proofpoint®

Protecting Patients, Providers and Payers

2019 Healthcare Threat Report

proofpoint.com

INTRODUCTION

Few industries can claim a mission more critical, data more sensitive, or operations more complex than healthcare. Unfortunately, few industries are finding it more challenging to keep it all protected.

Cyber attacks are exposing personal data. Ransomware is shutting down emergency rooms. Fraudulent emails are defrauding business associates, patients, and clinical staff. These threats hurt the industry's ability to care for patients.

To help healthcare organizations better understand the evolving threat landscape, we analyzed a year's worth of cyber attacks against care providers, pharmaceutical/life sciences organizations and health insurers. As we analyzed hundreds of millions of malicious emails, one trend stood out: today's attacks target people, not just infrastructure.

They trick healthcare workers into opening an unsafe attachment or opening a questionable link that leads to malware. They impersonate members of your executive team, instructing staff to wire money or send sensitive information. And they hijack patients' trust with scams that cash in on your organization's brand equity.

Unless otherwise noted, the data in this report covers the time period spanning Q2 2018 to Q1 2019. We have seen similar trends in Q2 2019.

KEY FINDINGS

77% of email attacks on healthcare companies during the study used **malicious URLs**.

Targeted healthcare companies received about **43 impostor emails in Q1 2019** — a **300%** jump over the same quarter last year.

95% of targeted healthcare companies saw emails spoofing their own trusted domain. And all of them had their domain spoofed to target patients and business partners.

VIPs and other high-ranking workers aren't always attackers' biggest targets.

Many factors— such as access to the right data or systems, having a visible email—can make anyone a Very Attacked Person.

Emotet a versatile botnet that we classified as a banking Trojan in previous reports, accounted for **60%** of all malicious payloads **in the first quarter of 2019.**

Subject lines that included **"payment," request,"** and **"urgent"** and related terms appeared in **55%** of all impostor email attacks.

For each targeted healthcare organization, an average of **65** staff members were attacked in Q1 2019

Banking Trojans were the biggest threat to healthcare companies over that period, accounting for **41%** of malicious payloads during our study.

The largest volume of impostor email attacks targeting healthcare arrived on weekdays between **7 AM & 1 PM** in the targets' time zone.

51% of email sent from healthcare-owned domains in Q1 was unverified by DMARC, a sign that they might be spoofed.

SECTION 1 MALWARE THREATS

Malware is an umbrella term for a wide range of malicious code delivered and installed on users' systems and servers. More sophisticated strains combine the capabilities of two or more malware types, and we often see malware using advanced techniques to avoid detection.

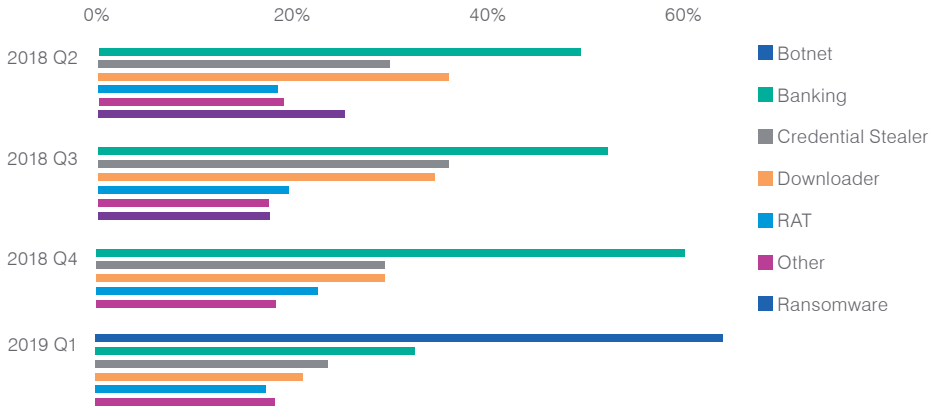
Emotet is a prime example. The malware strain, once considered a banking Trojan, has evolved to become a tool for distributing spam, stealing information, and other malicious activities. As a result, we now classify it as botnet malware.

Emotet was by far the biggest malware payload in emails sent to healthcare companies in the first quarter. It's the first appearance in recent quarters of botnets as a category of malware targeting the healthcare sector.

At the other end of the spectrum, ransomware, which was rampant in Q2 2018, has largely disappeared in the ensuing quarters. Stealers, downloaders and RATs have also declined during that period, though not as dramatically.

