WHITE PAPER

The Future of Email Security in the Cloud

And Why You Should Reexamine Your Approach Now

TABLE OF CONTENTS

EXECUTIVE SUMMARY

Email remains the most widely used communication method for business. Studies estimate that nearly 125 billion business emails are sent each day – a three percent year-over-year growth since 2015.[1] Technology writer Chris Nerney explained why email still reigns as a primary method of professional communication in a July 2018 blog: "Email is highly functional. Anyone with an email account can send an email to anyone else with an email address, no matter which client they use. In the business world, there's a lot of value to that, and it's probably the main reason why messaging apps, social media and collaboration platforms haven't yet rendered email obsolete."[2]

Yet due to its inherent security flaws, email also remains one of the most common attack vectors. In a 2018 survey of IT professionals, GreatHorn determined that the average organization has three security products in place to combat email threats; however, 40 percent of that same group sees email threats bypass these security solutions and be delivered into inboxes on a weekly basis.[3] Despite email's tenure and prevalence, few organizations have email security threats under control – even with great manpower and tool investment.

The traditional approach to email security is failing.

The traditional approach to email security is failing, and the problem is plaguing organizations across all industries. In fact, a LinkedIn survey of more than 1,900 security professionals indicated that email security is a top priority for more than half of organizations.[4] Threats consistently are becoming more sophisticated and slipping past traditional security measures, while the changing technology landscape creates new security demands. As more organizations embrace modern IT infrastructure, they are looking to tackle the challenge with solutions that are just as dynamic as their cloud-based email systems.

This white paper will guide security teams as they reexamine their approach to cloud-based email.

THE EVOLUTION OF THREATS: FROM PRINCE TO PAYLOAD TO IMPERSONATION

A LOOK AT EARLY EMAIL THREATS

When electronic communications first rose to prevalence in the late 1980s and early 1990s, IT infrastructure looked very different than it does today. Technology was more tangible, and email security efforts were focused on encryption to ensure privacy versus the identification and remediation of threats.[5] It wasn't long before the Nigerian prince arrived on the scene. Fraudsters learned to manipulate electronic communication to proliferate this centuries-old scam, among others. The burgeoning increase of personal computer use in the late 1990s, along with the adoption of email as an efficient form of communication and file sharing for businesses, elevated email as a top threat vector.

Email threats quickly evolved from fairly innocuous spam and fraud attempts to include malicious attachments harboring payloads of malware that could cripple an enterprise, and organizations turned to secure email gateways as the new standard for protection. Like a firewall for email, these gateways identified threats at a single point of vulnerability – the entry point – and relied on known variables that assumed successful identification.

> "For some people, Google controls most of their identity online, and losing access to that critical account could be devastating.
>
> - Steve Ragan, CSO

As detection capabilities improved and payload-based threats were more easily recognized and thwarted, malicious actors sought new ways to compromise business via email. In the late 1990s, they found that by impersonating businesses and individuals, they could lure unsuspecting victims to click on links and readily hand over credentials or financial data.[6] And so began the era of phishing, and with it, the email security landscape changed forever.

NEXT-GENERATION THREATS PLAGUE THE ENTERPRISE

Nearly two decades later, phishing attempts have grown to be one of the greatest threats to the enterprise. A LinkedIn survey of more than 1,900 security professionals reported phishing attempts as the greatest security concern.[7] And rightfully so, as Verizon reports that 13 percent of all breaches start with

a phishing attack and an astounding 70 percent of breaches associated with nation-state or state-affiliated actors involved phishing. Email is by far the most common threat vector for social-based attacks at 96 percent, with motivations ranging from financial gain to credential theft to espionage.

A global trend that makes email an appealing threat vector for malicious actors is the growing association of email addresses with both professional and personal identities. Email addresses serve as credentials for a plethora of online business applications and systems, providing access to sensitive data such as intellectual property, customers' personally identifiable information or medical records. For consumers, email addresses are used to access everything from online shopping carts and social media to financial accounts to health portals. They are connected to almost every aspect of life, which makes stolen credentials extremely valuable.

