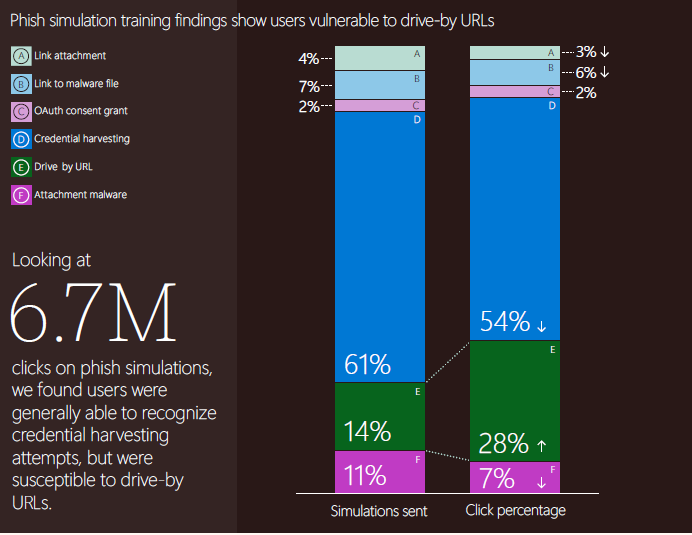
Chapter 2 p.30

Phish simulation training findings show users vulnerable to drive-by URLs

Stacked bar graph showing Phish simulation training data. Simulations sent show Link attachment: 4%, Link to malware file: 7%, OAuth consent grant: 2%, Credential harvesting: 61%, Drive-by URL: 14%, and Attachment malware: 11%. Click percentage show Link attachment: 3%, Link to malware file: 6%, OAuth consent grant: 2%, Credential harvesting: 54%, Drive-by URL: 28%, and Attachment malware: 7%. Users were seen vulnerable to drive-by URLs. Looking at 6.7M clicks on phish simulations, we found users were generally able to recognize credential harvesting attempts, but were susceptible to drive-by URLs.

Source: Microsoft Defender for Office 365, attack simulation training data