Malware Volumes by Family

Emotet, formerly a banking Trojan now considered botnet malware, was by far the biggest malicious payload in emails sent to healthcare companies in Q1.



Banking Trojan traffic in Q2 through Q4 2018 includes Emotet, which we reclassified as a botnet in Q1 2019. Emotet volumes, regardless of classification, rose steadily during the duration of this study.

Emotet went on a hiatus from June through mid-September 2019, outside the collection period for much of the data presented in this report. The malware is now back with regular activity as of the distribution of this report.

Whatever happened to ransomware?

Ransomware attacks have fallen to a fraction of their 2017 heyday, though several high-profile attacks have made headlines in recent weeks. Security researchers have several theories about this apparent vanishing act.

One of the leading theories follows the money. The value of cryptocurrency, attackers' preferred form of payment, has fallen from 2017 highs and remains volatile. That has made ransomware less of a sure bet for attackers.

Another theory is that ransomware attackers "overharvested" the pool of potential victims. Ransomware's meteoric rise—and the headlines it generated—may have spurred organizations to act. Many have bolstered their cyber defenses, trained users to be more security-aware and adopt more robust backup regimens. The result: fewer organizations paid the ransoms.

We're also seeing the use of ransomware in more carefully targeted, high-ransom attacks on victims who are most likely to pay. This is a big shift from the "spray and pray" ransomware campaigns of 2017.

In many recent cases, the targeted organizations may have already been compromised before being hit with ransomware. This condition allowed attackers to install ransomware on key, vulnerable pieces of infrastructure after carefully studying the target to determine where a system lockout would hurt the most. The approach boosted the chances of a payout, making the effort worth it.

Even before we reclassified it as botnet malware, Emotet was a threat to healthcare companies. It was one of the top three malware strains by message volume in Q3 2018, and it went on to dominate the following two quarters.

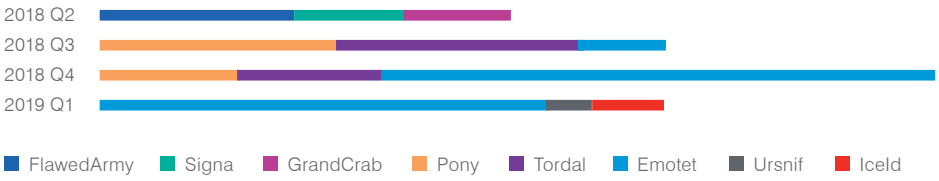
Attackers appear to be moving away from single-purpose threats to the versatile malware strain. Call it the Swiss Army knife effect. Depending on how attackers deploy it, Emotet can serve as a downloader, information stealer, spambot and more. That makes it useful to attackers—and a growing threat to healthcare organizations.

Emotet's influence was clear in other ways, including the ratio of URL-based email attacks vs. attachment-based attacks. About 77% of malicious emails sent to healthcare companies in the four quarters through Q1 2019 used a URL, Emotet accounting for much of that total.

Emotet volume has declined sharply in recent months. Such hiatuses often coincide with attackers retooling the malware or making changes to their infrastructure. Even with the pause, Emotet remains a prime example of the type of robust, multipurpose malware we see targeting healthcare and other industries.

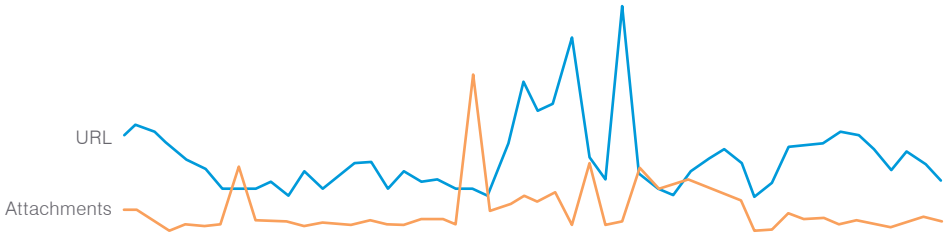
Relative Message Volumes Associated with Top Malware Families Distributed to Healthcare Organizations

Attackers appear to be moving away from standalone threats to Emotet, which can be a loader, stealer and banker.



Relative Weekly Malicious Message Volumes at Healthcare Organizations, URLs vs. Attachments, 2018

About 77% of malicious emails sent to healthcare companies used a URL, driven by Emotet.



