proofpoint

REPORT

EMAIL FRAUD THREAT REPORT

YEAR IN REVIEW

proofpoint.com

Email fraud, also known as business email compromise (BEC), is one of today's greatest cyber-threats. These socially engineered attacks seek to exploit people rather than technology. They are highly targeted, sent in low volumes and impersonate people in authority.

Email fraud preys on human nature—fear, the desire to please and more—to steal money and valuable information from employees, customers and business partners.

Proofpoint analysed more than 160 billion emails sent to more than 2,400 companies spanning 150 countries.

Here are our findings for 2017.

EMAIL FRAUD CONTINUES TO SOAR

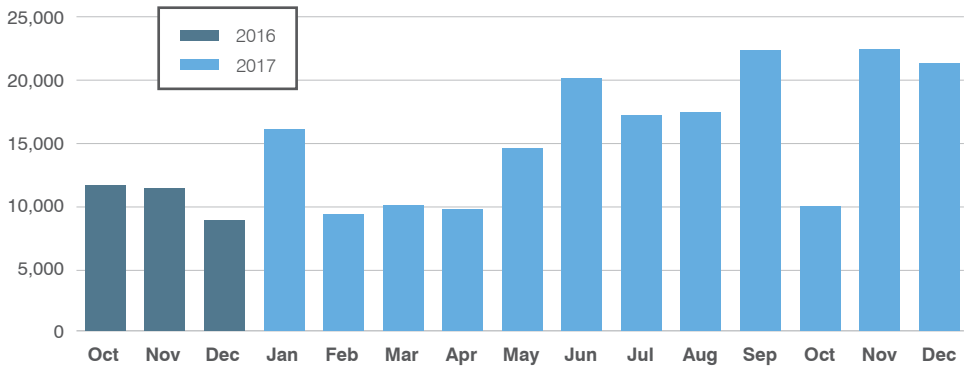
EMAIL FRAUD
In email fraud attacks, an email or series of emails purporting to come from a top executive or partner firm asks the recipient to transfer money or send sensitive information. It does not use malicious attachments or URLs, so it can be hard to detect and stop.

EMAIL FRAUD was rife in 2017. While the threat continues to be highly targeted, attacks were launched against more organisations and more frequently compared to 2016.

The percentage of companies targeted by at least one email fraud attack steadily rose, reaching a new high of 88.8% in Q4. That's up 13.8 percentage points over the 75.0% of organisations targeted in the same quarter last year.

On average, companies were targeted by 18.5 fraudulent emails per quarter, up 17% over the previous year. In sheer volume, the year ended with two of the three biggest quarters that we've ever seen for email fraud.

Business Email Compromise attacks detected and blocked by Proofpoint
Q3 and Q4 represented two of the three biggest quarters we've ever recorded in email fraud volume.



FRAUDSTERS REACH FURTHER DOWN THE ORGANISATION

Criminals have moved beyond CEO-to-CFO spoofing as they expand their reach within organisations.

Spoofing more identities

After holding steady for the first three quarters, the average number of identities spoofed per organisation more than doubled in Q4 to about 10 identities.

This shift makes sense. As security teams ramp up efforts to warn employees of CEO spoofing threats, the bad guys find other authority figures to impersonate. Nearly half (47%) of organisations had more than five identities spoofed in Q4, almost double the previous quarter's total.

Targeting a wider range of roles

The average number of people targeted within a given organisation levelled off in Q4 at about 13. But criminals are targeting people deeper within the organisation and across more business groups, such as HR and accounts payable. In many cases, they can craft a convincing email using social engineering and employee information widely available on the web and social media.

As attackers dug further down the organisation in Q4, 41% of targeted companies faced attacks in which more than five identities were spoofed and more than five employees were targeted.