A 2017 study by Google and UC Berkeley asserted that phishing posed a greater threat than data breaches because of the accuracy of data gleaned.[8] Results showed only 7 percent of passwords exposed by a data breach were still in use, compared to 25 percent stolen through phishing or keylogging.[9]

A recent SANS survey of 277 IT professionals confirmed that attacks exploiting users were the most common reported by respondents.[10] As many as 53 percent pointed to social engineering and phishing attacks, 50 percent cited ransomware and 40 percent reported credential theft. This data supports that email-based threats are a perpetual problem that must be addressed.

Industry-wide discussions often focus on the continual evolution of email-based threats, which continue to grow in sophistication, frequently evading traditional security measures. A quick internet search reveals a great deal of content explaining the multitude of threats, including spear and whale phishing,[11] which target fewer high-value targets versus trying to get credentials for thousands; clone phishing (also known as impersonations), which replicates the sender and message body of legitimate

BEC drives 48% of internet crime-driven financial loss, according to the FBI, which issued a formal alert on July 12, 2018. Reported in all 50 states and 150 countries, this type of impersonation attack is responsible for more than $12 billion in global losses since 2013, including $1.6 billion in U.S. losses between June 2016 and May 2018.

FBI Alert: Business Email Compromise the 12 Billion Dollar Scam

Attackers leverage publicly available information to impersonate trusted people or businesses

emails; and social engineering attacks such as business email compromise (BEC), which targets businesses that often work with foreign suppliers and/or businesses and regularly perform wire transfer payments.[12]

A deep dive into each type of attack is not warranted due to the copious amounts of information already available; however, there are a few hallmark characteristics worth highlighting:

Social Engineering
Phishers leverage manipulation tactics to prey on individuals in an effort to collect confidential information.

Impersonation
Attackers gather publicly available information and potentially data from the dark web to learn about organizations and individuals then leverage this information to impersonate people and/or businesses the intended target trusts, increasing effectiveness.

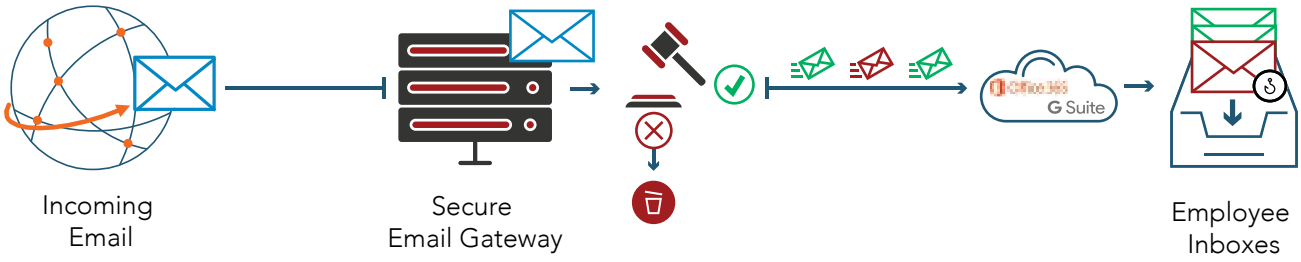
Simplicity
Each of these tactics, while sophisticated in nature, tends to be very simple in structure. Unlike advanced malware attacks, which require a high level of technical expertise, impersonation attacks can be as simple as a short email from a spoofed email address. The personally tailored content of the email is the focus, and the advent of phishing kits has made these attacks even easier for the less technical.[13]

These features, which make these advanced email threats increasingly difficult to identify and mitigate, have prompted a fundamental shift in the enterprise approach to email security.