Infection control

Here are the main categories of malware and what they do.

- **Ransomware**—Locks away victims' files until victims pay a "ransom" to regain access
- **Backdoor**—Gives attackers undetected access to the compromised system
- **Banking Trojan** (or banker)—Allows attackers to view or steal banking credentials to access victims' accounts
- **Keylogger**—Captures typing on infected systems, allowing attackers to see user input such as credentials and other sensitive information
- **Stealer**—Steals data such as contacts, browser passwords and more
- **RAT** (remote access Trojan)—Gives attackers widespread access to and control over infected systems
- **Downloader**—Downloads other malware, depending on attackers' needs
- **POS**—Compromises point-of-sale device to steal credit card numbers, debit card and pin numbers, transaction history, and more
- **Botnet**—A collection of computers compromised and under the control of attackers for large spam campaigns and other attacks

Malware attacks accounted for most attacks over the course of our study.

The volume and share of attachment- and URL-based attacks is constantly shifting. But URL attacks have played a growing role in recent quarters. URL-based attacks are effective because although users have grown more cautious about opening attachments, they still click URLs. That's especially true if the URL is that of a known, trusted source such as a file-sharing service. Attackers often use these services to host malware, linking to the malicious files in a URL.

Unlike attacks that use malicious file attachments, URL-based email campaigns typically contain no malicious payload. There's no code to analyze, match against known malware signatures, or run in a sandbox. The risky code is not in the email itself but on the website the URL links to.

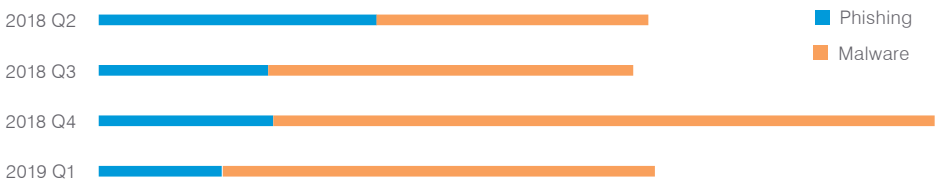
Attackers can easily create new URLs—much faster than security tools can analyze them and update their blocklists. Bad URLs are also easy to disguise with link-shortening tools, which have legitimate business purposes and are therefore assumed benign. And it's easy to host malicious code on popular file-sharing sites such as Dropbox and OneDrive, which have become a normal, trusted part of modern business.

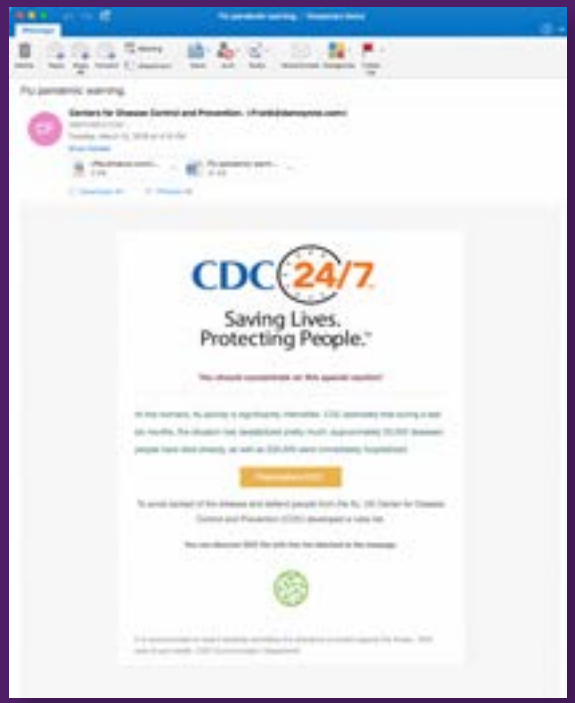
Even under the best circumstances, some users will click on an unsafe URL that appears in an email. Attackers have grown skilled at researching their targets and using social engineering to exploit human nature. Some lures are just too well researched, expertly crafted, and psychologically potent to resist every time.

It might seem intuitive to associate file attachments with malware attacks and URLs with phishing. But in many cases, the reverse is also true—file attachments can just as easily be used in phishing attacks, and URLs in malware attacks. What form the threat takes—URL or an attachment—reflects attacker's chosen tactics, not necessarily their tools or objectives.

