GreatHorn | Inspired eLearning | dmarcian

Email Security Cubed:

A Layered Approach to Reducing Cyber-Risk

Phishing attacks are on the rise. Your organization faces higher risk. But a fact-based approach to security – integrating three effective layers of email safeguards – can measurably improve your risk profile.

WHITEPAPER

September, 2020

Email provides your organization with a business-critical channel for communication among your employees, partners, and customers. But chief information security officers (CISOs) know that email presents inherent security pitfalls. If not addressed effectively, these weaknesses can:

- Expose sensitive customer and employee data
- Reveal valuable intellectual property
- Lead to significant financial loss, costly legal action, and lasting damage to your brand

Think email security isn't an issue in your organization? PwC research suggests otherwise. In 2019, the firm simulated nearly 1,000 phishing attacks against large financial institutions. Seventy percent of the emails slipped past company protections and 7% of links were clicked on by users.[1]

Now, a global crisis has compounded these threats. Organizations have experienced nearly a sevenfold increase in spear phishing attacks since the start of the coronavirus pandemic, according to McKinsey. "Remote workers are … bombarded with attacks based on COVID-19-crisis themes that are taking advantage of delayed updates to email and web filters," the firm reports.[2]

For example, emails disguised as government announcements have prompted users to click on links that appear to lead to the U.S. Centers for Disease Control and Prevention (CDC) or World Health Organization (WHO). The links launch malware attacks or drive users to pages that look legitimate but are designed to steal credentials.[3]

It's not just your frontline workers in the crosshairs. The C-suite is equally vulnerable. "Fraudsters have tried to get executives to move money to fund vendors, operations and virus-related-response activities," McKinsey notes.[4]

Emails disguised as government announcements launch malware attacks or drive users to pages that look legitimate but are designed to steal credentials.

[1] *"How Well Does Your Industry Defend Against Elementary Phishing Campaigns?" PwC, 2019*
[2] *"COVID-19 Crisis Shifts Cybersecurity Priorities and Budgets," McKinsey, July 2020*
[3] *"COVID-19 Exploited by Malicious Cyber Actors," U.S. Cybersecurity and Infrastructure Security Agency (CISA), April 2020*
[4] *"How the Response to COVID-19 Has Increased Cyberrisk," McKinsey, March 2020*

The good news is that a fact-based security strategy can equip you to master your email security risk. This innovative concept integrates three effective layers of email safeguards to measurably improve your email protections:

DMARC

Eliminates unauthorized use of your email domain, gives you visibility into who's using your email, and allows others to confirm the validity of your email.

Security Awareness Training

Enables you to gauge user-associated risks, empowers employees to understand email vulnerabilities, and drives culture shift to prioritize security.

Advanced Threat Protection

Guides in-the-moment user behaviors, applies a fact-based approach to risk reduction, and leverages aggregated data to accurately detect emerging threats.

This layered approach to email security enables you to report real metrics to demonstrate how you're reducing your risk. It can transform the way you manage phishing attacks and tangibly bolster your risk management strategy.

A layered approach to email security can transform the way you manage phishing attacks and tangibly bolster your risk management strategy.

DMARC: Validity and Visibility

Domain-based Message Authentication, Reporting and Conformance (DMARC) is an industry standard designed to prevent unauthorized email use. It provides a way for your organization to declare which email is yours and decide what to do with email that isn't. A robust reporting mechanism gives you visibility into who's sending email on your behalf and who might be masquerading as your organization.

DMARC improves email security in four ways:

1. **Protections** – You can monitor email flow for threats and unknown senders. You can also prevent spoofing and phishing emails from being sent from your domain.

2. **Visibility** – You gain detailed insight into emails sent on behalf of your domain.

3. **Identity** – Your email is easy to identify across a large and growing footprint of DMARC-capable receivers.

4. **Deliverability** – You can make sure your emails are delivered using the same technology large companies use for their emails.

