Cyber Resilience for Email

The Human Firewall

Mounil Patel, Field CTO
September 2018
Why do we feel we are failing Cyber Security for eMail?
Email Attacks

~30% of phishing attacks were opened

100s Median time to first click

91% of attacks start with a phish

66% of malware was installed via malicious email attachments

$5B BEC is $5B global scam

Defense Arms Race

90% of global organizations have seen Phishing attack volume increase and 40% have seen the volume of impersonation attacks increase.
• Messages Inspected by Mimecast: 9,281,487

• 696,664 Total Spam = 370,296 Rejected + 326,368 Quarantined
  - Reasons include: RBL, IP/Domain Reputation, Anti-Spoofing, Spam Signature

• 7.5% of delivered messages would have have been rejected or quarantined as spam by Mimecast

• Average spam emails missed per user per week: 22

URL Protect – On Average 1 of every 686 clicks are to bad sites
Skills Gap

3.5 million unfilled information security positions by 2022 globally.
Hello Chase Online™ Customer,

We are sorry, due to several failed attempts to access your account, we have temporarily deactivated it (https://protect-eu.mimecast.com/s/). You are required to reactivate your bank account to log in and continue using it.

Click to follow link

Please login to www.chase.com and enter your information correctly.

We apologize for any inconvenience this may have caused and look forward to taking further action with you to ensure your account remains secure.

Please do not reply to this automatically system generated email.

Sincerely,
Your Chase Online™ Banking Team
78% of organizations that experienced a ransomware attack over the past year report that downtime lasted for at least one day, with three days of downtime being the average.
Data Recovery

Three days is the average time to recover for organizations that had suffered an email-based attack in the past 12 months.
Ensuring predictable outcome through comprehensive security controls before, continuity during, and automated recovery after an attack.
Thank You!