THREAT REPORT

proofpoint.

EMAIL FRAUD IN HEALTHCARE

2019 REPORT

proofpoint.com

EXECUTIVE SUMMARY

Proofpoint regularly conducts extensive research to highlight the threats, trends, and key takeaways we see within our large customer base and in the wider threat landscape.

Every day, we analyze more than 5 billion email messages, hundreds of millions of social media posts and more than 250 million malware samples to protect organizations around the world from advanced threats. We continue to see sophisticated threats across email, social media and the web. That gives us a unique vantage point from which to reveal and analyze the tactics, tools and targets of today’s cyber attacks.

This *Email Fraud in Healthcare* report is designed to provide actionable intelligence you can use to better combat today’s attacks, anticipate emerging threats and manage your security posture. Along with our findings, the report recommends steps you can take to protect your people, data and brand.

EMAIL FRAUD HAS COST ORGANIZATIONS AROUND THE GLOBE **$12.5 BILLION** SINCE THE END OF 2013.

INTRODUCTION

Email fraud, also known as business email compromise (BEC), is one of today's biggest cyber threats. According to the FBI, email fraud has cost organizations around the globe $12.5 billion since the end of 2013.[1]

Email fraud preys on human nature—fear, trust, and the desire to please—to steal money and valuable information from organizations of every size, across every industry, everywhere in the world.

These socially engineered attacks seek to exploit people rather than technology. They are highly targeted. And they use identity deception tactics (such as spoofing) to pose as trusted colleagues and business partners.

For healthcare, email fraud is especially harmful. It hurts the most vulnerable segment of the population and the people dedicated to helping them.

For this study, Proofpoint analyzed more than 160 billion emails sent across 150 countries in both 2017 and 2018 to identify email fraud attack trends targeting more than 450 healthcare organizations.

KEY FINDINGS

- Healthcare organizations were targeted in 96 email fraud attacks on average in Q4 2018—a 473% jump over Q1 2017.
- Wire-transfer fraud is healthcare's most common form of email fraud.
- Within targeted healthcare organizations, 65 staff members were attacked in Q4 2018 on average.
- The largest volume of email fraud attacks targeting healthcare arrived on weekdays between 7 a.m. and 1 p.m. in the targets' time zone.
- 95% of healthcare organizations were targeted by an attack using their own trusted domain. And all of them had their domain spoofed to target patients and business partners.
- 45% of all email sent from healthcare-owned domains in Q4 appeared suspicious, including 65% sent to employees, 42% sent to patients, and 15% sent to business partners.

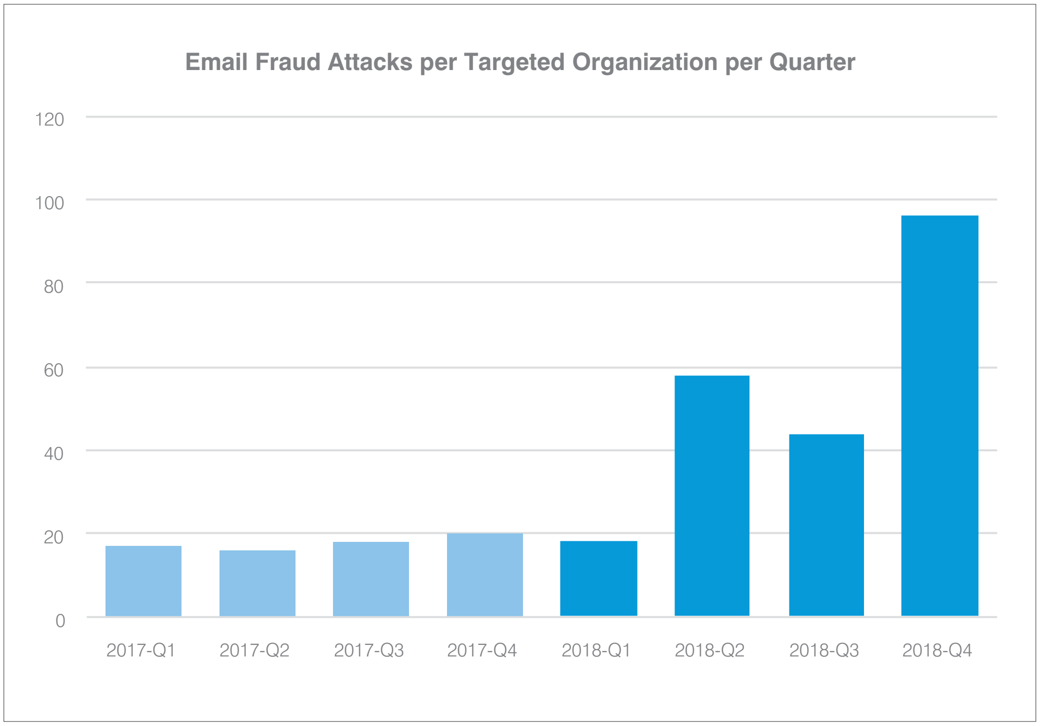
[1] FBI. "Business E-Mail Compromise: the 12 Billion Dollar Scam." July 2018.