ONE-TO-ONE ATTACKS

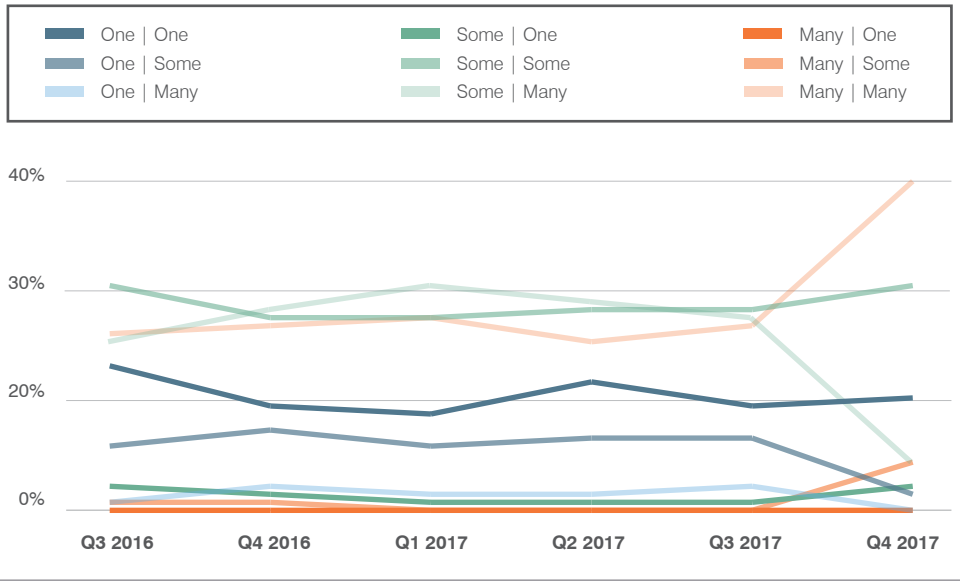
In one-to-one email fraud, an attacker spoofs one identify (typically the CEO) and targets one recipient (typically the CFO).

MANY-TO-MANY ATTACKS

In many-to-many attacks, fraudsters impersonate multiple executives and target several recipients. For example, an attacker might try impersonating several managers and target a company's whole finance team.

Identities Spoofed vs. Emails Sent

Moving on from simple **one-to-one** attacks, fraudsters are impersonating more authority figures and targeting more people within the organisation. We call these **many-to-many** attacks.



TO ATTACKERS, SIZE DOESN'T MATTER

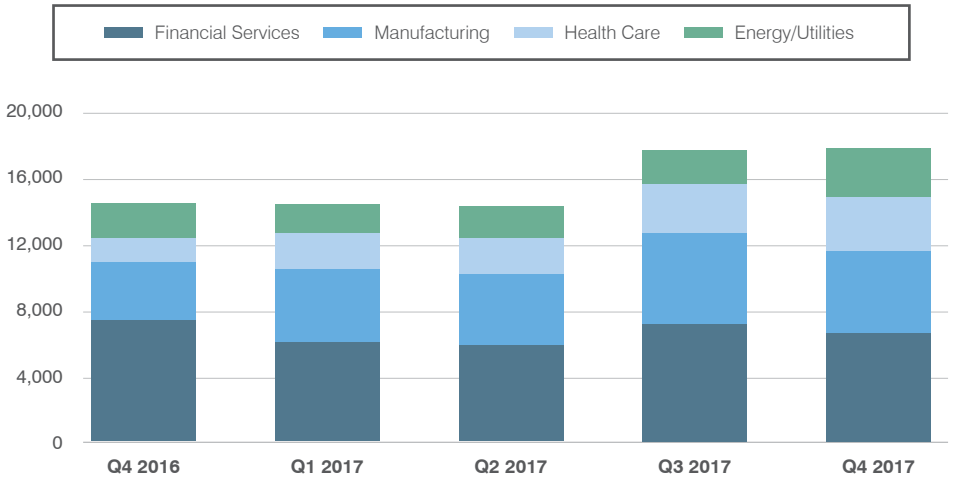
Fraudsters target organisations of all sizes. They are also opportunistic, targeting companies across all industries.

