AGARI

WHITE PAPER

Trusted Email Identity

Securing the Foundation of Digital Communications

Executive Summary

While new business communication and collaboration tools emerge every day, an employee's email address often serves as the one constant identity that is leveraged by other forms of digital communication, including cloud productivity suites, collaboration applications, and even text messaging.

But despite the fact that email remains the most popular method of communication, its ubiquity, along with well-known limitations in its technology underpinnings, make it the leading attack vector for cybercriminals.

Spear phishing, business email compromise (BEC) scams and other forms of advanced email attacks successfully bilk businesses out of billions of dollars each year, accounting for more than half of all business losses from cybercrime. Beyond the potential for financial, legal, and regulatory calamity, these crimes can decimate brand trust, obliterate competitive advantage, and even put lives or national security at risk.

Traditional approaches to corporate email security focus largely on inspecting message content and assessing the reputation of a message's infrastructure of origin. But these techniques have become ineffective as attacks have grown more targeted in nature and increasingly blend in with legitimate email traffic delivered through trusted, mainstream email platforms.

By employing identity deception to impersonate a senior executive, a trusted supplier, or an important customer, today's most successful email attacks exploit the identity markers of trusted individuals and brands to dupe victims into making costly mistakes. Whether it's initiating a wire transfer, revealing login credentials, or disclosing sensitive information, the dangers are real—and no organization or industry is immune.

To neutralize the threat from email-based impersonation scams, organizations most find ways to go beyond assessing content or sending infrastructure to establish the identities behind the email messages directed at corporate inboxes. To achieve this, data scientists at Agari leverage vast amounts of email telemetry and machine learning to enable you to predict whether the email messages you and your employees receive can be trusted, opened, answered, and acted upon.

Email phishing is the go-to attack used to target your workforce and supply chain, with reported fraud losses in excess of

$18B

2013 - 2019

according to FBI/IC3

Table of Contents

Dead Ringer: How Identity Deception Has Changed the Game for Email Fraudsters

Instead of relying solely on malware, phishing links, or other forms of malicious content, the modern email attack primarily leverages identity deception. Specifically, the attacker sends an email message that appears to come from a known identity—an individual or brand that is often trusted by the recipient.

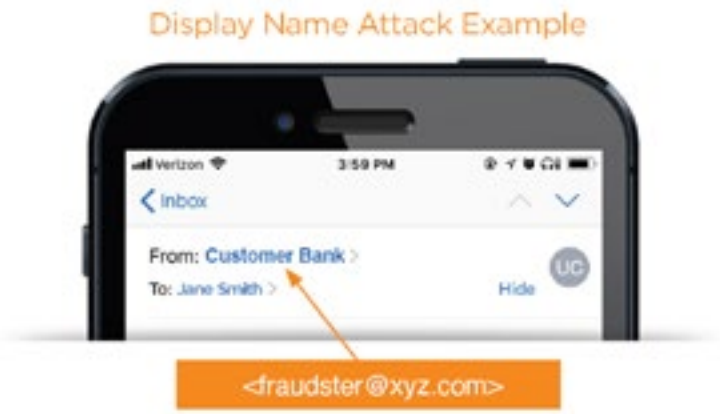
By manipulating the "from" header, subject header, and the message body of emails, attackers exploit the trust associated with that impersonated identity to bamboozle employees into costly mistakes. The price tag: Nearly $30 billion in business losses since 2016. Despite rising awareness for such scams, a recent study found that one-third of employees will obey a fraudulent email request, no questions asked.

To understand how cybercriminals evade detection and con employees into wiring money, revealing login credentials, or disclosing sensitive information, a look at the most common forms of identity deception is a good place to start.

'From' Line Fraudsters: Most Common Forms of Identity Deception

The key to any identity-based attack is impersonation—manipulating components of an email message to match or closely resemble identity markers found in legitimate messages.

The most common form of identity deception is **Display Name Deception**. Many email clients show only the display name in certain views, and attackers often insert the identity of a trusted individual (such as the name of a senior executive) or a well-known brand (such as the name of the targeted individual's bank) as the display name.