EMAIL FRAUD SKYROCKETS

Healthcare organizations were targeted 473% more often in Q4 2018 vs. Q1 2017.

While email fraud was abundant in 2017, it soared in 2018. We saw more attacks, more healthcare targets, and more frequent attacks.

HEALTHCARE ORGANIZATIONS WERE TARGETED **473% MORE OFTEN IN Q4 2018 VS. Q1 2017.**



This increase is consistent with the email fraud problem overall. Every industry we track saw a significant rise in the same period. Healthcare providers were targeted with 32 email fraud attacks per month (96 for the quarter) on average in Q4 of 2018. More than half (53%) were attacked more often, with incidents up 200% to 600% during the two-year period. Not a single company saw a decrease.

Larger companies were targeted more frequently than smaller companies. This is a stark contrast to email fraud in other industries, where we see no correlation at all between company size and number of attacks.

FRAUDSTERS IMPERSONATE AND TARGET MORE PEOPLE

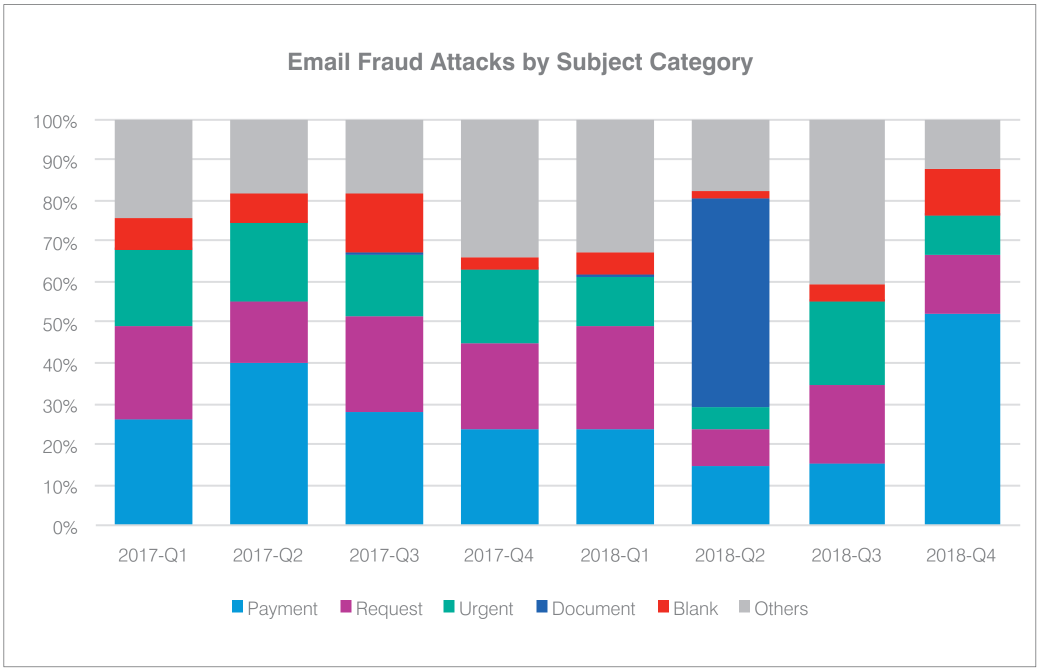
As criminals grow more sophisticated, they are spoofing (or impersonating) more identities and targeting more people within organizations.