DMARC is built on the Sender Policy Framework (SPF) and DomainKeys Identified Mail (DKIM) authentication protocols. SPF is a list of servers allowed to send on behalf of your domain. DKIM affixes each email with a tamper-proof seal that's verified on delivery.

SPF and DKIM can associate a piece of email with a domain. DMARC ties the results of SPF and DKIM to email content – specifically, the domain in the From: header.

For an email message to be DMARC-compliant, the domain in the From: header must match the domain validated by SPF or the source domain found in a valid DKIM signature. If the domains match and at least one verification mechanism succeeds, receivers can accept that the email legitimately comes from the specified domain.

DMARC allows a domain owner to indicate that its messages are protected by SPF or DKIM. It also tells the recipient what to do if neither SPF nor DKIM is verified. Domain owners can set their DMARC policy ("p=") like so:

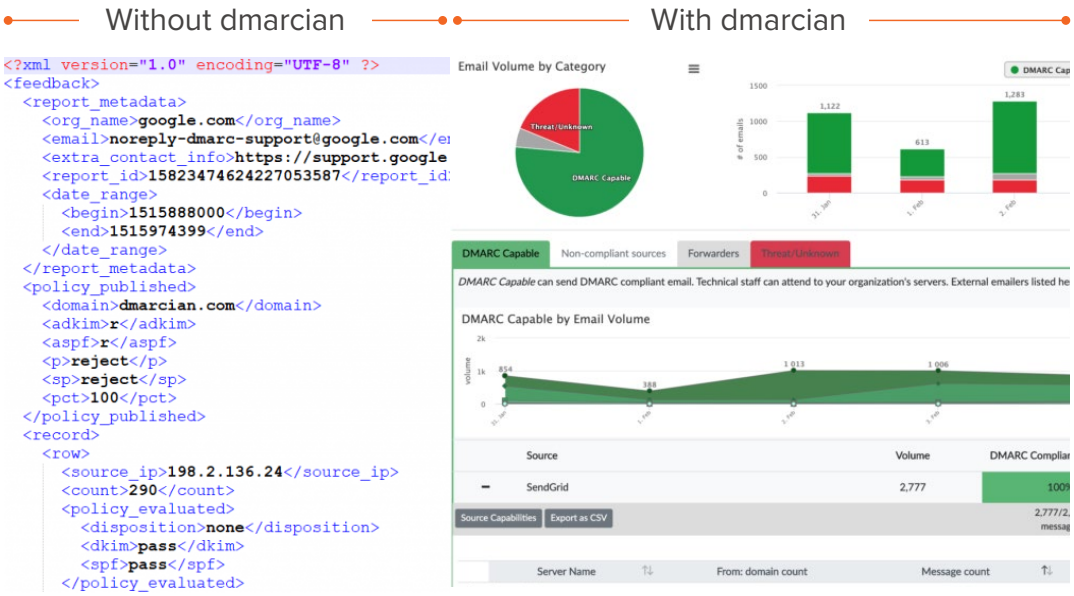
- **Monitor (p=none)** – Collects feedback but doesn't restrict email flows
- **Quarantine (p=quarantine)** – Moves failed messages to the spam folder
- **Reject (p=reject)** – Rejects the message

DMARC policy typically starts with p=none, a monitoring phase that gives visibility into how your domain is being used and how SPF and DKIM are functioning. P=reject, in contrast, instructs email receivers to refuse to accept an email that fails DMARC. This functionality is an excellent control against any unauthorized email making use of your domain.

Solutions such as dmarcian's DMARC software-as-a-service (SaaS) platform can help you achieve a holistic view of your email security. dmarcian categorizes email sources and shows DMARC compliance status based on source, SPF, and DKIM. It also sends alerts on potential threats to your domain. Additionally, it interprets XML reports from receiving email servers to supply user-friendly visualizations. (See Figure 1.)

dmarcian's DMARC software-as-a-service (SaaS) platform can help you achieve a holistic view of your email security.