Companies of all sizes attacked

We have seen almost no connection between company size and how often it is targeted by email fraud since we started tracking this information in 2016. Only one quarter (Q2 of 2017) showed any correlation at all—attackers revealed a slight preference for larger targets.

Attackers Target Many Industries

Financial services and manufacturing are among the most frequently targeted. But we have seen widespread email fraud attacks across all industries.



That attacks fall on small and large targets evenly may seem surprising. But from the attacker's point of view, the pattern makes sense. Larger organisations may be richer targets. But smaller entities are often more vulnerable to these advanced threats.

Attackers target many industries

In earlier research, we saw a mostly uniform spread of email fraud attempts across industries. (Though the financial services, manufacturing, healthcare and energy/utility sectors were targeted slightly more frequently.)

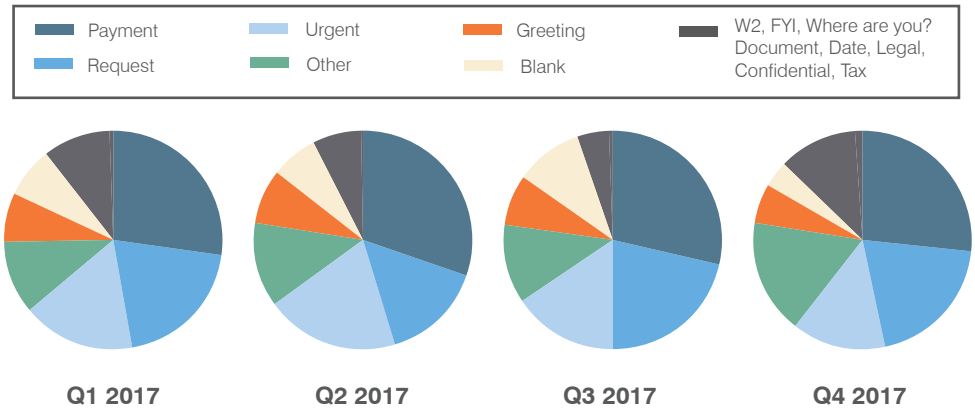
In Q4, attackers targeted new industries. In the property sector, criminals found new ways to cash in on high-value transactions. And in education, attacks jumped 77% from the previous quarter and 120% over the same period in the previous year.

SHIFTING EMAIL FRAUD TACTICS

To evade traditional security tools and reach their victims, fraudsters are always changing their technique.

Subject Lines Used in Email Fraud Attempts

'Payment', 'request' and 'urgent' are always popular subject lines, but we saw a spike in legal-related subjects in Q4.



BANK-TRANSFER FRAUD
In bank-fraud scams the attacker sends an email impersonating an executive. The email tricks the recipient into sending money by disguising the transfer as a normal business transaction or an important deal that requires secrecy.

W2 SCAMS
In this scam, someone spoofing an executive asks the finance department to send employee records. Those records are then used for identity theft and other attacks. It's named after the W2 tax form US employers use to report workers' wages.

Bank-transfer fraud

BANK-TRANSFER FRAUD continues to be the most frequent form of email fraud at nearly 27% of email fraud message volume. Email subject categories usually include some variation of the word 'payment'.

Tax scams

W2 TAX-DOCUMENT SCAMS increased in the first quarters of each of the past two years, probably due to the looming US filing deadline. For instance, we saw a 3,408% spike in Q1 vs. the previous quarter. In Q2 as the filing deadline passed, the volume of these attacks dropped down to a steady rate.

Shifting personas and subject lines

Attackers take on a range of personalities to impersonate a trusted authority. Throughout 2017, email fraud attacks shifted between subject categories that included 'urgent' and those that included 'request'.

'Urgent' and 'request'

Messages that fall under the 'urgent' subject category are typically more direct and concise. Messages that include 'request' in the subject line take a softer approach. They establish more of a back-and-forth rapport before asking for the prized information.

'Legal'

Two more subject categories spiked in Q4: those that included a date and those that included the word 'legal'.