Relative Message Volumes for Phishing vs. Malware Attacks Against Healthcare Organizations

Malware-based attacks have dominated over the last year, spiking in Q4 2018.





The GandCrab cash-grab: how a ransomware strain hit healthcare

Our researchers recently analyzed a ransomware campaign targeting the healthcare sector. Cyber criminals used email disguised as an alert from the U.S. Centers for Disease Control and Prevention—the kind of email that concerned healthcare workers might open right away.

The message, which displayed the CDC 24-7 logo, warned of a flu pandemic and offered a "rules list" to contain the outbreak in the form of a Microsoft Word document.

But when opened, the file triggered the installation of GandCrab ransomware.

GandCrab was offered as a service to cyber criminals, who paid the malware's creator a commission for ransoms they collected from victims. The creator reportedly announced plans to "retire" at the end of June after GandCrab generated $2 billion in ransom payments.[1] The move came days before researchers released a free decryptor that gave victims access to bypass the ransomware and regain access to their files.[2]

Although ransomware attacks have largely dwindled, healthcare workers' laser focus on protecting patients will always leave them vulnerable to socially engineered threats like those used to spread GandCrab.

1. Catalin Cimpanu (ZDNet). "GandCrab ransomware operation says it's shutting down." June 2019.
2. Danny Palmer (ZDNet). "Game Over for GandCrab: New free decryption tool allows victims to unlock all versions of this ransomware." June 2019.

SECTION 2 HEALTHCARE'S VERY ATTACKED PEOPLE

Executives and other VIPs are not always cyber attackers' biggest targets. That's why we use the term Very Attacked People to describe those most heavily targeted by cyber threats.

In many cases, healthcare VAPs are workers with roles that give them privileged access to sensitive data, systems or relationships. In other cases, it's someone with a public-facing email address. These can include shared accounts and email aliases, which are usually permanent, forward email to several recipients, and hard to secure with multifactor authentication.

Assessing user risk: the VAP model

Just as people are unique, so is their value to cyber attackers and risk to employers. They have distinct digital habits and weak spots. They're targeted by attackers in diverse ways and with varying intensity. And they have unique professional contacts and privileged access to data on the network and in the cloud.

Together, these factors make up a user's overall risk in what we call the VAP (vulnerability, attacks, and privilege) index.

Vulnerability
Users' vulnerability starts with users' digital behavior—how they work and what they click. Some employees may work remotely or access company email through their personal devices. They may use cloud-based file storage and install third-party add-ons to their cloud apps. Or they may be especially receptive to attackers' email phishing tactics.

Attacks
All cyber attacks are not created equal. While every one is potentially harmful, some are more dangerous, targeted, or sophisticated than others.

Indiscriminate "commodity" threats might be more numerous than other kinds of threats. But they're usually less worrisome because they're well understood and more easily blocked. Other threats might appear in only a handful of attacks. But they can pose a more serious danger because of their sophistication or the people they target.

Privilege
Privilege measures all the potentially valuable things people have access to, such as data, financial authority, key relationships, and more. Measuring this aspect of risk is key because it reflects the potential payoff for attackers—and harm to organizations if compromised.

In many cases, people with the most visible email addresses, including shared email accounts, drew a disproportionate share of the most targeted attacks. Here are just a few of the reasons someone might be on attackers' radars:

- They have public-facing contact information
- They are long-tenured workers, increasing the chances that their email address is eventually revealed
- They are included in a public-facing distribution list
- Their email address was leaked in an earlier data breach
- They were recently published or featured in an announcement or news report, often with their email address

Here are three real-world examples of VAPs in three categories of healthcare. We show the 20 most heavily targeted email addresses at each organization. Using social engineering research—and the same public information an attacker would use—we matched each address to its owner. (We've omitted some details to protect customers' privacy.)

Get to know your VAPs

Here are some examples of Very Attacked People we saw in various segments of the healthcare sector. The profiles are based on an analysis of more than 70 healthcare organizations.

Large Teaching Hospital

In this example, the email account most targeted by attackers is a shared email alias used to request patient information. The next three are professors, followed by three HR-related roles, two more professors, and several director-level positions.