Figure 1: Interpreting DMARC XML Reports



Employees can become effective partners with your IT and security functions in strengthening your cyber-defenses.

dmarcian can deliver tangible security improvements. For example, a global agriculture and food company experienced frequent spam and phishing attacks, especially for a newly acquired domain and previously unknown email sources. The enterprise was also challenged by a C-suite that didn't understand the need to invest in a DMARC initiative to lock down its domains.

dmarcian can supply an effective solution. When the IT team established a DMARC record, the dmarcian dashboard clearly proved to management that lax email security needed to be addressed. It also highlighted business-critical issues around domain protection and brand integrity.

After the organization implemented a more restrictive DMARC policy, its illegitimate email traffic plummeted from 75% to less than 5%. Now when it acquires a domain, DMARC illuminates how it's being used and whether it's being abused. That allows the company to make informed decisions, reduce margin of error, and lower associated costs.

Security Awareness, Risk Readiness

Employees are a frequent target of phishing and business email compromise (BEC) attacks. Some IT and security teams view end users as the weakest link in their security chain. But if that's the case, it's only because workers lack sufficient security training. The fact is employees can become effective partners with your IT and security functions in strengthening your cyber-defenses.

One reason security training is crucial is because traditional security solutions can be limited in their effectiveness against phishing. After all, phishing begins not with technology but with social engineering designed to prompt user action – downloading an attachment, clicking a link, sharing a password, or transferring funds. Security awareness empowers your people to recognize and respond appropriately to email-based attacks.

Typical approaches to employee training often fall short, however. That's because they're usually compliance-focused, merely requiring workers to check a box confirming they've seen a once-a-year security presentation. Unfortunately, research shows – and experience confirms – that people quickly forget information they don't engage with often.

Security awareness training should do more than just promote knowledge retention. It also needs to drive employee motivation around protecting data resources.

The solution is spaced learning, a research-validated concept that reinforces knowledge through repetition. In practical terms, that means providing users with targeted security training throughout the year. These reinforcements can take various forms, from topic-specific videos to practice exercises such as interactive phishing simulations.

But short memories aren't the only problem. Convincing employees to pay attention to security issues and habitually follow security best practices is a perennial pain point for CISOs. So, security-awareness training should do more than just promote knowledge retention. It also needs to drive employee motivation around protecting data resources.

Achieving that goal means meeting learners where they are. Effective training shows users what's in it for them and the benefits of strong security not only to the organization but also to their ability to do their job effectively.

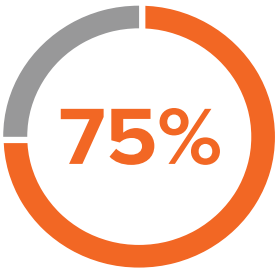
Finally, learning needs to be something employees want to experience. That calls for engaging formats and high production quality. Trainings should also be relatable with inclusive imagery and scenario-based simulations so learners can visualize themselves in the situation.

Effective security training results in measurable outcomes. Solutions from Inspired eLearning, a provider of security awareness and compliance training, have been shown to trim training times by 50% and slash phishing breaches by 75%. (See Figure 2.) The company's client data also shows that combining its training with phishing simulations can reduce annual phishing susceptibility from 30% to as little as 2%.

In addition, Inspired eLearning's Cybersecurity Quotient (CyQ™) Assessments provide metrics on how much users understand and test against common cyber-threats such as social engineering and password compromise. Its reporting platform then creates a "threat profile" for each user to help enterprises understand their level of email risk.

Figure 2: Security Training with Inspired eLearning[5]

Employee security awareness training time savings



Reduction in phishing-related data breaches

The answer is a purpose-built solution that applies advanced threat detection to specifically address email security.

Advanced Threats, Proactive Protections

In addition to DMARC and security awareness training, the third layer of protection is an integrated security solution specifically designed to safeguard against advanced email threats. Advanced threats are those that use social engineering and other phishing techniques to bypass traditional security controls. In place of imprecise volumetric onslaughts, they take advantage of individualized attacks that have a higher likelihood of success.