Though still small in absolute terms, attacks that took a 'legal' angle grew 1,850% over the previous year. The most rampant of these scams had an email subject that read 'lawyer's call'.

In these attacks, the fraudster typically tries to move the interaction away from email and direct the bank transfer over the phone. These attacks work because the attacker impersonates someone in authority—but someone whom the victim doesn't normally work with. And because much of the contact takes place offline, these scams are harder for security teams to detect and stop.

Fabricated email histories

Fraud attempts that included fake email histories rose in each quarter of 2017.

This technique uses 'Re:' or 'Fwd:' in the subject line, a false email history, or both. The fabricated email chain appends a realistic-looking email history that suggests that the required stakeholders have already approved the request.

In Q4, more than 11% of all email fraud attacks included a version of this technique. That's up from 7.3% from the same quarter, one year ago.

DOMAIN AND DISPLAY-NAME SPOOFING LEAD ATTACK TECHNIQUES

Over the course of 2017, the mix of email fraud messages shifted between domain spoofing, display-name spoofing and lookalike domain (or cousin domain) attacks.

Domain spoofing

DOMAIN-SPOOFING attacks, in which criminals hijack an organisation's trusted email domains, continue to make up a large portion of email fraud attacks. In Q4, 69% of organisations targeted by email fraud saw at least one domain-spoofing attack. And across all of 2017, nearly 93% of organisations were targeted by one.

Display-name spoofing

DISPLAY-NAME SPOOFING through web-based email services accounted for about 40% of email fraud attacks in Q4. Aol.com and gmail.com were the preferred sending domains for these threats, though attackers also use many other domains.

DMARC adoption

Domain-spoofing attacks can be prevented by implementing **DMARC** email authentication. It's no wonder we saw significant initiatives to increase DMARC adoption in 2017.

In October, the US Department of Homeland Security issued Binding Operational Directive 18-01. The directive aims to increase security for people who receive email from federal agencies or visit a federal website. A key part of the directive orders all civilian federal agencies to deploy DMARC quickly.

At the time the directive was announced, nearly 1 in every 8 emails sent from a .gov email address was fraudulent. Only about 17% of the agencies had adopted DMARC.

About 90 days into the initiative, that percentage has more than tripled. Nearly 52% of agencies have hit the first DMARC milestone deadline.

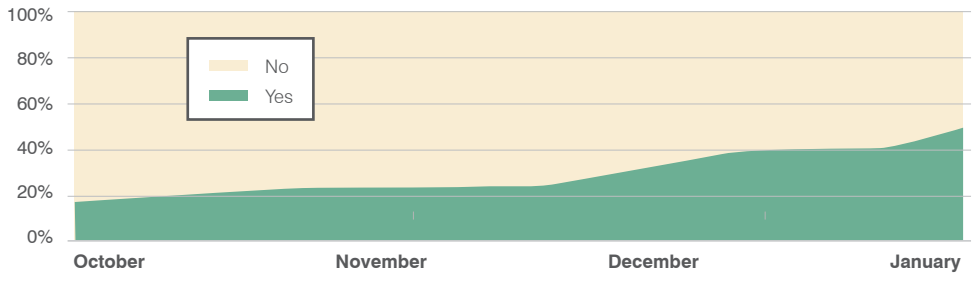
DOMAIN SPOOFING
Spoofing impersonates trusted colleagues or contacts by making an attacker's emails appear to come from a legitimate and expected address.

DISPLAY-NAME SPOOFING
Display-name spoofing places a familiar name and email address in the 'From:' field that users see on incoming emails. When the recipient replies, the response actually goes to the address specified in the email's 'Reply to:' header.

DMARC
DMARC, which stands for 'Domain-based Message Authentication, Reporting and Conformance', is an email authentication protocol that can prevent many email fraud attacks.

US Federal DMARC Deployment Among Civilian Agencies

More agencies are rolling out email authentication in the wake of a US federal directive. But nearly half have still not met the first milestone.



