RapidScale
A Cox Business Company

SOMMITA
TECHNOLOGY GROUP, LLC

COX BUSINESS®

Executive Guide

Email Security: Why It's Not Just About Email

In the beginning, email was conceived as an easier, faster way for people already connected in close-knit professional communities (e.g., academia, government, the sciences) to exchange information. The possibility that anyone would use email for fraudulent purposes? The designers of the original email protocols weren't particularly worried about that. Now, this lack of basic security is a real problem and a key reason why email has become a primary vector for all kinds of enterprise security issues. That's why email security is not just about email—it's about protecting your entire organization.

People concerned with the email security issue have often predicted that it would go away because email was going to go away. Don't count on that happening anytime soon. While instant messaging, texting and social media have stolen some of email's thunder, especially among younger audiences, email not only holds on, but it also continues to flourish:[1]

- The number of worldwide email users is now around four billion (equivalent to half the people on the planet), and that figure grows every year
- Well over three hundred billion emails are sent every day

Email is nothing if not versatile: it's equally at home on the desktop as in mobile environments, on-premises or delivered via the cloud. It's relatively easy (and cheap) for anyone to maintain multiple email accounts. Over time, it's become more than a form of communication—an email address is the price of entry to many other online activities, including social networking, instant messaging and numerous business transactions.

For all of these reasons and more, betting on email to just go away anytime soon is not a good bet. Criminals know this, which is why they remain highly inventive at exploiting email's many security deficiencies.

From Malware to Phishing and Ransomware

In the beginning, email security was mainly about controlling the threat of malware-laden attachments with a side dish of stopping unwanted marketing spam. But things have kept evolving.

Today, a primary email security challenge is phishing. If you've received an email advising you to instantly click on a link and enter your credentials to take advantage of a huge financial windfall or to clean up a problem with one of your accounts, you've likely been phished.

[1]- The Radicati Group, Inc. www.radicati.com

Phishing has been on the rise for years and exploded during the pandemic. According to a survey by Mimecast[2] (the email security company and partner of RapidScale):

- Email threats rose by 64% in 2020
- Employees worldwide are clicking on malicious URLs embedded in emails three times as often as they had before.

These same kinds of phishing attacks have helped drive the rise of ransomware. In the Mimecast survey, more than 60% of companies reported suffering a ransomware attack. More than half paid the ransom, but of these a third still failed to get their data back.

Impersonation Attacks via Email

A specific kind of phishing known as Business Email Compromise (BEC)—in which the criminal impersonates a business associate—has become particularly common. Some typical examples of BEC phishing include:

- An accounts payable person getting an email with attached invoice purportedly from a vendor the company regularly deals with, but asking that the payment be sent to an updated mailing address
- An assistant receiving an email from someone purporting to be the company CEO with instructions to purchase dozens of gift cards (to send out as employee rewards) and asking for the serial numbers of all the cards so that the CEO can let the employees know right away
- A human resources person getting an email requesting an update to an employee's bank account used for direct deposit
- A homebuyer receiving a message from a title company with instructions on how to wire the down payment for a specific property

A recent twist on BEC is for attackers to request an accounts receivable aging report that might contain data on payments overdue, points of contact for each customer and other information. The attackers then use that information to send convincing payment requests to the customers on the list. In January 2021, more than ten percent of all BEC attacks involved a request for an aging report.[3]

Think this can't happen to you? Between 2013 and 2015, Facebook and Google were defrauded out of more than $100 million by a gang of cybercriminals who impersonated their suppliers and sent fake invoices via email.[4]

Email Security is Evolving

The evolution of threats is forcing IT teams to rethink the planning, purchasing and management of their business security systems. Some of the major developments taking place right now include:

- Greater use of AI-based tools and machine learning to identify inventive phishing attacks more quickly
- Extended detection and response (XDR) solutions that integrate threat detection, investigation and response enabling faster, more effective responses to intrusions
- Greater compliance with DMARC—the Domain-based Message Authentication Reporting and Conformance protocol—for authenticating that an email sent from an organization's domain is a legitimate message and not fraudulent

While all of these provide security advantages, none are (or claim to be) a silver bullet.

For example, AI and machine learning tools are effective, but used on their own they tend to generate a large number of false positives. To be truly effective, AI needs to be used in combination with other detection capabilities.

