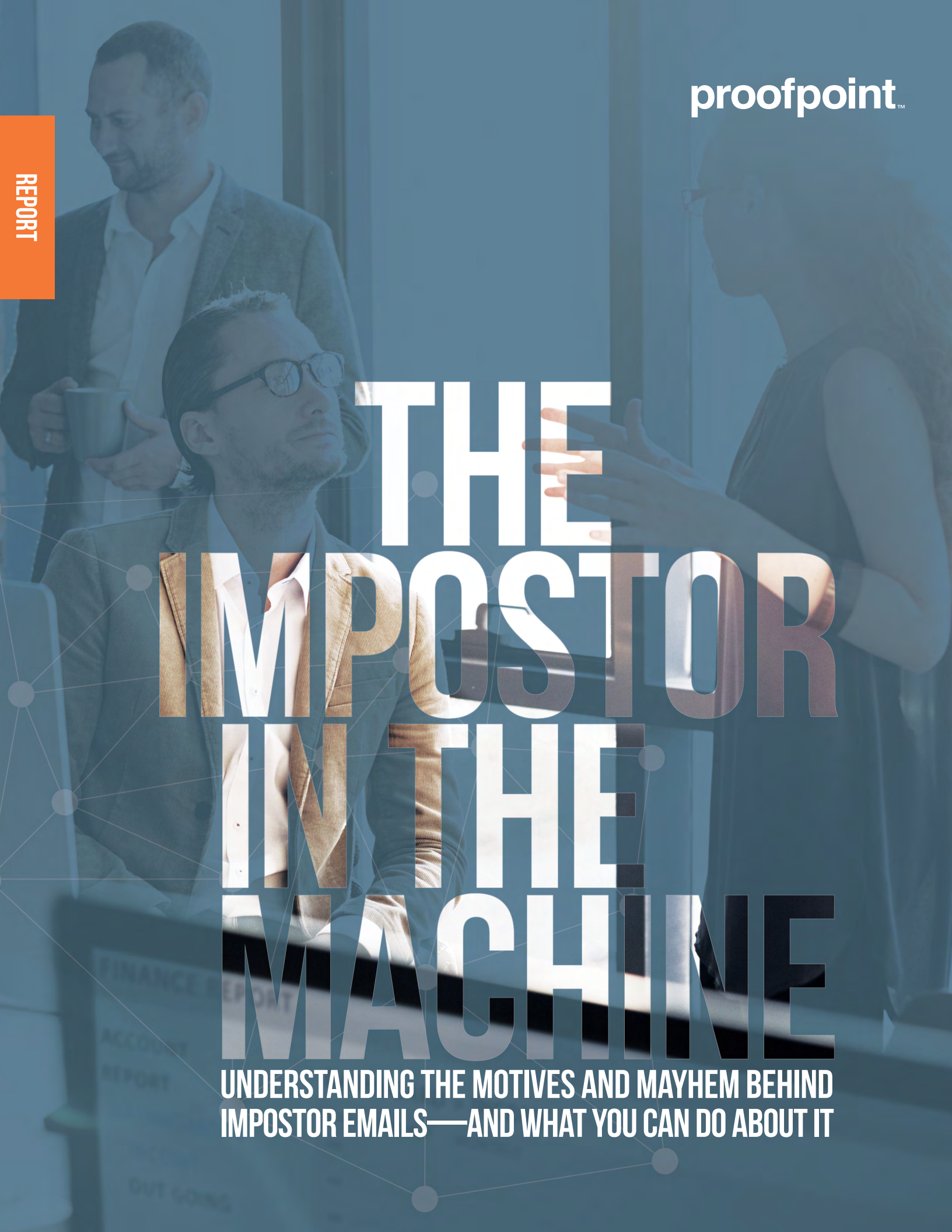


proofpoint™

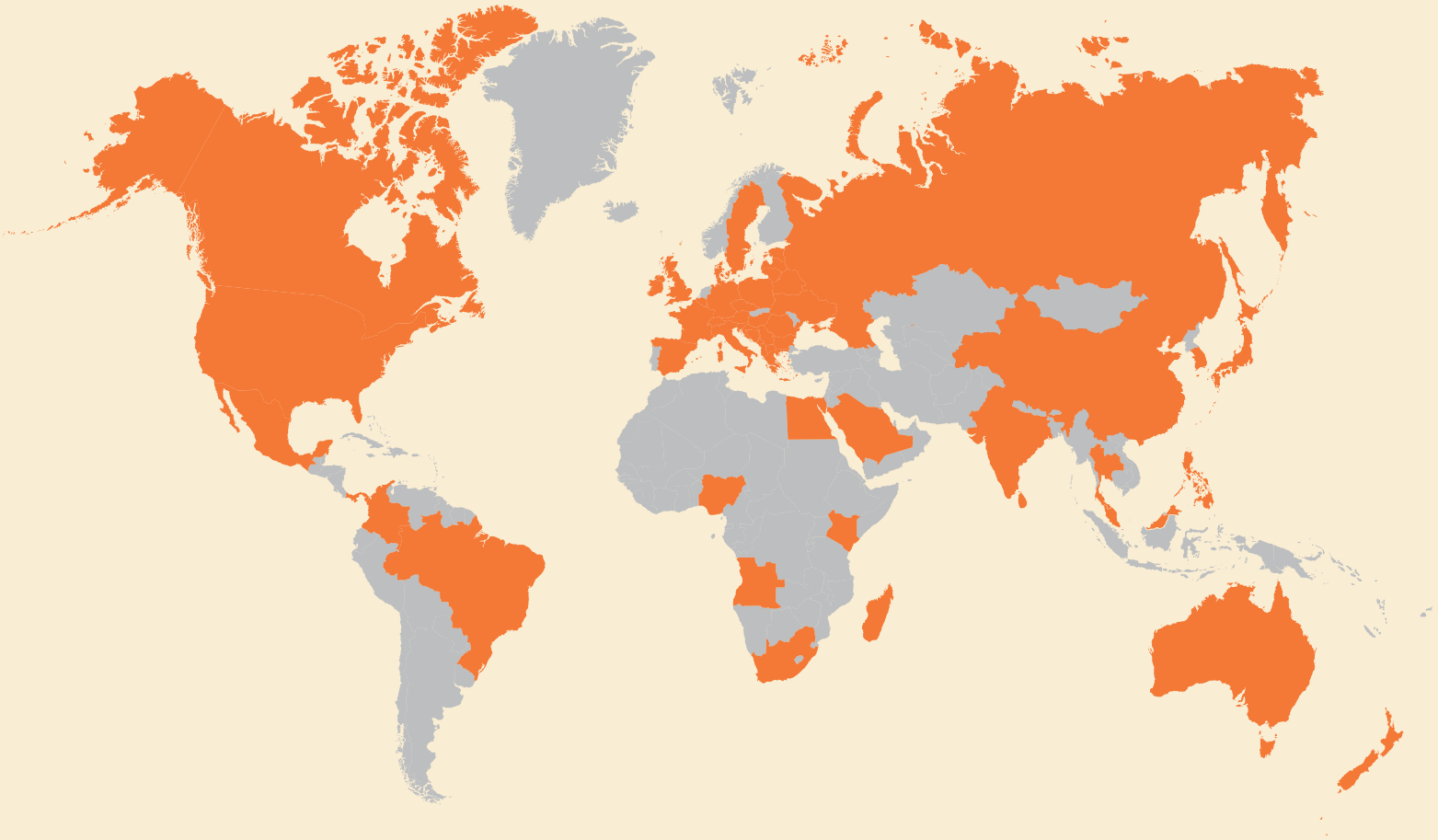
REPORT

THE IMPOSTOR IN THE MACHINE

UNDERSTANDING THE MOTIVES AND MAYHEM BEHIND IMPOSTOR EMAILS—AND WHAT YOU CAN DO ABOUT IT

IMPOSTOR EMAIL IS AN EMERGING GLOBAL THREAT

THE ORANGE PORTIONS OF THE INFOGRAPHIC SHOW THE WIDE SPREAD IMPACT OF IMPOSTOR EMAILS WORLDWIDE.