Large Pharmaceutical

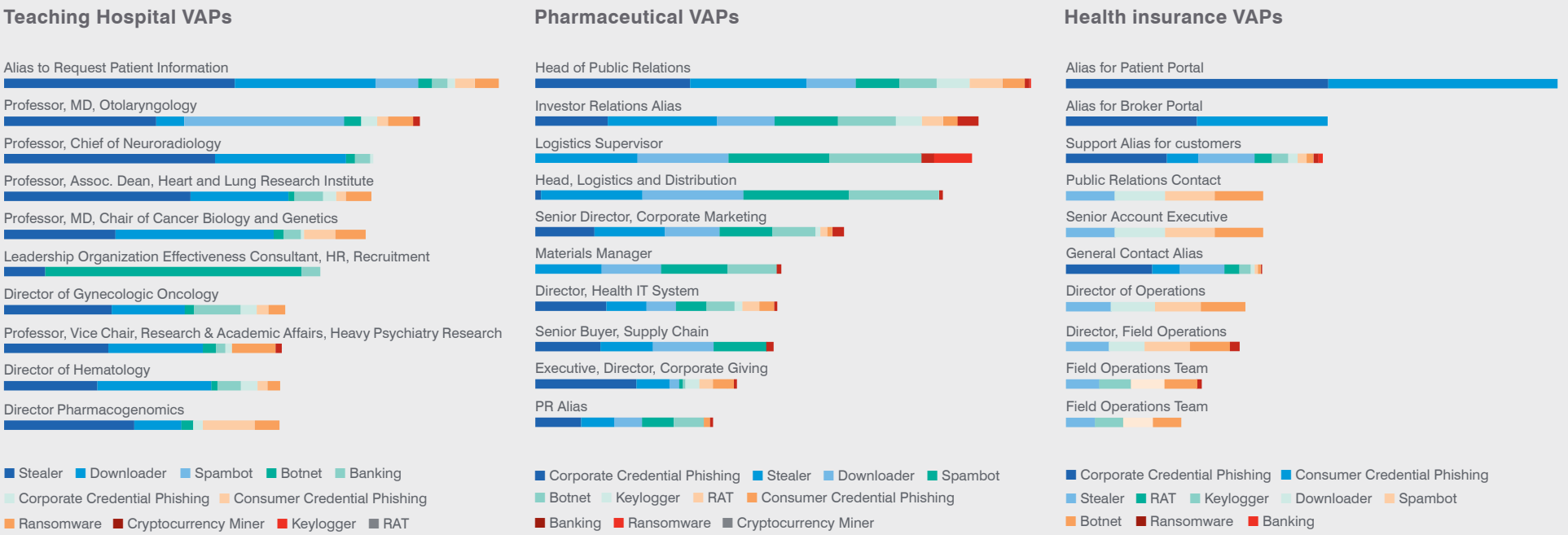
In this example, public-facing email addresses and aliases are among the most targeted. They include the drugmaker's head of public relations and the PR alias, its investor relations alias, corporate marketing directors, and director of corporate giving. These emails are among the easiest to obtain, making them easy targets for attackers. Even if they don't represent attackers' ultimate target.

Only one of the addresses, the company's vice president for research and development, is someone who fits the standard definition of a VIP.

Large Insurer

In this example, the top three most attacked email addresses are aliases, as is more than half of the top 15 on this list. Several director-level targets also appear, along with four members of the insurer's field operations team.

Relative Malicious Message Volume by Top Targeted Roles



SECTION 3 IMPOSTOR THREATS

Impostor emails are fraudulent messages designed to look like they're from someone the recipient knows or can trust.

Unlike traditional email attacks, impostor attacks—including email fraud—don't use malware attachments or malicious links or other common phishing techniques. Instead, they rely on social engineering to trick the victim into doing something the attackers wants. That can be anything from transferring money to the attack to sending sensitive information.

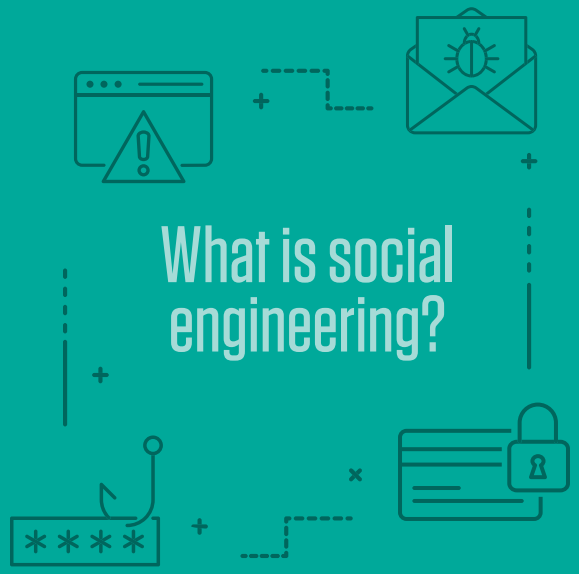
These attacks can be hard to detect because they don't exploit technical vulnerabilities. They target human nature.