[2]- Securing the Enterprise in the Covid World: The State of Email Security, Mimecast
[3]- https://www.darkreading.com/threat-intelligence/how-attackers-weigh-the-pros-and-cons-of-bec-techniques/d/d-id/1341060
[4]- https://www.cnbc.com/2019/03/27/phishing-email-scam-stole-100-million-from-facebook-and-google.html

The email security solutions that RapidScale provides (based on our partnership with Mimecast) draw on multiple detection technologies including more than 50 integrated detection engines, open APIs and off-the-shelf third-party integrations coupled with threat data mined from Mimecast's 40,000+ customer base. This makes it possible to exceed the protections that are included with cloud-based email solutions such as Microsoft 365. For example, in rigorous testing, Mimecast has determined that its secure email gateway platform is able to block 22% more malicious content than Microsoft.[5]

Taking Security Seriously

Covid-19 has confronted us with the stark realities of a global pandemic. But for cybercriminals, the pandemic has been an opportunity to significantly ramp up their attacks, often using Covid-19 as a cover. Both phenomena are a measure of how interconnected we've become and the challenges we face in staying safe and secure on every level.

Unquestionably, these challenges will continue to grow and evolve. Just as email revolutionized communications decades ago while introducing a wide range of new risks, the new tools we use now to adapt and collaborate in the new world of remote work are introducing their own security challenges.

None of this should obscure the fact that real progress has been made in security. Advanced technologies such as AI, layered email defenses and tighter integration into other security mechanisms, like network security monitoring—these all hold out promise for greater protection tomorrow. But so do much simpler measures that can be implemented today, including two-factor authentication and regularly training employees in attack-resistant behaviors.

The bottom line: Organizations that take security seriously and invest in realistic solutions to address their vulnerabilities will be in the best possible position to recover more quickly from the inevitable intrusion, while preventing more and more attacks from ever happening in the first place.

An Adaptable Security Framework

Because every organization's security needs are different, and security challenges keep evolving, rather than thinking solely in terms of specific solution, the National Institute of Standards and Technology (NIST) in its Cybersecurity Framework suggests organizations consider security in terms of five core functions:

Identification
Pinpointing the critical resources that need to be protected and the risks associated with those resources. For example, a company might identify the personally identifiable information (PII) of its customers as its most critical resource and phishing attacks on employees—especially those working remotely—as its primary entry-point risk.

Protection
What measures will be most effective in protecting those resources and addressing those risks? This might include using AI to screen and discard phishing emails, greater implementation of two-phase authentication and training users to better identify suspicious emails.

Detection
What would be the best methods for detecting an intrusion or attack such as monitoring user logins for anomalies?

Response
In the event of a successful attack, the company will need to respond. Thinking this through in advance will make it easier to operate in crisis mode. Typical responses will include emergency efforts to halt the intrusion, communication to key stakeholders as well as processes for making use of backup data.

Recovery
What steps will be required to return to normal operation? Restoring data from an offsite backup? Cleansing user devices?

[5]- Mimecast Cyber Resilience Insights Blog, https://www.mimecast.com/blog/cloud-email-security-supplements-7-questions-cess-vendors-dont-want-you-to-ask/

How RapidScale Delivers Protection

For protection against today's sophisticated online threats, a traditional, perimeter-based security strategy (e.g., firewalls, antivirus) have long been insufficient. That's why RapidScale and Mimecast have teamed up to deliver a comprehensive, multilevel approach that starts with email security and adds data protection, web security, awareness training and threat intelligence—all in one powerful, easy-to-use platform:

Email
Advanced email security focused on the latest, socially engineered phishing and targeted impersonation attacks

Web
Cloud-based web protection at the DNS level that stops malware and inappropriate web use in its tracks

Employee Awareness
Dramatically reduce security risks due to human error with engaging, regular end-user training

Data
An independent, 100% cloud-based archive to help simplify data management and discovery, while also meeting complex compliance requirements

Intelligence
Threat intelligence specific to your environment detailing how you've been targeted, what cyber threats have been blocked and why

Microsoft 365 and Microsoft Exchange Integration
Augmenting built-in Microsoft 365 security while maintaining choice and control

Talk to Sommita about Security

Contact Sommita to leverage our cybersecurity expertise so we can begin helping you with a comprehensive solution designed for your business.

RapidScale
A Cox Business Company
rapidscale.net

SOMMITA
TECHNOLOGY GROUP, LLC
sommita.net

COX BUSINESS®