Shortly after the directive was announced, the National Health Information Sharing and Analysis Center (NH-ISAC)—an industry group that helps healthcare providers share security information—asked its members to pledge to deploy DMARC in 2018.

A CLOSER LOOK AT LOOKALIKE DOMAINS

LOOKALIKE-DOMAIN SPOOFING

In lookalike-domain spoofing, attackers register domain names deceptively similar to those of trusted brands.

LOOKALIKE-DOMAIN SPOOFING, in which the attacker registers a domain confusingly similar to a trusted domain, is another effective tactic. Attackers trick people into giving up valuable information with emails that appear to be from someone familiar.

Attackers craft these impostor domains by making small, hard-to-notice changes to the original domain. They may swap out individual characters, such as the numeral 0 in place of the letter O. Or they may insert characters, such as adding an S at the end of the domain.

The volume of lookalike-domain attacks is not as high as display-name and domain-spoofing attacks. That's probably because the technique requires the attacker to register a domain, which costs money. But given that a single trusted domain name could have countless similar-looking variations, attackers have many openings to launch such attacks.

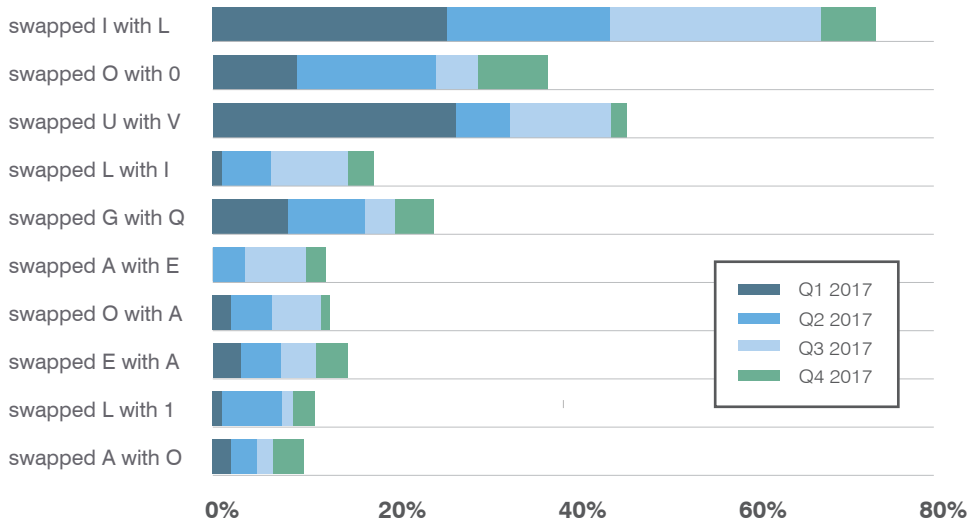
Character shifting

Like other email fraud tactics, lookalike-domain techniques change every quarter. But looking across 2017, individual character swapping was the most popular, occurring nearly 38% of the time. The most common swaps were:

- An L in place of an I (17.4%)
- The numeral 0 for the letter O (8.7%)
- V for U (8%)