SOURCE: fsroundtable.org/business-email-compromise-costing-its-victims-millions-simple-tips-can-help-foil-fraudsters

THE IMPOSTOR IN THE MACHINE

UNDERSTANDING THE MOTIVES AND MAYHEM BEHIND IMPOSTOR EMAILS—AND WHAT YOU CAN DO ABOUT IT

Advanced threats are shifting once again, and you and your company will likely become the target of a new type of threat. Carefully planned and researched, impostor emails target specific people in your company. Either you become the target of this attack or you become the unwitting victim. Impostor emails do not use malware or URLs found in typical credential phishing schemes.

Dubbed "business email compromise" by the FBI, also known as CEO fraud, man-in-the-email, whaling attacks and other unsavory titles, impostor emails are purpose-built to impersonate C-level executives and trick unsuspecting employees. According to the Internet Crime Center (IC3) of the FBI, impostor attacks increased by more than 270% in 2015 alone. Victim companies come from all 50 U.S. states and nearly 80 countries, resulting in more than $2 billion in losses since late 2013.[1]

You may not even know you are a victim of an impostor email right away. Security tool alarms do not go off. There is no ransom note. Your systems continue to run and everything seems like business as usual. That is the point.

Global in scope, impostor emails have grown to target companies both large and small in every part of the world. From New Zealand to Belgium, companies from every industry have suffered tremendous losses.

Here is a small sampling of recent impostor attacks during the last year:

- A Hong Kong subsidiary at Ubiquiti Networks, Inc. discovered that it had made more than $45 million in payments over an extended period to attackers using impostor emails to pose as a supplier.[2]
- Crelan, a Belgian bank recently lost more than $70 million due to impostor emails, discovering the fraud only after the company conducted an internal audit.[3]
- In New Zealand, a higher education provider, TWoA, lost more than $100,000 when their CFO fell victim to an impostor email, believing the payment request came from the organization's president.[4]
- Luminant Corp., an electric utility company in Dallas, Texas sent a little over $98,000 in response to an email request that they thought was coming from a company executive. Later it was learned that attackers sent an impostor email from a domain name with just two letters transposed.[5]

THE IMPOSTORS AT YOUR GATES

Successful impostor emails result from employing a variety of research strategies against your company. Activities may include scouring social media sites and news announcements to rummaging through company trash to learn more about company business, executives, and their direct reports. You may receive cleverly disguised phone calls on a variety of subjects aimed at learning more about your personnel, customers, and suppliers. Understanding your business process and partners is crucial to a successful attack.

Attackers with a sound reconnaissance strategy invest money and time in intelligence gathering. The first step is qualifying a worthy target. If you have many supply partners and executives that frequently travel abroad, your company is the ideal target for an impostor email. Taking advantage of the time difference and the many hours an executive spends in transit and unreachable is key to a successful attack.

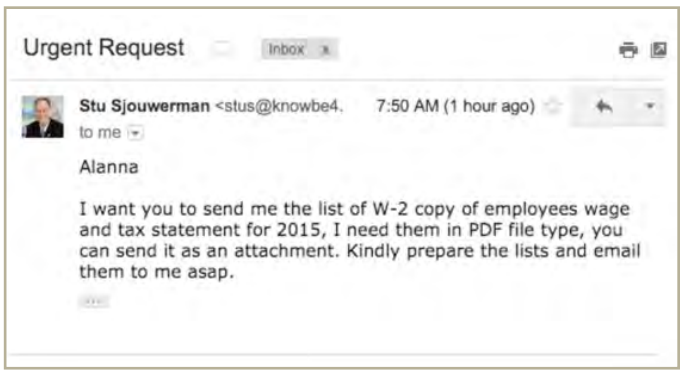
There are two angles involved with targeting executives. In the case of the always-traveling executive, this is the person attackers study and seek to impersonate. They use every resource available to understand the targets schedule, familiar language, peers, and direct reports. It is very likely your company will receive phone calls to gather more information to learn about suppliers and customers. For example, knowing your companies travel agency can be valuable information to an attacker.