Advanced threats might leverage information in the public domain, such as details about your business operations, to build trust with recipients. They might use Gmail and Yahoo accounts that can pass authentication checks, because they come from legitimate email services. They might target individuals in your company who have access to financial systems. Because they can be missed by your existing security technology, they can be insidious.

The answer is a purpose-built solution that applies advanced threat detection to specifically address email security.
Such a solution should counter phishing and other email attacks by analyzing multiple criteria:

Relationship Strength

Examines the strength of a sender's individual relationship to the recipient, with a "friends of friends" view that accounts for the sender's overall relationship with others in the recipient's organization.

Spoofing Likelihood

Analyzes employee display-name spoofs, domain spoofs, and domain look-alikes, including comparison against known email addresses, executive impersonation tactics, and email authentication standards.

Technical Fingerprint

Conducts sophisticated analysis of domain reputation, sending IP, and header information, including variations in expected authentication results for DMARC, SPF, and DKIM.

Content Analysis

Performs deep content inspection based on keywords, regular expressions (RegEx), attachments, and URLs to identify common spear phishing tactics. These include wire transfers and W2 requests, credential-theft attacks, and business-service impersonations.

Communication Patterns

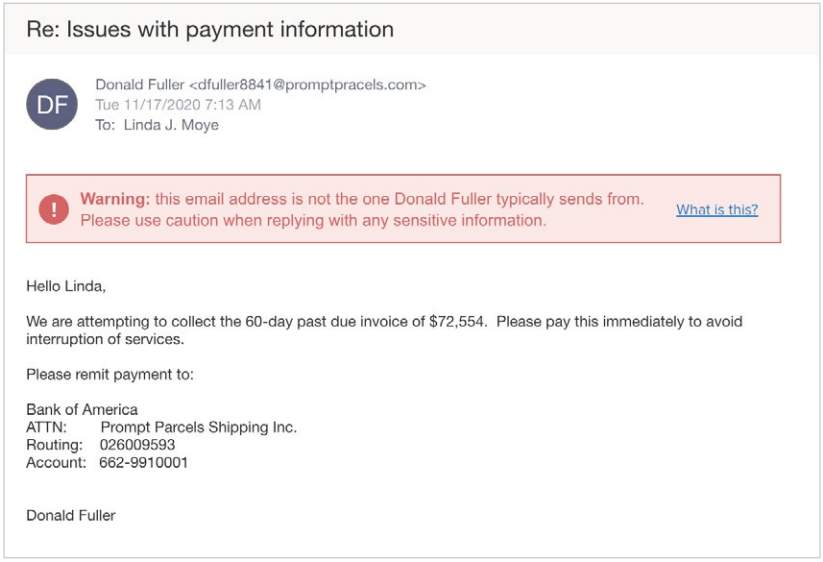
Recognizes communication patterns unique to a specific individual and organization, such as email frequency, volume, recipients, and sending patterns.

Advanced threat detection applies these criteria to take threat-relevant actions, including:

- **Subject line label** – The software injects an alert in the email subject line warning the user that the message contains suspicious content such as financial details.
- **Dynamic bannering** – The application applies a more prominent, context-based notice that the email originates from an external source and appears, for instance, to be requesting a funds transfer. (See Figure 3.)
- **Link protection** – For an uncommon link, it can redirect to a safe page that warns the user before proceeding. For a known malicious link, it can disable the link altogether.
- **Move to user's trash** – For an email that's more likely to contain a threat, the application can move the message to the user's trash or other designated folder.
- **Quarantine with release** – For an even more suspicious email, the software can remove the email from the recipient's inbox and provide a notification that the email was quarantined. The user is offered a workflow to request the email's release from quarantine. The email would then enter a process for further analysis – either automated or manual – before it's released to the user.
- **Silent quarantine** – Finally, if the email contains a known malicious link or attachment, it's simply removed from the recipient's inbox.