Email fraud attacks spoofed 15 healthcare staff members on average across multiple messages. About half (49%) of organizations were targeted using at least five spoofed identities. And 40% of were targeted using between two to five spoofed identities.

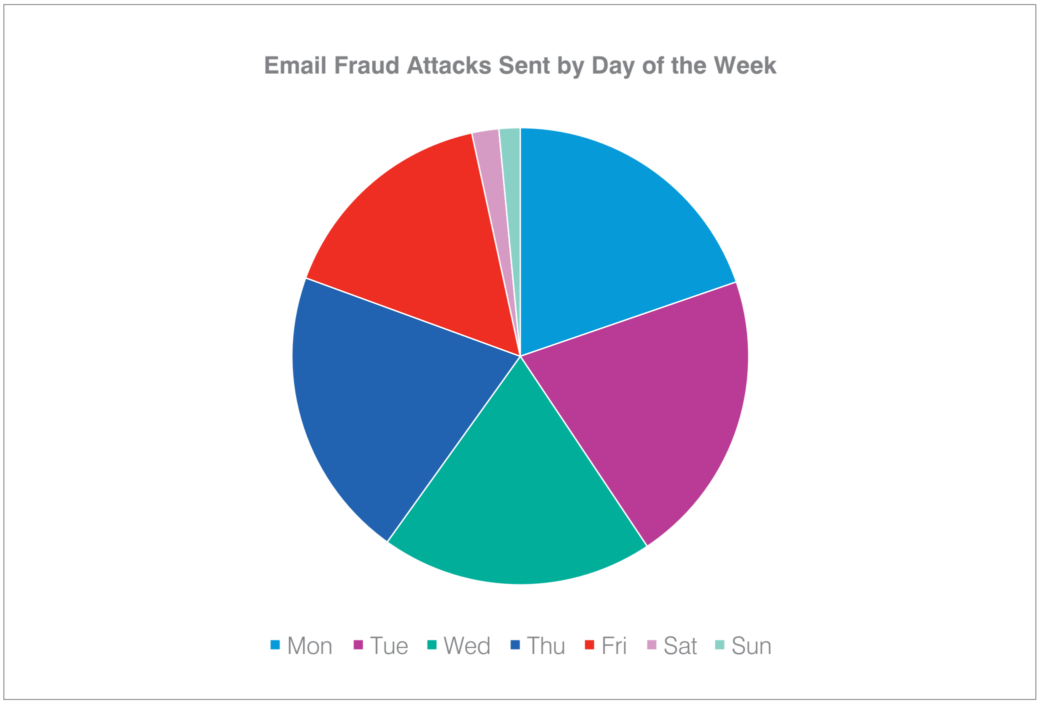
The median number of staff members targeted by email fraud in a given healthcare organization was 23. More than three quarters (77%) of had more than five employees targeted. A mere 7% had just one person targeted.

SOCIALLY ENGINEERED FOR SUCCESS

OVER THE PAST TWO YEARS, THE MOST POPULAR SUBJECT CATEGORIES USED TO TARGET HEALTHCARE ORGANIZATIONS HAVE INCLUDED **"PAYMENT," "REQUEST," AND "URGENT."**

