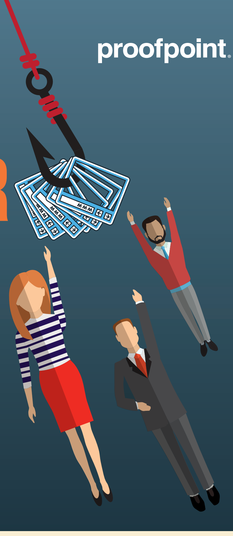
proofpoint.

THE HUMAN FACTOR 2017

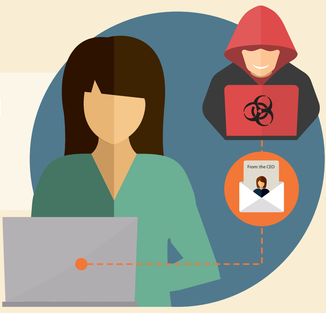
Malicious emails exploit people, not code.

Here are the top techniques cyber criminals used in 2016 to trick users into engaging with malicious emails and social media posts.



BUSINESS EMAIL COMPROMISE (BEC) ATTACKS ARE RISING.

BEC message volume rose from 1% in 2015 to **42% by the end of 2016.**



SOCIAL MEDIA ACCOUNT PHISHING TRENDS UP.

Social media account phishing **increased 150%** in 2016.

MALWARE CATEGORIES VARY DISTRIBUTION BY DAY.

Ransomware campaigns **favour Tuesday through Thursday.**

TIME IS MONEY.

87% of clicks on malicious URLs occur within first 24 hours of delivery

Nearly 50% of clicks occur within an hour

25% of clicks occur in just ten minutes

ATTACKS PEAK MID-DAY.

Clicks peak 4-5 hours after the start of the business day: that is, right around lunchtime.

FRAUDULENT MOBILE APPS TRICK USERS.

Malicious apps feature **stolen branding and misleading names** to convince users to download malware.

MORE MOBILE PHONES MEANS MORE RISK.

42% of clicks on malicious URLs were made from mobile devices, **double last year's rate of 20%**.

DOWNLOAD THE COMPLETE REPORT

proofpoint.com/uk/human-factor-report-2017