

# EMAIL: AN EASY TARGET FOR CYBER ATTACKS

Every day, attackers send a whopping 150 million phishing emails. If printed and laid end-to-end, these malicious messages would stretch over 26,000 miles—far enough to circle the earth.

## ABOUT 269 BILLION EMAILS ARE SENT EACH DAY.<sup>1</sup>

**2/3**

Nearly 2 out of every 3 emails sent are SPAM.<sup>3</sup>

**91%**

Almost all cyber crimes start with email.<sup>1</sup>

**84%**

A majority of organizations have been spear-phished.<sup>5</sup>

### Biggest targets

Most commonly, cyber predators target managers and executives, financial data, and intellectual property—seeking out proprietary information and personal data to leverage for their own gain or sell.

...  
**More attackers are going after personal contact info, customer information and physical assets.**

## HOW IT HAPPENS

**1**

### An unexpected approach

Cyber attackers use phone calls to help circumvent controls.

### RECON

An attacker calls an employee on the phone to notify them of a pending email or request a personal email address.



**3**

### PHISHING

Assuming the email is real, the employee clicks on an embedded link and unwittingly downloads malware.



**2**

### SOCIAL ENGINEERING

The attacker sends a follow-up email, referencing the phone call.



**4**

### EXFILTRATION

Once infected, hackers use email, web, file transfer and tunneling protocols to retrieve stolen data.



**5**

### MISSION ACCOMPLISHED

With stolen data in hand, hackers monetize the data in a variety of ways, such as holding it for ransom or selling it over the dark web.



95% of phishing-based breaches are followed by software installation.<sup>5</sup>

## THE COSTS OF AN EMAIL BREACH ARE SIGNIFICANT.

### FINANCIAL COST

**\$3.62M**

Average cost of an email breach

### REMIEDIATION TIME

**66 days**

Average time required to contain the breach

### RECURSION RATE

**27.7%**

Likelihood a second material data breach will occur within 24 months<sup>4</sup>

### Most-impacted Industries

On average globally, a breach costs \$141, a stolen record,<sup>4</sup> but some industries such as health care and financial services are disproportionately affected.

**\$200**

Education

**\$245**

Financial services

**\$380**

Health care

**\$188**

Life science

**\$223**

Human services

AVERAGE COST PER STOLEN RECORD<sup>4</sup>

Incident response teams and the extensive use of encryption reduce the cost of a data breach by as much as \$19 per compromised record.<sup>3</sup>

## FIREEYE EMAIL SECURITY MEANS BETTER PROTECTION.



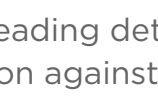
Safeguard your organization's business assets with industry-leading detection and protection against phishing and ransomware.



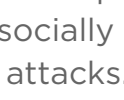
Get real-time, automated protection from spear-phishing and other socially engineered attacks.



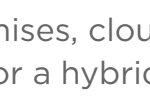
Stay secure, whether your email environment is on-premises, cloud-based or a hybrid.



Rest assured with always up-to-date protection; no upgrades needed.



Give your security team the information it needs to respond with comprehensive, contextual threat intelligence.



Stay on top of it all with protection from hard-to-detect multi-vector, multi-flow attacks.

Protect your people, data and assets with FireEye Email Security. Learn how at [fireeye.com/email](https://fireeye.com/email)

- Reduces business risk of unauthorized access
- Saves operational costs
- Deploys in minutes with no physical infrastructure

1 Radicati Group Email Statistics Report, 2017-2021.  
2 PhishMe (2016). Enterprise Phishing Susceptibility and Resiliency Report  
3 <https://securelist.com/analysis/quarterly-spam-reports/69932/spam-and-phishing-in-the-first-quarter-of-2015/>  
4 Ponemon Institute LLC (June 2017). "2017 Cost of Data Breach Study: Global Analysis."  
5 Vanson Bourne. "The Impact of Spear Phishing." 2016