Thanks to the fact that email providers such as Gmail and Yahoo allow a user to specify any value in the display name, this type of attack is simple and cheap to stage. Indeed, it has long been the tactic of choice for cybercriminals, accounting for 88% of all email attacks during the last six months of 2020. Gmail alone accounts for nearly half (43%) of all scams employing this form of identity deception.

It's also highly effective. Because the point of origin is an established and widely used cloud email service, these phishing emails easily evade most secure email gateway (SEG) defenses. And recipients all too often take the bait because the name matches one they are familiar with—either a brand they trust or a co-worker within their organization.

Other forms of deception include **lookalike domains**. Here, threat actors use common misspellings, homoglyphs, or Cyrillic characters that appear similar to the original characters in an impersonated domain name of a trusted service such as DocuSign, Dropbox, or Microsoft itself.

While large companies often register lookalike domains as "defensive domains" to prevent this form of attack, there's no way to register every possible permutation. Additionally, if the organization doesn't implement proper email authentication on these domains, cybercriminals can still spoof them, regardless of legal ownership. Today, 27% of all BEC attacks are launched from lookalike domains.

The most pernicious form of identity deception, however, occurs when the fraudster successfully infiltrates the email account or server belonging to the individual or brand they seek to impersonate. While low in volume, **Account Takeover (ATO)-based attacks** are by far the most difficult to detect. Not only do they possess legitimate identity markers and infrastructure belonging to the account's actual owner, their malicious email behavior is also camouflaged by the owner's more mundane behavioral characteristics.

Once upon a time, sending phishing emails to employees from a senior executive's compromised email account was the holy grail of ATO-based attacks. But today, using those and other pirated accounts to victimize entire supply chains is the name of the game in a particularly devastating variant of BEC known as Vendor Email Compromise, or VEC. While traditional BEC scams cost businesses an average $50,000 per incident, VEC-based attacks average $125,000, according to FinCEN.

Despite their differences, each of these forms of identity deception is designed to bypass legacy security controls and ultimately convince recipients to take some action out of the mistaken belief it was sent by an individual or organization they trust. Once the email security system has been bypassed, fraudsters are free to unleash social engineering lures on the weakest link in any cybersecurity effort: human beings.

Data Science: Defining Trusted Email Identity

Data scientists at Agari have found that the key to protecting against impersonation attacks is authenticating the components of email messages bearing identity markers that are otherwise indistinguishable from legitimate emails.

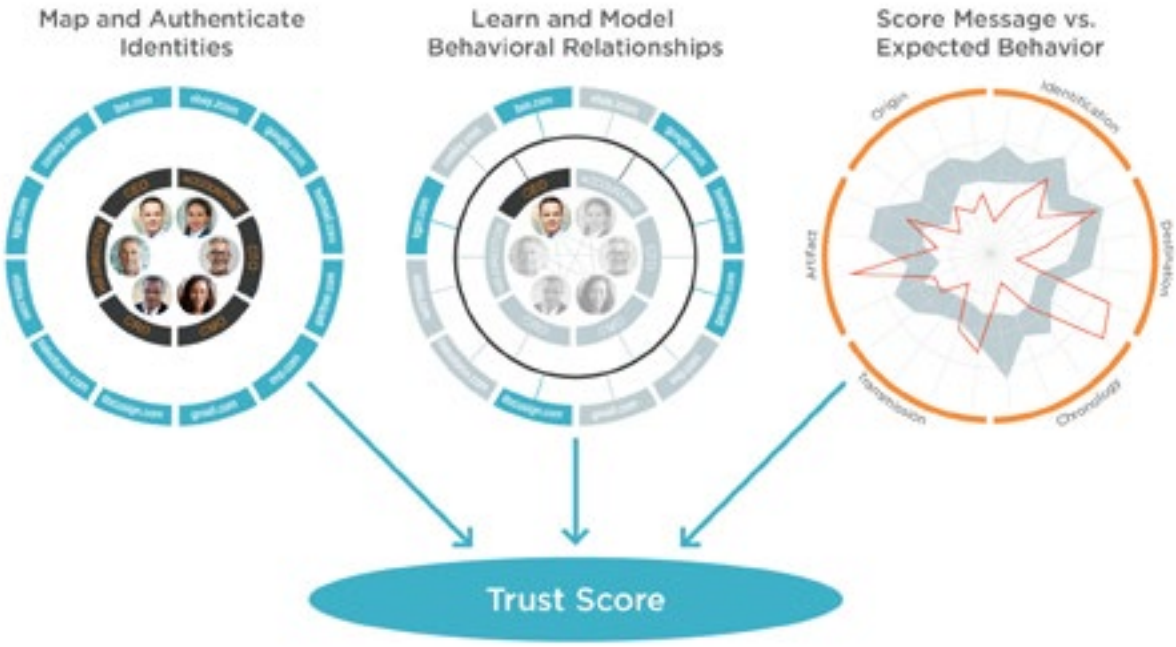
To do this, Agari amasses vast amounts of telemetric data to establish the relative risk associated with sender-receiver interactions and the trustworthiness of the underlying email address.