THE RISE AND FALL OF SECURE EMAIL GATEWAYS

PROTECTION AT THE PERIMETER

While the first attempts to secure email leveraged various encryption standards and protocols, it wasn't long before the industry shifted to a gateway approach. Much like a firewall provides network security at the perimeter, secure email gateways (SEGs) serve as a similar layer of protection from external threats.[14] Functioning as a filter for inbound emails, these solutions were – and still remain – highly focused on protecting the business group from external threats. Early gateways also incorporated archiving functionality, which saved and protected historical data. This not only provided redundancy in case of outages, it prevented data loss due to system failure, allowed for e-discovery and satisfied compliance requirements.



Traditional Pass / Fail approach only protects at the entry point

Sophisticated threats bypass gateway with no easy remediation method

The SEG uses tactics such as sender reputation filters, URL filters, spam filters, and web scanners to identify known threats.[15] Over the years, SEGs gained new features and capabilities, from encryption to advanced threat detection and remediation, but the approach has largely remained binary. Even for the more advanced solutions that incorporated threat intelligence, efficacy is dependent upon point-in-time knowledge about a specific threat. Emails enter the organization's network, pass through the gateway and when an email meets conditions XYZ, it is deleted, quarantined, or addressed according to some other policy-based action determined by the organization. Success is assumed based on binary conditions having been met.

Most email security tools assume success, leaving little resource to minimize damage if a threat makes it through the entrypoint

Despite being in the cloud, integrated email security features such as what's offered in G Suite Enterprise or through Microsoft Advanced Threat Protection (ATP), operate in a very similar fashion.

Although industry authentication protocols, such as sender policy framework (SPF), domain keys identified mail (DKIM) and even Domain-based Message Authentication, Reporting and Conformance (DMARC) are helpful authentication tools[16], many organizations lack the technical talent to accurately implement and configure, rendering them inadequate as sole arbiters of safe versus unsafe emails. The 2017 Online Trust Audit and Honor Roll showed that only 35 percent of banking institutions are effectively leveraging the DKIM protocol for top-level domains.[17] Only 53 percent of retailers are doing the same and overall adoption falls around 56 percent. DMARC relies on the proper configuration of both SPK and DKIM, making it even more complex to implement, accounting for a disappointing adoption rate of just 15 percent overall. Even when effectively leveraged, these protocols cannot detect impersonation attacks that use popular free emails services, such as Hotmail or consumer-facing Gmail to mimic email addresses. Because Microsoft and Google properly authenticate these accounts, they pass authentication protocols with no issue.

Additionally, this linear approach makes it nearly impossible to detect more sophisticated attacks, such as business email compromise and other impersonation attacks. These attacks are missing the key components typically used to identify threats, such as attachments or known malicious sender information or URLs. Because SEGs - and even the integrated email security features within Office 365 and G Suite - assume success based on binary factors, they lack an enhanced means of remediation beyond quarantine. Even those that incorporate threat intelligence from external sources can only act on information that is known. Because zero-days are, by definition, threats that have not yet been publicly identified, it is impossible for threat-intelligence-heavy methods to detect and prevent them.

A CULTURE OF BLAME AND FUD

As email-borne threats grew in prevalence, distrust in users' ability to discern harmful emails skyrocketed. Many organizations developed a culture of fear, uncertainty, and doubt, blaming users that fell for phishing scams and other socially engineered attacks. Users were labeled as complacent and the perpetual "weakest link."[18] Security leaders and compliance officers called for company-wide training and awareness to help educate users as well as top-down buy-in and support to enforce policies.

