EBOOK

proofpoint.

STOPPING EMAIL FRAUD

HOW PROOFPOINT HELPS PROTECT YOUR ORGANISATION FROM IMPOSTORS, PHISHERS AND OTHER NON-MALWARE THREATS

Today's email attacks have evolved. Unfortunately, most security tools haven't evolved with them.

Attackers are moving and adapting faster than most cyberdefences. They're bypassing security tools with new techniques and delivery methods. And some are avoiding legacy controls altogether through novel attacks that don't use malware at all.

Email fraud, sometimes called business email compromise (BEC), is one of them. Cybercriminals can easily spoof executives and business partners to trick people into sending money and other valuable information.

This growing threat has cost victims more than $6 billion since the FBI began tracking it in late 2013.[1] The average attack nets about $107,000.[2]

Partner spoofing attacks, where a fraudster pretends to be an organisation's trusted vendor, are also growing. In just one example, a Lithuanian man is accused of stealing more than $100 million in separate attacks on Google and Facebook in July 2017.[3] The man allegedly spoofed a vendor in the companies' supply chains.

These attacks are sophisticated and highly targeted. They exploit people, not technology. And stopping them requires a new people-centred approach.

Proofpoint Advanced Email Security uses a multilayered defence to stop unsafe email from reaching people's inbox—and keep sensitive information in your environment when something goes wrong.

1 FBI Internet Crime Complaint Center. '2017 Internet Crime Report'. May 2018.
2 Ibid.
3 Reuters. 'Lithuanian court upholds extradition of man to U.S. in $100 million fraud case'. August 2017.

Email fraud has cost victims more than

$6 BILLION

since the FBI began tracking it in late 2013.

The average attack nets about

$107,000

A Lithuanian man is accused of stealing more than

$100 MILLION

in separate attacks on Google and Facebook in July 2017.

DEPLOYING A MULTILAYERED DEFENCE: AN ANALOGY

Consider how airports manage a vast and changing mix of potential security issues. Most take a two-pronged approach, each of those prongs featuring multiple checks and procedures. At Proofpoint, we take a similar approach to securing your email. This guide explains how our multilayered defence uses identity control and content analysis to protect organisations from email fraud.

1 First, they check the flyer's passport and boarding pass to ensure that the person is authorised to travel and is, indeed, who the person claims to be. We call this identity control.

2 Second, the airport screens the luggage and has the person pass through an X-ray machine or scanner. This ensures that nothing bad is getting on the plane and that nothing's leaving that shouldn't be. We call this content analysis.

IDENTITY CONTROL: WHO'S REALLY SENDING THAT EMAIL?

Email fraud can be hard to detect with conventional cyberdefences. That's because it is highly targeted and sent in low volumes aimed at specific people or job roles. These emails don't have a payload. So there's no attachment or URL for security tools to detect, analyse and sandbox.

The messages are socially engineered for one sole purpose: tricking people into doing something on the attacker's behalf.

Due to the nature of email fraud, you need to validate the true identity of the email sender. If you can verify whether the email was sent by who it says it's from—and block any impostors—you can stop many of these threats outright.

JUMP TO AUTHENTICATION >

JUMP TO LOOKALIKE DOMAINS >

AUTHENTICATION

For identity control, we start with email authentication. This step stops attackers who try to hijack your email domain, a technique called domain spoofing. With email authentication, only someone from your company—or someone you authorise—can send email using your domain. This stops many attacks in their tracks.

DMARC authentication allows email senders to indicate that their messages are protected by two popular authentication techniques. And it and tells receivers what to do if neither of those authentication methods passes.

Proofpoint helps you to implement DMARC authentication quickly and confidently. We give you visibility into all the email coming into and going out of your organisation. With this visibility, you can authorise all legitimate senders trying to send emails on your behalf—and block any malicious emails spoofing your trusted domains or those of your suppliers.

LOOKALIKE DOMAINS

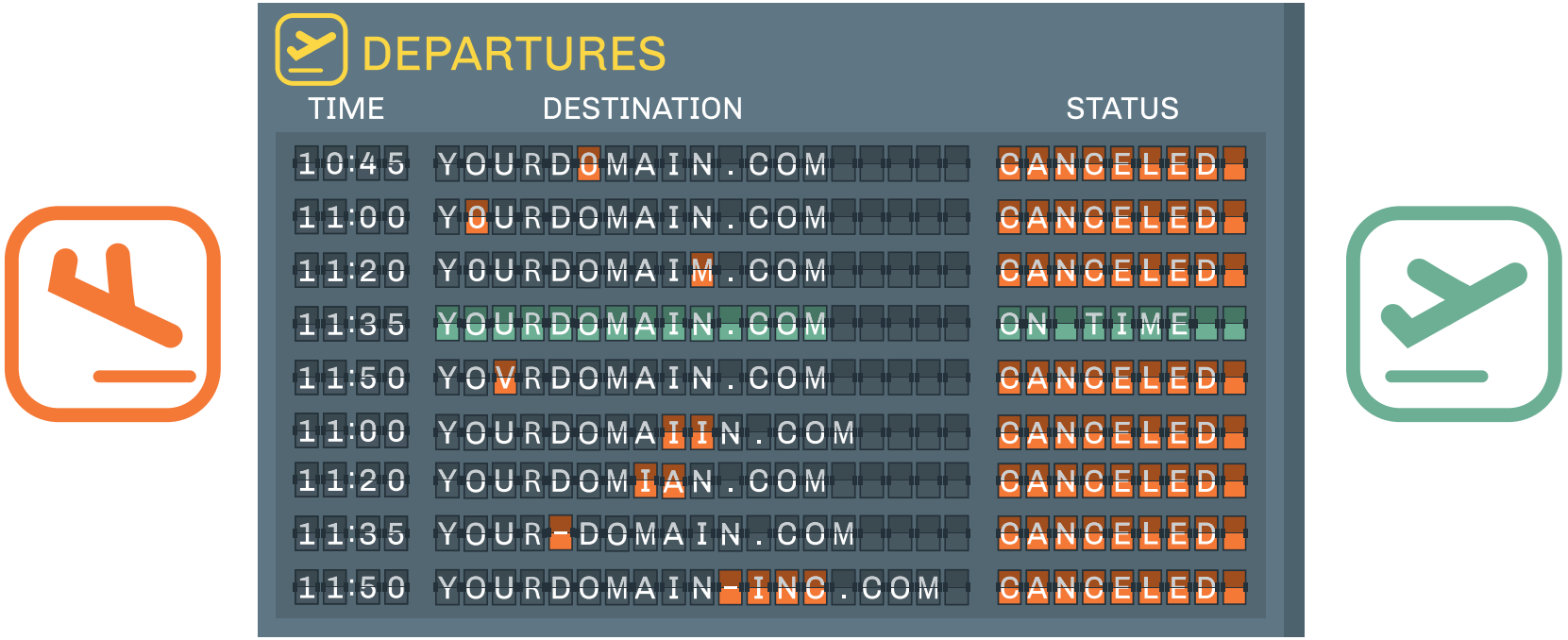
But even with authentication, it's easy for attackers to register domains that look a lot like yours. This tactic is sometimes called 'typosquatting'.