The Agari Identity Graph™ leverages this telemetric data and advanced machine learning techniques to model relationships and behavioral patterns between individuals, brands, businesses, services, and domains using hundreds of characteristics to define trusted communications.

The data science behind the Agari Identity Graph ferrets out sophisticated identity deception attacks using three discrete phases of analysis:

- **Identity Mapping:** This phase answers the question, "Which identity is perceived to be sending this message?" Individual messages are analyzed to determine the perceived identity and map it to a corresponding behavioral model.
- **Behavioral Analytics:** This phase answers the question, "Does this message match the expected behavior for that identity?" The features of a message are analyzed in the context of a behavioral signature for the detected identity to determine whether it represents anomalous behavior.
- **Trust Modeling:** This phase answers the question, "How is the perceived identity related to the recipient?" The closer the relationship, the less tolerance for anomalous behavior since the impact of an attack is greater.

Each of the three phases of the Agari Identity Graph leverages a variety of algorithms and machine learning models to come up with highly accurate answers to these questions. The results of these questions are combined to determine an overall score for a message.



The final identity score of an email message represents the probability that the message can be trusted, and can be used to trigger a policy-based action.

Operationalizing Trusted Email Security

The applicability of the Trusted Email Identity model outlined in this paper isn't based on hypotheticals. It's a proven reality for more than 500 of the world's most prominent organizations.

By combining vast amounts of telemetry data, machine learning, and API-based product integration, Agari operationalizes Trusted Email Identity to power products and services that detect, defend against, and respond to impersonation-based email attacks.

Agari Phishing Defense™ prevents email threats from reaching employee inboxes by scoring every message flowing into and within the organization to defend against low-volume, highly targeted identity deception-based attacks.

Agari Phishing Response™ prioritizes reported incidents, automating investigative analysis and triage, to elevate the most suspicious emails to the top of the list. Then, it reduces manual efforts with remediation workflows to accelerate time-to-containment.

Agari Brand Protection™ protects your customers from costly phishing attacks by automating and simplifying DMARC email authentication and enforcement, preserving brand identity, and boosting digital engagement.

Agari Active Defense™ **BEC Threat Intelligence Service** uses automated active engagement to uncover criminals' tactics and techniques and deliver highly-focused, actionable intel about specific phishing and BEC threats targeting your organization.

As the financial losses and reputational damage from phishing, BEC, and other advanced email threats continue to mount, technologies capable of establishing Trusted Email Identity can give corporate employees, customers, and partners the confidence to open, click, and trust everything in their inbox.

To see first hand how Agari gives you the upper hand in email security, please visit our Self-Service Demo Experience for:

- **Agari Brand Protection™**
- **Agari Phishing Defense™**
- **Agari Phishing Response™**
- **Agari Active Defense™**

About Agari

Agari is the Trusted Email Identity Company™, protecting brands and people from devastating phishing and socially-engineered attacks. Using applied data science and a diverse set of signals, Agari protects the workforce from inbound business email compromise, supply chain fraud, spear phishing, and account takeover-based attacks, reducing business risk and restoring trust to the inbox. Agari also prevents spoofing of outbound email from the enterprise to customers, increasing deliverability and preserving brand integrity.

Learn more at: agari.com