

ONE

IT ONLY TAKES ONE EMAIL FOR A CODE TRIAGE

The Path of an Email Attack

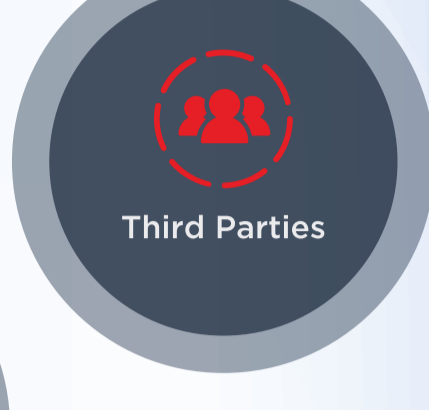
281 billion emails are sent each day.¹

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.

Why Healthcare is Under Attack

FireEye is currently tracking 17 advanced threat groups targeting Healthcare, including providers and facilities, insurance, medical equipment, pharmaceutical, biotechnology, and social services. Spear phishing and strategic web compromise are the most common attack vectors we see in healthcare, and it's among the top three industries that suffered the most significant attacks last year.²

-
- Healthcare records fetch the biggest payoff
- Interconnected devices often run on outdated systems and/or in the cloud
- Health Information exchange with third parties provide countless access points



32% of all emails received are clean. ³	91% Almost all cyber crimes start with email. ⁴	84% A majority of organizations have been spear phished. ⁵
--	--	---

How It Happens

AN UNEXPECTED APPROACH

Cyber attackers use phone calls to help circumvent controls.

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

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

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

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.

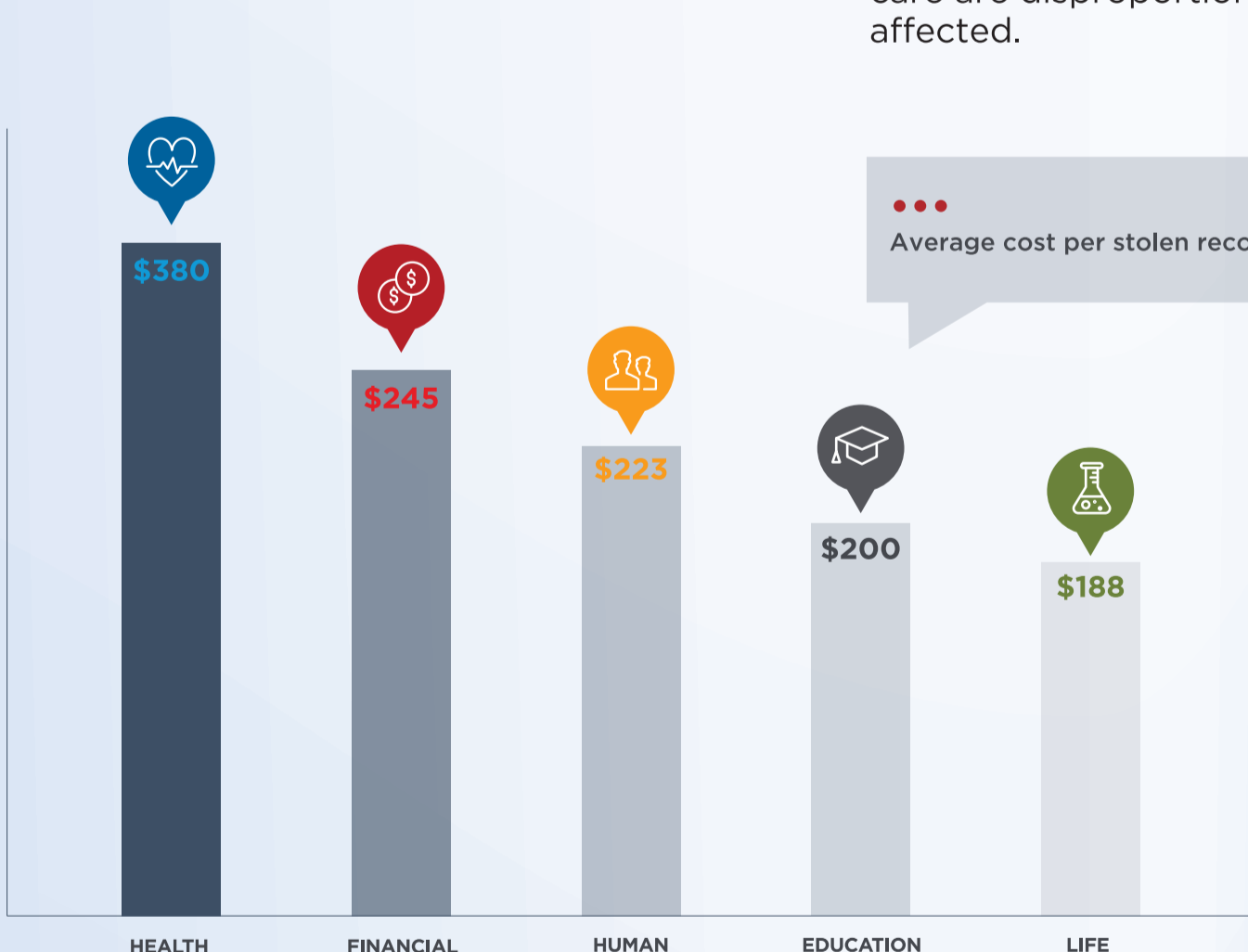
95% of phishing-based breaches are followed by software installation.⁵

The Costs of an Email Breach Are Significant

FINANCIAL COST \$3.62M Average cost of an email breach ⁶	REMIEDIATION TIME 66 days Average time required to contain the breach ⁶	RECURRENCE RATE 27.7% Likelihood a second material data breach will occur within 24 months ⁶
---	--	---

HEALTHCARE IS THE MOST IMPACTED INDUSTRY

On average globally, a breach costs \$141 for each stolen record, but some industries such as health care are disproportionately affected.



Incident response teams and the extensive use of encryption **reduce the cost of a data breach by as much as \$19 per compromised record.⁵**

FireEye Email Security means better protection

- Safeguard your organization's business assets 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.
- Respond to threats more effectively with comprehensive, contextual threat intelligence.
- Protect your organization from hard-to-detect multi-vector, multi-flow attacks.



Protect your people, data and assets with FireEye Email Security. Learn how at www.FireEye.com/email.html

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

1 Radicati Group (February 2017), Email Statistics Report, 2017-2021.
2 FireEye Intel and 2018 M-Trends Report
3 FireEye (August 2018), Get One Step Ahead of Email Threats, Email Threat Report for January-June 2018
4 PhishMe (2016), Enterprise Phishing Susceptibility and Resiliency Report
5 Vanson Bourne, "The Impact of Spear Phishing," 2016
6 Ponemon Institute LLC (June 2017), "2017 Cost of Data Breach Study: Global Analysis."