Some lookalike domains may swap out characters, such as the numeral '0' for the letter 'O', an uppercase 'I' for a lowercase 'L', or a 'V' for a 'U'. Others might insert additional characters, such as an 'S' at the end of the domain name, that a casual viewer won't easily notice.

Still others might use typographs or homographs—characters that look just like Latin characters to a human reader but are actually different to a computer. A domain that uses the Cyrillic 'A', for example, looks the same as one that uses a Latin 'A'. But the Cyrillic version could be registered separately by an email attacker.

There are countless combinations fraudsters can use to counterfeit trusted email domains. And unless your organisation has registered them all, DMARC alone won't stop them.

That's why we also help you to find lookalike domains—and shut them down before attackers get the chance to use them.



CONTENT ANALYSIS: WHAT'S IN THE EMAIL?

While domain spoofing and lookalike domains are common tactics used to commit email fraud, fraudsters have other ways of reaching their targets. You need to be able to identify malicious emails that show up at your gateway and block them before they reach your employees.

JUMP TO DYNAMIC CLASSIFICATION >

JUMP TO DATA LOSS PREVENTION >

JUMP TO DISPLAY NAME SPOOFING >

With Proofpoint Advanced Email Security, you can stop advanced attacks, mitigate their impact and keep your business running.

DYNAMIC CLASSIFICATION

Beyond authentication and lookalike domain protection, another layer of defence against email fraud attacks is **dynamic classification.** Dynamic classification analyses and manages email based on several factors, including:

- The email's content
- The sender's reputation
- The relationship between the sender and recipient

We typically look at several factors. Does the email come from a trusted sender—and does that sender have a good reputation? Does the email include a suspicious subject? Do the sender and the receiver have an existing email relationship? Does the body of the email look suspicious?

We score the email based on its level of riskiness. Then you can decide what to do with it according to that score—let it through, block it or route it to a quarantined folder.

DATA LOSS PREVENTION

The final layer is **data loss prevention, or DLP**. If an unsafe message somehow gets through all your other layers and manages to trick someone in your organisation, DLP can make sure that no sensitive information leaves your environment.

Our smart identifiers detect and analyse email fraud-related content, such as tax records and bank transfer information. These identifiers work within the email body and across a range of file types, including Microsoft Word, Adobe Acrobat and photo files.

DISPLAY-NAME SPOOFING

No matter what other tactics they use, most attackers spoof the sender display name in fraudulent emails. The display name is what appears in the 'From:' field when reading the message. It's unrelated to the sender's actual email address or where any replies are sent—it can be anything.

In display name spoofing, the attacker uses a familiar name to gain the recipient's trust. Fortunately, our dynamic classification capabilities detect, analyse and block email that spoofs display names at the gateway.

A COMPLETE SOLUTION

Today's email threats require complete email protection. That's why our multilayered approach solves your entire email security challenge—not just parts of it. With Proofpoint Advanced Email Security, you can stop advanced attacks, mitigate their impact, and keep your business running.

With **Proofpoint Email Protection** you can configure anti-spoofing policies and classify each email. Our Impostor Classifier blocks display-name and lookalike-domain spoofing at the gateway.

Proofpoint **Email Fraud Defense** gives you the visibility, tools and services to help you implement DMARC authentication quickly and confidently. With DMARC, you can automatically block attacks that spoof your trusted domains.

Proofpoint **Domain Discover** for Email automates the process of identifying, analysing and taking down malicious lookalike domains.

Finally, Proofpoint **Email Data Loss Prevention** helps you understand and act on the sensitive information leaving your environment through email.

COMPLETE VISIBILITY

- POLICY
- AUTHENTICATION
- CLASSIFICATION
- LOOKALIKE DOMAIN DISCOVERY
- ADVANCED DLP

FIND OUT MORE

To find out more about how Proofpoint can help you to stop email fraud, visit proofpoint.com/email.

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 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 utilise both the power of the cloud and a big-data-driven analytics platform to combat modern advanced threats.