Often times, the CEO is the always-traveling executive, hence the name CEO fraud. So on the receiving end, a C-level executive with financial authority could be the one that receives the last minute "before I board the plane request" from the CEO. Instructions may include wire transferring a payment to a supplier who happens to be located in the same area the CEO is visiting.

This scenario can easily victimize any executive's direct reports who routinely process payments. Another ploy involves understanding your suppliers, how they invoice, and using their language, forms, and procedures to, for example, change bank account information for an upcoming payment. If the attackers are successful, you may have been making payments to them for months without ever knowing it.

HOW IMPOSTORS FAKE YOU OUT

LinkedIn and other social media sites are the "go to" resource for profiling targets and the intended victims. Attackers profile C-level executives by examining content within social media sites, company PR releases and any news articles about the business. From there, social sleuthing efforts uncovers your direct reports. New employees in accounting and finance positions are highly coveted by attackers that use impostor



emails. They make the perfect victim for an impostor attack. Being new to the organization, they may not have the innate sense that something may be off with a payment request. They don't know enough about your suppliers or may be in a rush to make a good impression and not know when to slow down and question a transaction.

Once research on your company and executives is complete, they now have a complete profile of your company. They will also have a good portion of your business relationships outlined and maybe know about a couple of special corporate projects or code names. They have dossiers on most C-level executives, especially those in financial positions; they will know who their direct reports are and what their function is. In the next phase, they pull out the technological trickery designed to impersonate your company, or any executive they deem worthy. Alternatively, they may decide to impersonate one of your regular suppliers or maybe an accounting firm that works with your company.

If attackers intend to impersonate someone inside your company, they may register a domain name that is one or two letters off from yours. This creates a look-alike domain for use in the impostor email along with spoofed email addresses of executives previously profiled. Often times, attackers create domain and email addresses just hours before sending the impostor email. In other cases, they may do the same thing but mimic a supplier or another company such as an accounting or law firm that routinely requests payment from you.

THE IMPOSTOR EMAIL—FAKING IT UNTIL THEY MAKE IT

Attackers may begin contact with your company in a variety of ways. However, it usually boils down to a one shot email or a more conversational approach involving several emails and phone calls.

THE ONE SHOT DEAL

The one-shot impostor email relies heavily on sending the email at the perfect time. Ideally, attackers time the sending of an impostor email to coincide with their target's travel schedule. They may already have access to one or more employees' inboxes in order to pull this off. Attackers lie in wait to take advantage of the most opportune time to approach the victim with an impostor email. The message may come across as urgent, "I need the wire-transfer to be completed before I reach Hong Kong." On the other hand, it could be more nonchalant "I am just about to board the plane and I almost forgot we need to wire a payment to…"

OFTEN TIMES, ATTACKERS CREATE DOMAIN AND EMAIL ADDRESSES JUST HOURS BEFORE SENDING THE IMPOSTOR EMAIL

In many cases, impostor emails go undetected. After all, the emails don't include malware, URLs or malicious attachments. It is just a simple text message from a domain with no reputation score. Sometimes messages may even include, "Sent on my iPad" or something similar in the signature line to help disguise poor grammar typically found in impostor emails coming from another country.

Wealth management and investment firms are also targets of the one-shot approach. In this case, it involves targeting high net worth investors with substantial equities. Their financial advisor then becomes the victim. Attackers zero-in on wealthy investors, in the same way they target C-level executives. They profile investors and learn about their financial connections to help them make a falsified wire transfer request appear legitimate.

Another example of the one-time impostor email does not necessarily ask for a wire transfer but may ask for sensitive information in quick one-liner emails. For example, an impostor email that is currently circulating asks for employee W2s under the guise of a "wage review". This type of email may target a C-level human resources executive by sending an impostor email requesting the W2s to one or more of their direct reports.

THE CONVERSATIONALIST

Sometimes impostor email unfold over an extended period. In this approach, the target could be an executive involved with M&A activity, new products, or strategic partnerships. In this case, attackers create an impostor email as the way to inform the victim about an upcoming acquisition, partnership, or other hush-hush project calling for an upcoming wire transfer. These impostor emails usually ask for secrecy and discretion in performing the wire transfer as it involves a top-secret company activity. Impostor emails appear credible, often citing closely held project details or company code names. In this case, the impostor lures the victim into doing their bidding under a veil of secrecy.