Surging Volume

Healthcare organizations targeted by impostor emails received 43 messages of this type in Q1 2019—a 300% jump from a year ago and more than five times the volume in Q1 2017.

More than half the healthcare organization in our study were attacked more often than they were in Q1 2017. Not a single organization saw a decrease in impostor attacks over that period.

The average impostor attack spoofed (posed as) 15 healthcare staff members on average across multiple messages. Nearly half of healthcare organizations were targeted in attacks that spoofed at least five identities; about 40% were targeted in attacks that spoofed two to five identities.



In cybersecurity, social engineering refers to the strategies and tactics attackers use to trick you. In most cases, their goal is to get you to:

- Open a malicious email attachment
- Click on an unsafe URL
- Send money or valuable information directly

In other words, social engineering is the art and science of manipulation—hacking human nature rather than technology.

Most cyber attacks use some form of social engineering. They may:

- Spoof an email domain to craft an email that looks like it's from a colleague
- Mention personal details (gleaned from your social networks) to gain your trust
- Pique your curiosity with an attachment that you just can't resist opening
- Warn you to act right away by making the situation seem urgent

Social engineering works because it taps into the way the human brain works. It uses deep-rooted impulses—such as fear, desire, obedience, and empathy—and turns them against you. And it hijacks your normal thought process to spur you to act on attackers' behalf.

Social engineering is all about exploiting people. That's why stopping it requires a cyber defense focused on people, not technology. That includes stopping social engineering attempts from reaching their targets—and training people to recognize and report any attempts that get through.

Sender Unknown

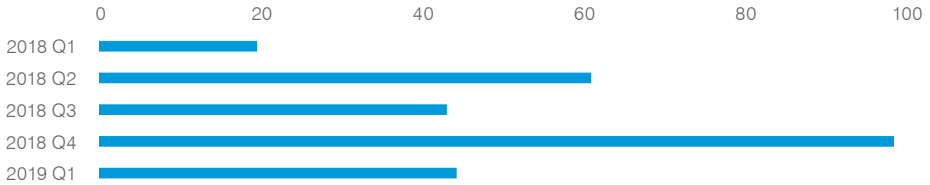
Only half of emails sent through internet domains owned by healthcare organizations could be verified through DMARC authentication.

DMARC, which stands for Domain Message Authentication Reporting & Conformance, is a framework for identifying and blocking spoofed emails. Not all unverified emails are spoofed, but DMARC provides assurances that an email from a healthcare provider is really coming from that organization.

Healthcare workers and patients were the most likely recipients of unverified email from a healthcare domain—54% and 52% of all messages to these groups were unverified. The good news: more than 87% of email from a healthcare domain sent to business partners were verified by DMARC.

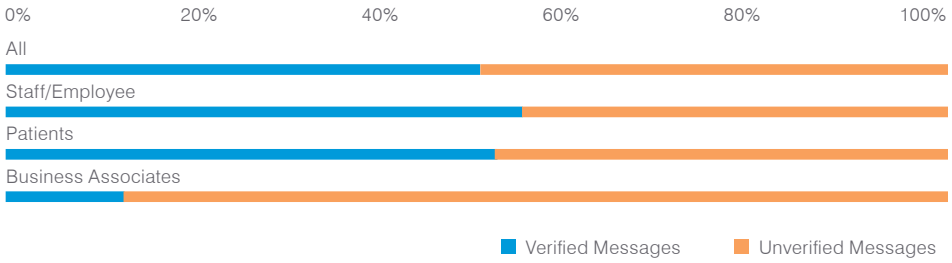
Impostor Email Attacks per Targeted Organization

Impostor emails targeting healthcare surged 300% from a year ago.



DMARC Authentication Status

Healthcare workers and patients were far more likely to receive unauthorized email.