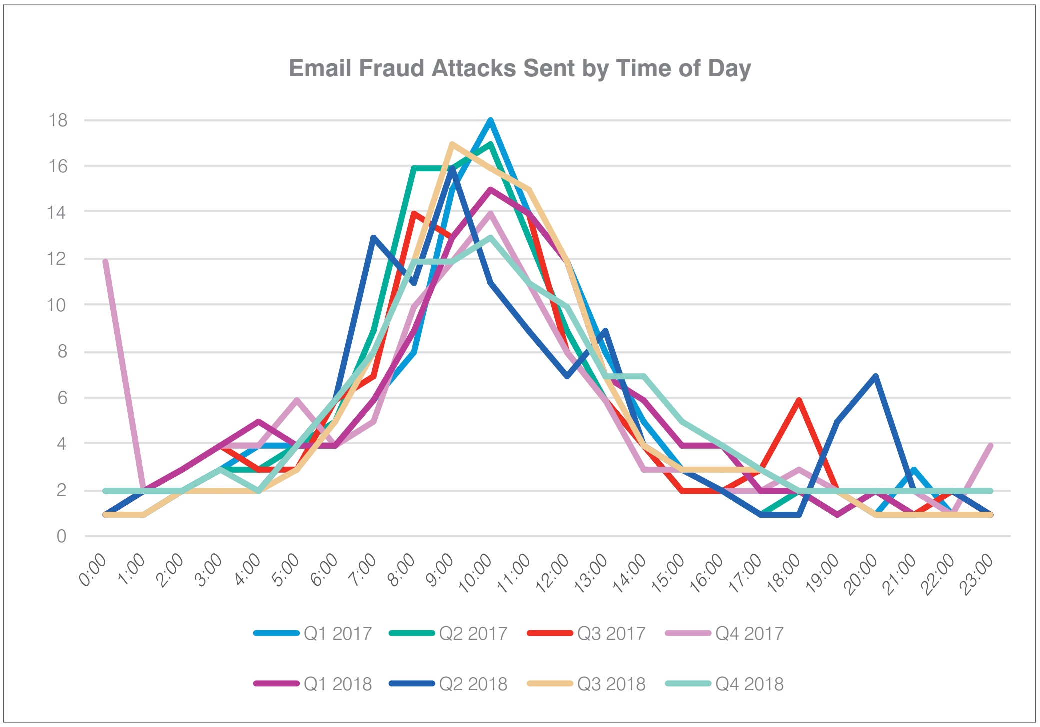


Wire-transfer scams are a huge component of email fraud. Over the past two years, the most popular subject categories used to target healthcare organizations have included "payment," "request," and "urgent."



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.

NEARLY 70% OF ALL EMAIL FRAUD ATTACKS AGAINST HEALTHCARE ORGANIZATIONS ARE SENT **BETWEEN 7 A.M. AND 1 P.M. IN THEIR TARGETS' TIME ZONES.**



Nearly 70% of all email fraud attacks against healthcare organizations are sent between 7 a.m. and 1 p.m. in their targets' time zones. The largest percentage arrives around 9 a.m., near the start of the workday.

TACTICS USED TO TARGET HEALTHCARE ORGANIZATIONS

Email fraudsters use a variety of techniques, often in tandem, to pose as someone the victim trusts or does business with. Here are the most common:

DISPLAY-NAME SPOOFING

Display-name spoofing is when an attacker simply changes an email display name to something that looks legitimate.

Display-name spoofing

Webmail services such as Gmail are the preferred vehicle for email fraud because they're free and easy to use. In email fraud, the attacker simply changes the display name. (Email display names are unrelated to the actual email address being used—they can be anything the sender wants it to be.) Over the course of 2017 and 2018, 33% of email fraud across healthcare used Gmail.com, AOL.com, Comcast.net, Inbox.lv, or RR.com.