Character-Swapping in Lookalike Domains

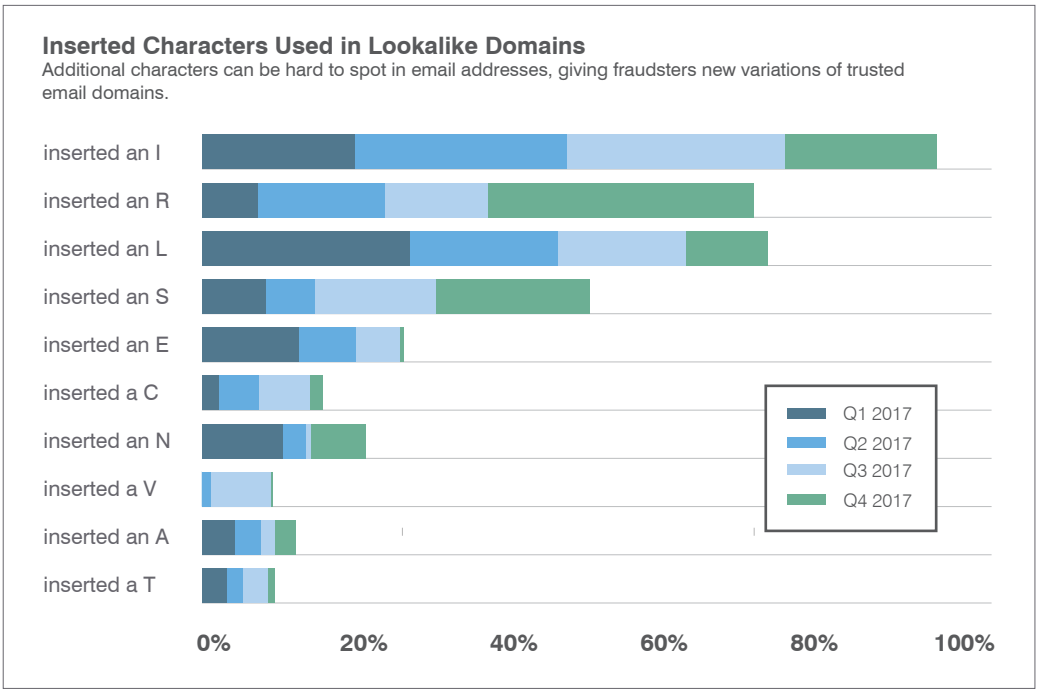
Because some characters resemble others, fraudsters have many options for creating domains that look like yours.



Inserting characters

Impostor domains that inserted an additional character occurred about 34% of the time over the year. The most common inserts were:

- An I (23.7%)
- An R (19.3%)
- An L (15.4%)



Other techniques

Another popular technique is adding or removing a leading or trailing character within the domain. This approach accounted for about 13% of registered lookalike domains.

Other lookalike-domain spoofing tactics include:

- Hyphenating
- Removing characters
- Using typographs and **HOMOGRAPHS**

HOMOGRAPH SPOOFING

Homograph spoofing mixes character sets from different languages to create lookalike domains that appear identical to people but are actually different to a computer. For example, an unsafe domain that uses the Cyrillic A would look the same as a trusted domain that uses a Latin A.

CONCLUSION AND RECOMMENDATIONS

Despite organisations' large investments in security, email fraud is on the rise. Cybercriminals are becoming more advanced. They are evading traditional security solutions, leaving employees as the last line of defence.

Email fraud tactics are always shifting. That's why you need a multilayered defence that includes:

1. **DMARC email authentication**. Block all impostor attacks that spoof trusted email domains.
2. **Dynamic classification**. Analyse the content and context of the email to stop display-name spoofing and cousin domain tactics at the email gateway.
3. **Lookalike domain discovery.** Identify and flag potentially risky domains registered by third parties.
4. **Data loss prevention.** Prevent sensitive information, such as W2s, from leaving your environment.

ARE YOU EQUIPPED TO STOP EMAIL FRAUD?

Get a free DMARC assessment to quickly understand your potential exposure to risk and see how DMARC authentication can help you prevent email fraud.

proofpoint.com/au/learn-more/dmarc-assessment

ABOUT PROOFPOINT

Proofpoint, Inc. (NASDAQ:PFPT), a next-generation cybersecurity company, enables organisations to protect the way their people work today from advanced threats and compliance risks. Proofpoint helps cybersecurity professionals to protect their users from the advanced attacks that target them (via email, mobile apps and social media), protect the critical information people create, and equip their teams with the right intelligence and tools to respond quickly when things go wrong. Leading organisations of all sizes, including over 50 per cent of the Fortune 100, rely on Proofpoint solutions, which are built for today's mobile and social-enabled IT environments and take advantage of both the power of the cloud and a big-data-driven analytics platform to combat modern advanced threats.

proofpoint. www.proofpoint.com

0118-051