The conversationalist may also imitate a supplier and start out an innocent-seeming conversation about the latest invoice status. If answered, the conversation can quickly grow into changing bank account information. Sometimes, impostor emails contain fictitious email conversations between key executives to back-up their need for a wire transfer. If the victim has not caught on to the ruse and the spoofed email addresses and requests look legitimate enough, impostor emails can silently siphon funds from your company over an extended period.

What makes the conversationalist threat brazen is that it often includes a phone call to get past policies requiring verbal confirmation of payment requests. In some cases, the impostor email may include contact information for a third party, for example, a person that supposedly works at your company's accounting or law firm to contact for further instructions. Contact phone numbers are then set-up in anticipation of a follow-up call. Attackers may preemptively call ahead of time to let the victim know the request is coming. This commonly takes place during non-work hours when an attacker may know that the target executive is abroad, in transit, or otherwise not reachable.

DEALING WITH THE IMPOSSIBLE IMPOSTOR

There are a number of approaches to take to protect your company against impostor emails. While these measures are helpful, they are not a cure-all defense against the determined impostor.

SECURITY AWARENESS TRAINING

Training tops the list of strategies to combat against these type of attacks. This can range from a friendly email reminder to look twice at any payment request, to online classes designed to help employees spot an impostor email. Typically, training comprises how to examine email addresses for authenticity and being aware of emails calling for secrecy or acting quickly.

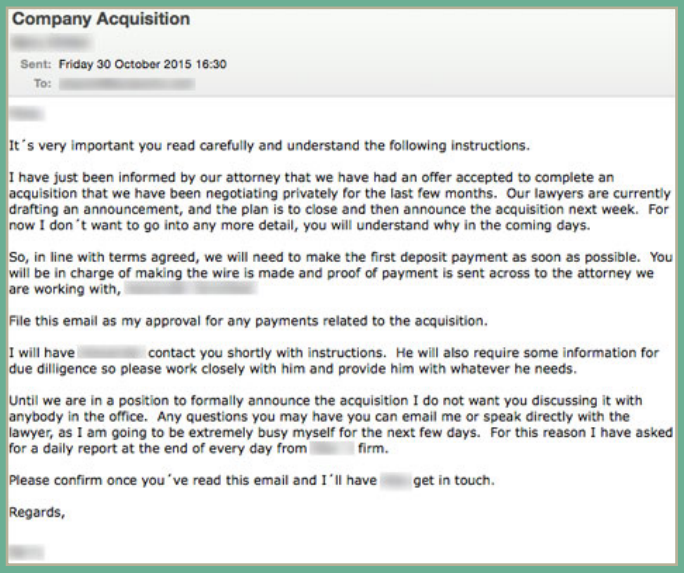
While training should always be an integral part of a security program, adding another facet to an already long list of things employees need to pay attention to is not very impactful. Especially, when considering these impostor emails are highly targeted to take advantage of executive travel schedules and specific knowledge about the company and personnel.

AUTHENTICATION STANDARDS

DMARC and DKIM filters out some impostor emails, but not all. DMARC is a relatively new standard and many regional ISPs are still in the planning stages of implementation, so usage is inconsistent across geographies. It also cannot protect against attackers using display name spoofing, similar sounding domains, or DNS servers publishing phony routing information.

Sender Policy Framework (SPF) will cut down on some variants of email spoofing, but it cannot detect impostor emails that come from an intentionally misspelled domain.

NEW EMPLOYEES IN ACCOUNTING AND FINANCE POSITIONS ARE HIGHLY COVETED BY ATTACKERS THAT USE IMPOSTOR EMAILS. THEY MAKE THE PERFECT VICTIM FOR AN IMPOSTOR ATTACK. BEING NEW TO THE ORGANIZATION, THEY MAY NOT HAVE THE INNATE SENSE THAT SOMETHING MAY BE OFF WITH A PAYMENT REQUEST.



