KEY FINDINGS.

THE GLOBAL THREAT INTELLIGENCE REPORT
JULY - DECEMBER 2024

mimecast

RISK RADAR

While threat actor activity has increased across almost all metrics, some trends stand out.

01 TRUSTED SERVICES ENABLE THREAT ACTORS

Attackers are increasingly leveraging trusted platforms like Microsoft, Google, and Evernote to host payloads and send phishing attacks.

02 AUTHENTICATION MAKES ATTACKS MORE DIFFICULT, BUT AI LOWERS THE BAR

SPF, DKIM, and DMARC help attacks appear to come from a trusted source. These make attacks more complicated, while the spread of AI chat bots allows cybercriminals to gain the skills necessary for hacking.

03 GEOPOLITICAL TENSIONS FUEL CYBERATTACKS

Global political instability — such as the Russia-Ukraine war and European elections — is intensifying cyber risks, with geopolitical threats and cyber risks ranked as the top two concerns in recent surveys.

04 HUMAN ERROR REMAINS THE WEAKEST LINK

Insider actions accounted for 68% of breaches in 2023, while 34% of employees fear being the exploited vulnerability in future attacks.

05 MALICIOUS LINKS, MALICIOUS FILES AND IMPERSONATION DOMINATE THREATS PER USER

The Arts, Entertainment & Recreation, Legal Services, and Media & Publishing industries saw the most threats per user in H2 2024.

DOWNLOAD THE REPORT