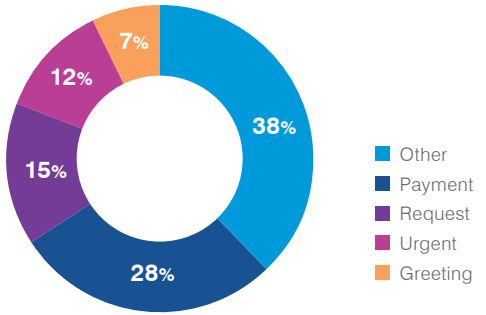
Grabbing Attention

Email fraudsters use a range of techniques to trick recipients into opening the email and acting on it. Attention-grabbing subject lines—especially ones that short-circuit the decision-making process and spur the recipient to open the email—are a big part of social engineering.

In the four quarters through Q1 2019, the most popular subject categories used to target healthcare organizations included "**payment**," "**request**," and "**urgent**." These terms are often associated with wire-transfer fraud, a potential clue to attackers' motives.

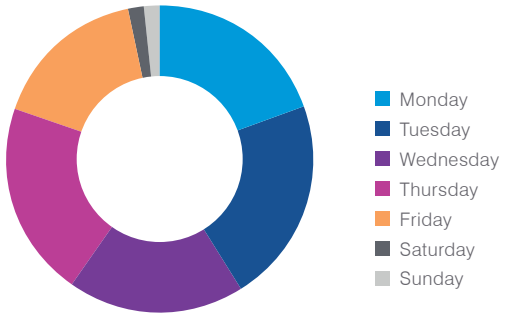
Impostor Attacks by Subject Category—Q1 2018-Q1 2019

"Payment," "request," and "urgent" were the most popular terms used in subject lines of impostor emails.



Email fraud attacks are socially engineered to target specific people who, due to their job roles, can carry out criminals' wishes. For that reason, fraudsters regularly target healthcare companies on weekdays. Most attacks are sent Monday–Thursday. Volume dips on Friday before falling sharply for the weekend.

Impostor email sent, by days of the week—Q1 2018-Q1 2019



The upshot: attackers time their emails to trick users when they are at work—and possibly too busy or stressed to think twice about opening that email.

CONCLUSION AND RECOMMENDATIONS

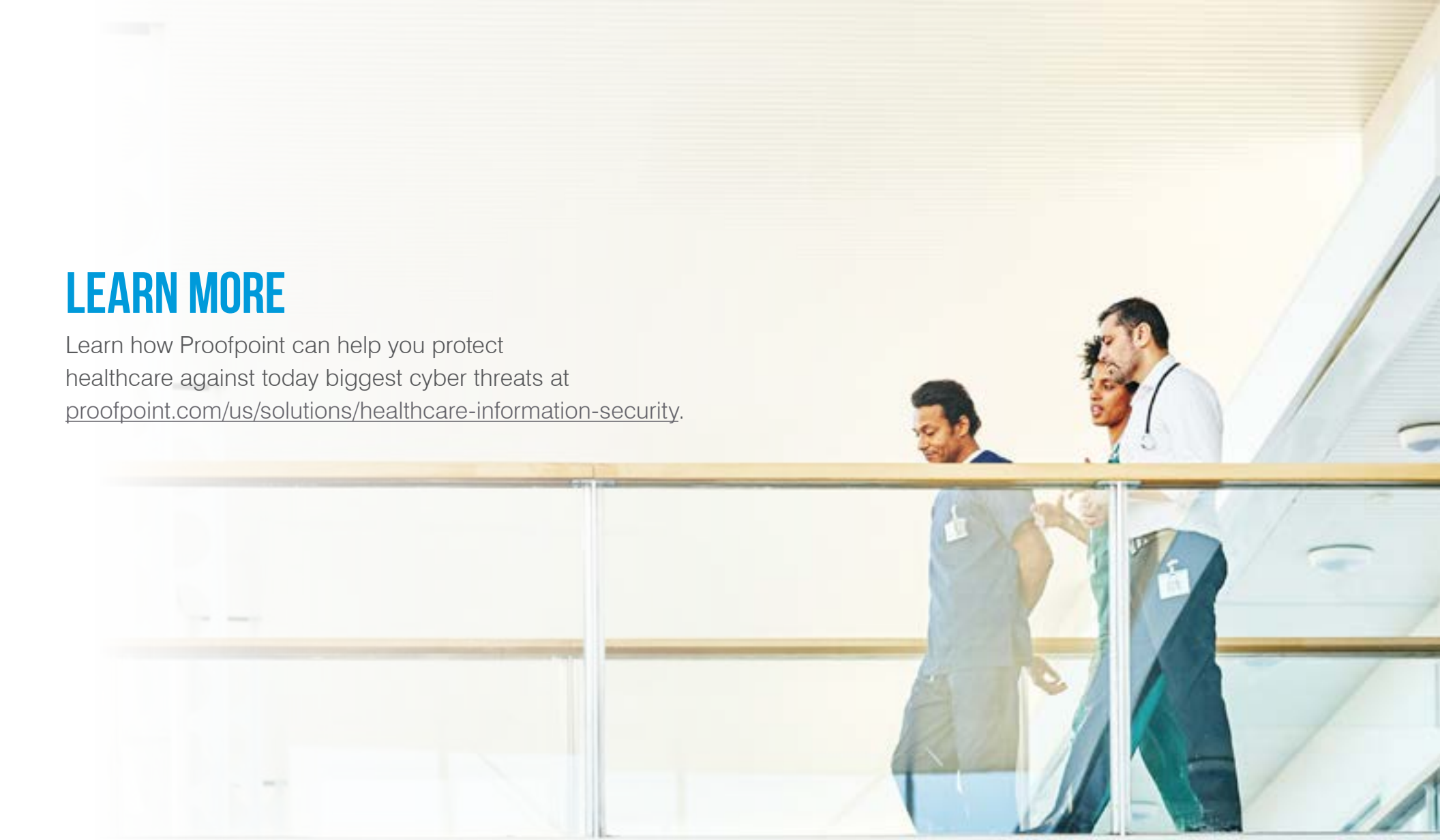
Today's attacks target people, not just technology. They exploit the human factor: healthcare workers' natural curiosity, acute time constraints and desire to serve. Protecting against these threats requires a new, people-centered approach to security.