Company Acquisition

Sent: Friday 30 October 2015 16:30
To:

It´s very important you read carefully and understand the following instructions.

I have just been informed by our attorney that we have had an offer accepted to complete an acquisition that we have been negotiating privately for the last few months. Our lawyers are currently drafting an announcement, and the plan is to close and then announce the acquisition next week. For now I don´t want to go into any more detail, you will understand why in the coming days.

So, in line with terms agreed, we will need to make the first deposit payment as soon as possible. You will be in charge of making the wire is made and proof of payment is sent across to the attorney we are working with,

File this email as my approval for any payments related to the acquisition.

I will have contact you shortly with instructions. He will also require some information for due diligence so please work closely with him and provide him with whatever he needs.

Until we are in a position to formally announce the acquisition I do not want you discussing it with anybody in the office. Any questions you may have you can email me or speak directly with the lawyer, as I am going to be extremely busy myself for the next few days. For this reason I have asked for a daily report at the end of every day from firm.

Please confirm once you´ve read this email and I´ll have get in touch.

Regards,

IMPROVE PAYMENT VERIFICATION PROCEDURES

Establishing increased policies around payments is another way companies seek to protect themselves from impostor emails. The FBI suggests implementing a two-step verification process that includes checks via phone calls. Using encrypted email can also help ensure employees are communicating with intended parties.

Improving payment policies can definitely help, but it may not guard against the determined impostor who set-up dedicated phone numbers for verification or reaches out to employees with authentic sounding follow-up calls. It also may fail when dealing with employees who are new, in a hurry, or have a situation that does not conform to policy guidelines.

DEFENSES AGAINST IMPOSTOR MAYHEM

Impostor emails are a result of attackers shifting tactics to evade security solutions that are designed to detect malware attachments and malicious URLs, It is important to remember that impostor emails are one-off emails, not an attack campaign like Dridex. Therefore, while impostor emails happen in just about every country, their actual numbers are very small. Lack of volume makes it easier for impostor emails to get to your employees since traditional defenses generally require a sample before they are able to detect these emails.

The best way to safeguard your company against impostor emails is a combination of improving corporate policies and using a next-generation email security solution. Companies need to adopt solutions that do not solely depend on reputation and basic email filtering. With granular controls, next-generation email solutions can identify and quarantine impostor emails before they ever reach an employee's inbox. Only then, can you significantly reduce the mayhem this type of threat brings to your organization.

WITH GRANULAR CONTROLS, NEXT-GENERATION EMAIL SOLUTIONS CAN IDENTIFY AND QUARANTINE IMPOSTOR EMAILS BEFORE THEY EVER REACH AN EMPLOYEE'S INBOX.

LEARN MORE

Learn more about how Enterprise Protection from Proofpoint can help you effectively block impostor emails and stop them before they ever reach your employees, please visit proofpoint.com/us/solutions/products/enterprise-protection

[1] Business E-Mail Compromise, An Emerging Global Threat, August 28, 2016, fbi.gov/news/stories/2015/august/business-e-mail-compromise/business-e-mail-compromise