> It has never been easier for scam artists to launch convincing, targeted phishing and extortion scams that are automated on a global scale. And given the sheer volume of hacked and stolen personal data now available online, it seems almost certain we will soon witness many variations on these phishing campaigns that leverage customized data elements to enhance their effectiveness.
>
> - Brian Krebs

Security training and awareness has grown to become a multi-billion-dollar industry.[19] LinkedIn's Cybersecurity Trends Report indicates that 27 percent of organizations have prioritized security training and awareness in their 2018 budget. Yet in spite of the increasing spend, the efficacy of security training and awareness programs is still lacking. Primarily delivered in the form of videos or slide presentations, they often are not representative of real-world situations. This could be why 1 in 25 users will still click on a phishing email, according to the 2018 Verizon Data Breach Report.[20]

In the best-case scenario, users become more skilled at identifying these threats, but organizations must be careful to not perpetuate the culture of fear, which can also increase risk.

A recent phishing campaign turned the typical scam on its head and preyed on users' fear of being the victim of a security breach. First reported by Bryan Krebs[21], the Sextortion scam targeted users directly as a hacker claimed to have compromised an account with malware and demanded a bitcoin payment in return for secrecy. Although the scam was consumer-focused, Krebs warned that this was just the beginning, noting the possibility of future bad actors to leverage a fresh password breach – perhaps one that the breached company wasn't even aware of yet. The best way to address this new threat is to arm users with the information they need in the moment so that they can make more educated decisions.

CONSTANTLY CHANGING INFRASTRUCTURE DEMANDS ADAPTIVE PROTECTION

In the last decade, enterprise technology has evolved to meet demands for performance and scale. Organizations of all sizes are embracing modern technology such as cloud and software-as-a-service platforms because they offer a host of benefits, including cost optimization, reduced maintenance and improved reliability and efficiency. Cloud technology enables companies to rapidly spin up new infrastructure with very little time and resources. This agility is often leveraged for testing environments and skunkworks projects, or auto-scaling for point-in-time demand. All signs point to cloud technology as the future of digital business and a clear competitive advantage.[22]

With features including email, chat, document sharing, and more, cloud-based offerings like Office 365 and Gmail enable collaboration and communication to anywhere, from anywhere, which is driving massive enterprise adoption. Computerworld reported in July 2018 that 4 million businesses have now subscribed to G Suite, Google's collection of cloud-based productivity and collaboration applications – up by 1 million from the previous year.[23] And this is just a fraction of the total number of businesses that have embraced cloud-based solutions. An April 2018 brief reported that Office 365 Commercial had more than 135 million active users – a significant piece of Microsoft's 90 percent market share.[24]

While this migration to an open, collaborative, and self-service-driven infrastructure has fundamentally increased business' ability to quickly react to market demands and remain agile in a competitive marketplace, it has created significant challenges for the security community. Often accused of being a blocker, security teams are now tasked with a seemingly impossible challenge – secure an increasingly borderless organization without impeding business operations and velocity.

Consider now the structure of traditional email solutions that have been built in the same authoritative and permission-based model as the static legacy infrastructure supporting them. In today's environment, because the perimeter is blurred, SEGs, which function as gatekeepers, cannot adequately protect the cloud user.

Inherently dynamic and adaptive, cloud architecture requires a fundamentally different approach to security. Because digital business remains in a constant state of change – with new technology, workflows and threats emerging every day – infrastructure must be ultra-agile, scalable and responsive,[25] and likewise, protection solutions must be adaptive to support this. Gartner listed this movement to a model of continuous adaptive risk and trust (CARTA) as a top ten trend for 2018.[26]

THE GROWING THREAT GAP

The disparity between the binary, perimeter-focused method and the dynamic, user-focused attributes of cloud-native email solutions is creating a growing threat gap for the modern enterprise. The fact that cloud email providers Microsoft and Google themselves rely on such outdated detection and protection methods demonstrates how engrained this mindset is within the email security community. As a result, socially engineered attacks are slipping through this gap and costing organizations millions.

Impersonation emails are the most common type of threat to penetrate this gap. Various forms of sender and URL spoofing allow BEC and other socially engineered email threats to evade SEGs. GreatHorn's 2018 survey indicated that – despite whatever email security measures they have in place – 15.8 percent of security professionals or their users see email threats (categorized as impersonations, wire transfer requests, W2 requests, payload attacks/malware, business services spoofing, or credential theft) on a daily basis, with an additional 24.2 percent seeing threats weekly – a total of 40 percent seeing email threats at least weekly.[27] Overall, nearly half of all respondents actively see impersonations bypass existing email security solutions.