Such alerts and actions also provide employees with in-the-moment training. Because they're engaged at the moment of risk, workers gain awareness of threats, learn the right behaviors, and are empowered to follow security policy while doing their jobs effectively.

Figure 3: Account Takeover Protection



Advanced threat detection should enable a fact-based approach to email security. For example, it should apply advanced analytics and machine learning (ML) to relevant data such as how frequently an email recipient engages with the sender, how long it has been since the last interaction, whether the email originates from a new domain, whether the return path deviates from a previous return path, and so on.

Your solution should also allow you to capture metrics that show tangible security improvements, such as reductions in mean time to detection and mean time to remediation. Such quantitative results equip you to demonstrate to executive stakeholders a return on your security investments.

GreatHorn offers a robust solution for advanced threat detection to help you achieve the highest levels of security for your email traffic, supporting a layered approach by incorporating data from dmarcian's DMARC platform and Inspired eLearning's user risk profiles.

Combining DMARC and Advanced Threat Detection into a single pane of glass, organizations can more effectively identify where a domain is not setup correctly. With visual representations to understand risk, along with step-by-step instructions, and easy navigation to fix any improper setup, this integration combined ease-of-use across the breadth of email security.

Integrating security awareness training and Advanced Threat Detection provides a unified view into an individual's risk profile, along with an overview of the organization's risk profile at aggregate. As the weakest link, end users' behavior can be tracked between systems, setting up policies to enroll users into selected programs based on their success with training, or based on their behaviors with or types of phishing emails they receive. This advanced integration more effectively mitigates risk across the organization, providing the granularity required to safeguard the organization.

In addition, our ML algorithms learn from historical data to become more accurate over time. And our collective intelligence – built on the management of billions of emails every month across our client base – allows all our clients to benefit from continual enhancements. Advanced threat detection from GreatHorn empowers your organization to detect, protect, and respond to email threats. (See Figure 4.)

Figure 4: Detect, Protect, Respond

Proliferating, targeted attacks are raising the bar on email security. As Gartner advises, "assessing widespread security threat trends such as ransomware and phishing requires a continuous adaptive risk and trust assessment strategic approach."[6]

That's why smart organizations are investing in a layered approach to shoring up their email security. They gain the capabilities they need to protect their data from exposure and their organization from the cost, disruption, and brand erosion of breaches. They also better manage enterprise risk to help ensure the long-term success of their business.

Advanced threat detection should enable a fact-based approach to email security.

[6] *"How to Respond to the 2020 Threat Landscape," Gartner, April 2020*

About GreatHorn

GreatHorn protects organizations from more advanced threats than any other email security platform. By combining its highly sophisticated threat detection engine with accessible user context tools and integrated incident response capabilities, GreatHorn Email Security shields businesses from both sophisticated phishing attacks and fastmoving zero-day threats, freeing security teams from the tedium of email security management while enabling them to respond to genuine threats faster than ever before.

By combining deep relationship analytics with continuously evolving user and organizational profiling, GreatHorn's cloud-native email security platform provides adaptive, anomaly-based threat detection that secures email from malware, ransomware, executive impersonations, credential theft attempts, business services spoofing, and other social engineering-based phishing attacks.

About Inspired eLearning

Inspired eLearning offers a variety of turn-key eLearning solutions, including tiered Security Awareness, Compliance & HR training programs, PhishProof phishing assessment software, tailored courseware design and development, content integration, and a fully hosted, web-based eLearning course delivery and tracking system based on the iLMS (Inspired Learning Management System).

About dmarcian

Founded by the co-author of the DMARC specification, dmarcian has been providing products and expert services that help domain owners secure their digital assets, since 2012. Our SaaS reporting application alleviates pain points associated with processing complex DMARC reports and aids organizations in identifying steps necessary to reach their DMARC goals. The result is a safer email ecosystem for all.