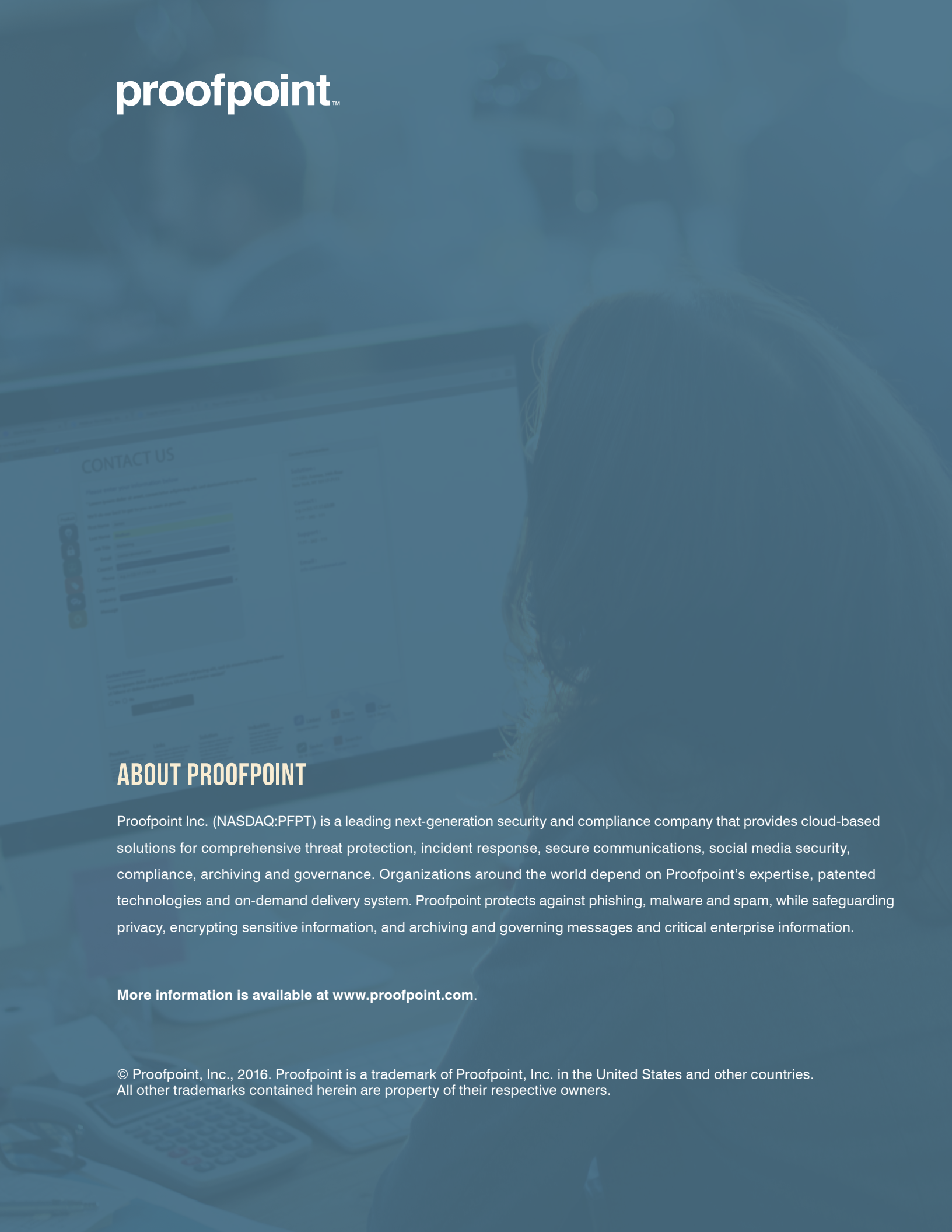
[2] Tech Firm Ubiquiti Suffers $46M Cyberheist, August 15, 2015, krebsonsecurity.com/2015/08/tech-firm-ubiquiti-suffers-46m-cyberheist

[3] Belgian Bank Loses €70 Million to Classic CEO Fraud Social Engineering Trick, January 25, 2016, news.softpedia.com/news/belgian-bank-loses-70-million-to-classic-ceo-fraud-social-engineering-trick-499388.shtml

[4] New Zealanders lose $12m to scams, January 1, 2016, stuff.co.nz/business/money/75536670/New-Zealanders-lose-12m-to-scams

[5] Nigerian charged in sophisticated email scam is in custody in Dallas, January 1, 2016, dallasnews.com/news/crime/headlines/20160101-nigerian-charged-in-sophisticated-email-scam-is-in-custody-in-dallas.ece

proofpoint™



ABOUT PROOFPOINT

Proofpoint Inc. (NASDAQ:PFPT) is a leading next-generation security and compliance company that provides cloud-based solutions for comprehensive threat protection, incident response, secure communications, social media security, compliance, archiving and governance. Organizations around the world depend on Proofpoint's expertise, patented technologies and on-demand delivery system. Proofpoint protects against phishing, malware and spam, while safeguarding privacy, encrypting sensitive information, and archiving and governing messages and critical enterprise information.

More information is available at www.proofpoint.com.