Because secure email gateways rely heavily on binary good / bad evaluation, even emails with malicious attachments can slip through if the malware is not already a known threat. GreatHorn research indicated that more than 33 percent of security professionals see payload attacks bypass their SEGs. The result is that between both payload-based and payload-free (i.e. phishing) attacks, 40 percent of security professionals have to take significant remediation action (such as suspending compromised accounts, PowerShell scripts, resetting compromised third-party accounts, etc.) on at least a monthly basis, and half of those do so weekly.

Since most SEGs can't analyze intra-domain email, account takeover attacks have particularly high success rates as they come from a trusted sender.

Finally, the SEG's inherent gatekeeper approach makes it impossible to identify internal email threats. This is a key factor in why BEC attempts are so successful. Spoofed sender names look like corporate emails, and since so many organizations don't have authentication set up properly, such emails are often allowed to bypass gateways. Additionally, compromised accounts can be used in an account takeover fashion to launch internal attacks on other employees. Since most SEGs can't analyze intra-domain email, such attacks have particularly high success rates as they come from a trusted sender. Primarily targeting Office 365 users, chain phishing campaigns harvest account credentials, then use compromised accounts to amplify phishing attempts to other internal and external users.[28] Because credentials provide access to the entire Office suite – including chat functions – the attack surface in this scenario is expanded.

This threat pattern also increases the chance that the attacker will be able to secure cloud credentials, opening up the potential for corporate sabotage, intellectual property theft, exposure of customer and employee data, and much more. Needless to say, impact and loss throughout the organization can be significant.

THE FUTURE: ADAPTIVE EMAIL PROTECTION

There is an assumption that security is ingrained in the fabric of the cloud along with a consistent cycle of evaluation and remediation. Consider how many cloud-based SaaS applications dynamically prompt for two-factor authentication after recognizing the user is attempting access from an unknown device. This context-based change is triggered automatically, and users have come to expect this behavior as an additional layer of protection with cloud-based applications.

Successfully securing cloud-native email against next-generation threats requires a similar shift in our approach. Like the cloud architecture it is protecting, security must be dynamic, nuanced, and multifaceted. It should balance protection and business enablement, through automation, nuanced threat evaluation, and user empowerment.

WHAT IS ADAPTIVE EMAIL PROTECTION?

Adaptive email protection embraces the cyclical approach to security and remediation, similar to what is outlined in Gartner's CARTA model.[29] Instead of utilizing static analysis to score emails only against known threat indicators, this model

> “Anomaly detection and machine learning are helping us to find bad guys that have otherwise bypassed our rules-based prevention systems. That’s why analytics are so relevant to security operations today; they are good at finding bad guys in the data that other systems missed.”
>
> - Eric Ahim, Research Director, Gartner

embraces the nuances of context to identify threats that typically evade traditional security solutions.

Rather than simply focusing on what makes an email “bad,” such an approach also analyzes what makes an email “good” – creating a baseline for understanding the expected communication patterns for a given organization and even a given individual. Advanced technology can then be used to identify the anomalies to that pattern that can indicate a threat.