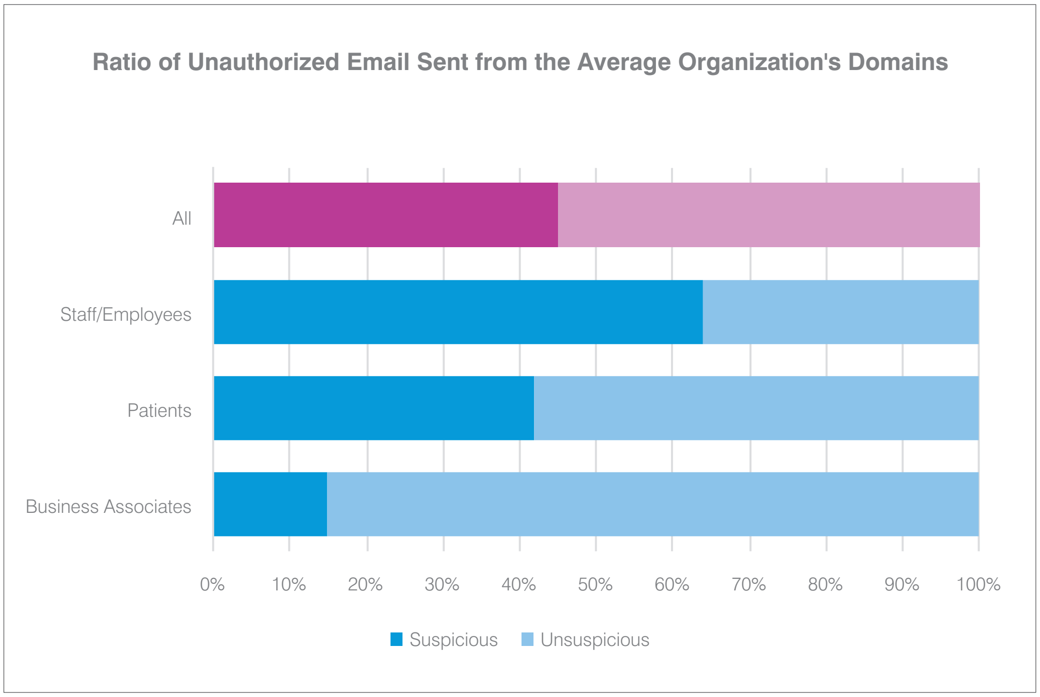
DOMAIN SPOOFING

Domain Spoofing is sending fraudulent emails from an organization's own trusted domain.

Domain spoofing

Another common tactic is sending fraudulent email from the organization's own trusted domain. This is called domain spoofing. Criminals spoof healthcare-owned domains to target the organization's staff, patients and business partners.

In Q4 2018, 95% of healthcare firms were targeted by at least one email fraud attack launched from their own domain. The average organization was targeted with 57 domain spoofing attacks. Every one of companies in our study had their domains spoofed by attackers sending fraudulent messages to patients and business partners.



Overall, 45% of email sent from healthcare-owned domains in Q4 appeared suspicious. The percentage was even higher for email sent to employees, at 65%. Roughly 42% of the email sent to patients from hospital-owned domains was suspicious, as was 15% of email sent to business partners.

LOOKALIKE DOMAINS

Lookalike domains are web and email domains that are created to look similar to a trusted domain in order to appear to be coming from a legitimate source.

Lookalike domains

Attackers often register lookalike web and email domains to trick people into believing an email is sent from someone they trust. They create new, deceptively similar domains by swapping characters (such as replacing the letter “o” with the numeral “0”) or inserting an additional character (such as an “s” or a hyphen). In 2017 and 2018, 67% of healthcare providers were targeted by attacks launched from lookalike domains.

CONCLUSION AND RECOMMENDATIONS

Despite organizations’ large investments in security, email fraud continues to rise. Cyber criminals are growing more advanced. And attacks are evading traditional security tools, leaving people as the last line of defense.

Email fraud tactics are always shifting. That’s why you need a multi-layered defense.

To protect your staff, patients and business partners from email fraud, consider the following:

- **Email authentication (DMARC).** Block all impostor attacks that spoof your trusted domains
- **Machine learning and policy enforcement.** Analyze the contents and context of email to stop display-name spoofing and lookalike domains at the email gateway.
- **Domain monitoring.** Automatically identify and flag potentially risky domains registered by fraudsters.

For the latest threat research and guidance about today’s advanced threats and digital risks, visit **proofpoint.com/us/threat-insight**