We recommend the following:

- **Adopt a people-centered security posture.** Attackers do not view the world in terms of a network diagram. Deploy a solution that gives you visibility into who's being attacked, how they're being attacked, and whether they clicked. Consider the individual risk each user represents, including how they're targeted, what data they have access to, and whether they tend to fall prey to attacks.
- **Train users to spot and report malicious email.** Regular training and simulated attacks can stop many attacks and help identify people who are especially vulnerable. The best simulations mimic real-world attack techniques. Look for solutions that tie into current trends and the latest threat intelligence.
- **At the same time, assume that users will eventually click some threats.** Attackers will always find new ways to exploit human nature. Find a solution that spots and blocks inbound email threats targeting employees before they reach the inbox. And stop outside threats that use your domain to target customers.
- **Build a robust email fraud defense.** Email fraud can be hard to detect with conventional security tools. Invest in a solution that can manage email based on custom quarantine and blocking policies. Your solution should analyze both external and internal email—attackers may use compromised accounts to trick users within the same organization.
- **Isolate risky websites and URLs.** Keep risky web content out of your environment. Web isolation technology can render web pages from suspicious and unverified URLs in a protected container within users' normal web browser. Web isolation can be a critical safeguard for shared email accounts, which are difficult to secure with multifactor authentication. The same technology can isolate users' personal web browsing and web-based email services, giving them freedom and privacy without compromising the enterprise.
- **Protect your brand reputation and customers in channels you don't own.** Fight attacks that target your customers over social media, email, and the web—especially fake accounts that piggyback on your brand. And look for a complete social media security solution that scans all social networks and reports fraudulent activity.
- **Partner with a threat intelligence vendor.** Focused, targeted attacks call for advanced threat intelligence. Leverage a solution that combines static and dynamic techniques to detect new attack tools, tactics, and targets—and then learns from them.

LEARN MORE

Learn how Proofpoint can help you protect healthcare against today biggest cyber threats at proofpoint.com/us/solutions/healthcare-information-security.



ABOUT PROOFPOINT

Proofpoint, Inc. (NASDAQ: PFPT) is a leading cybersecurity company that protects organizations' greatest assets and biggest risks: their people. With an integrated suite of cloud-based solutions, Proofpoint helps companies around the world stop targeted threats, safeguard their data, and make their users more resilient against cyber attacks. Leading organizations of all sizes, including more than half of the Fortune 1000, rely on Proofpoint for people-centric security and compliance solutions that mitigate their most critical risks across email, the cloud, social media, and the web. More information is available at www.proofpoint.com.

proofpoint.

0719-015