The cycle of continuous email security and remediation:

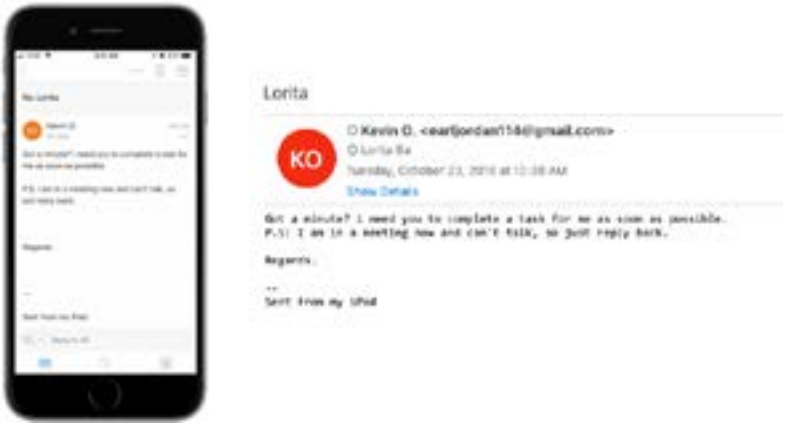
- Detect likely and known threats
- Analyze for expected communication patterns
- Administer mail according to a company’s risk tolerance
- Provide users with context-based warnings
- Easily search and remove newly identified threats from inboxes
- Continuously monitor against emerging threats

Unlike the traditional approach, which acts on known information about existing threats, adaptive email protection leverages advanced analytics about sender relationships and behavior to detect anomalies beyond the known, and subsequently uses the results to enrich a growing dataset to continuously improve efficacy.

Ideally, this cycle is continuously improving via machine learning and policy refinement as it learns and adapts to an organization’s unique communication patterns, threat profile, and risk tolerance. As a result, this approach has the critical ability to identify the payload-free phishing attempts that bypass other security measures.

For example, many popular consumer email services – like Gmail – contain features that make spoofing sender information fairly simple. Because Gmail meets typical authentication standards and the spoofed name may be familiar, this impersonation attempt would not trigger alert or quarantine from traditional email security solutions. Yet with an adaptive email solution in place, such an email would be flagged as a potential threat

after applying context based on what has been seen previously compared to the current situation. For instance, has this user received an email from this sender via Gmail before? Does this user typically only communicate with internal users? Has anyone else in the organization been contacted by this address before? Does the return path match the sender? The answers to these questions not only determine point-in-time action but also feed the continuous cycle of security and remediation.



The same email viewed on a mobile device and on a desktop. Note that on the mobile device, the email address is obfuscated.

An adaptive email security approach provides more comprehensive protection than static, perimeter-based models

The ability to use context to evaluate risk also provides an opportunity for additional user awareness training. Whereas most security awareness programs rely either on generic training sessions or targeting users through "educational" attacks, organizations employing this adaptive email protection can provide users with context as to why a given email could be a threat. This has a two-fold effect – on the one hand, users gain in-context training as to what to be aware of, and on the other hand, security professionals can be less restrictive about which emails they quarantine or block, thereby minimizing the negative impact security can have on business operations.

As organizations increasingly move toward a more open IT infrastructure that embraces cloud technology, it's critical that they also rethink how they incorporate security. An adaptive email security approach provides much more comprehensive protection than the static, perimeter-based model.

CONCLUSION

Email is the most widely used and trusted business system, yet it remains the least secure. The increasing sophistication of email-based threats and the concurrent modernization of IT infrastructure present unique challenges that demand a new approach to security. SEGs inherently lack the ability to effectively secure cloud-based email from the multitude of threats that are constantly growing in sophistication and volume.

Organizations using cloud-based email cannot expect adequate protection from traditional options that are not responsive enough to function with dynamic cloud environments. Instead, they should seek responsive, agile, cloud-native solutions with the following capabilities:

Anomaly-based Threat Detection
The ability to integrate deep relationship analytics with user and organizational profiling to identify the anomalies that typify social engineering campaigns but aren't detected by binary methods of analysis.

Emergent Threat Intelligence
The ability to block known and emerging global threats by combining real-time, global user data with threat intelligence feeds from third-party providers.

Context-based User Engagement
Automated, contextual warnings and reminders that help employees make better decisions by providing contextual information (e.g., warning banners on emails or link protection with a destination site preview.)

Automated Defense
The ability to easily adjust automated response actions (e.g. quarantine, user warnings, etc.) based on an organization's risk tolerance, business processes, and enforced policies.

Post-Delivery Incident Response
The ability to identify breadth of exposure from newly identified threats and remove them from user inboxes, even post-delivery, with no time restrictions.

Organizations should also consider solutions that connect users to resources – for instance, reminders about corporate wire transfer policies or links to tips for identifying phishing attempts – in real time, enables them to make informed choices about what action to take in the moment. This in-context user awareness training can augment mandatory, periodic awareness training, creating a more educated, effective workforce.

The time has come for the transformation of email security from binary, static email filtering to a cloud-first, context-based strategy that embraces adaptive email protection and transforms users from "the weakest links" into IT partners.

ABOUT GREATHORN

GreatHorn simplifies email security by automating the cycle of email security – through continuous threat detection, defense, and incident response. Office 365 and G Suite customers using GreatHorn not only gain enterprise-class protection against both sophisticated phishing attacks and traditional threats, they also reduce complexity, manual remediation time, and negative impact on business operations.

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. More information is available at www.greathorn.com.

GreatHorn

Corporate Headquarters:
260 Charles Street, Suite 300, Waltham, MA 02453

Phone: 855-478-4676 | **Email:** info@greathorn.com

REFERENCES

1. The Radicati Group. "Email Statistics Report 2015-2019." May 2015.
2. Workplace of the future. DXC.Technology. "Why email still isn't going away." Chris Nerney, July 2018.
3. GreatHorn. "Trends, Challenges and Benchmarks in Email Security," July 2018.
4. LinkedIn. "Cybersecurity Trends: 2017 Spotlight Report." 2017.
5. Springer. "Encrypted Email: The History and Technology of Message Privacy." H. Orman, 2015.
6. Computerworld. "Sidebar: The Origins of Phishing." Russell Kay, January 2004.
7. LinkedIn. "Cybersecurity Trends: 2017 Spotlight Report." 2017.
8. "Data Breaches, Phishing or Malware: Understanding the Risks of Stolen Credentials." Google, University of California, Berkeley, and the International Computer Science Institute, 2017.
9. CSO. "Why you should fear phishing more than data breaches." Steve Ragan, November 2017.
10. Dark Reading. "Less Than Half of Cyberattacks Detected via Antivirus." Kelly Sheridan, July 2018.
11. CSO. "Types of phishing attacks and how to identify them." Famida Rashid, October 2017.
12. FBI Internet Crime Complain Center. "2017 Internet Crime Report." May 2018.
13. CSO. "What are phishing kits? Web components of phishing attacks explained." Steve Ragan, August 2018.
14. Network World. "How do messaging-security gateways work?" Joel Snyder, October 2007.
15. Dark Reading. "How Many Layers Does Your Email Security Need?" Chris Harget, June 2016.
16. SearchSecurity TechTarget. "Phishing." Margaret Rouse, October 2017.
17. Online Trust Alliance. "2017 Online Trust Audit and Honor Roll." The Internet Society, 2017.
18. SANS Institute. "The Weakest Link…This Is Not a Game!" Jack Daniels, 2001.
19. Cybersecurity Ventures. "Security Awareness Training Explosion." John P. Mello, February 2017.
20. Verizon. "2018 Verizon Data Breach Report." April 2018.
21. Krebs on Security "The Year Targeted Phishing Went Mainstream." Brian Krebs, August 2018.

22. Gartner. "Top 4 Challenges Facing IT Infrastructure Leaders." Susan Moore, April 2018.

23. Computerworld. "Google touts G Suite momentum in office productivity battle." Matthew Finnegan, July 2018.

24. Reuters. "Microsoft CEO Says Office 365 Commercial Now Has More Than 135 Million Active Monthly Users." April 2018.

25. Gartner. "Top 4 Challenges Facing IT Infrastructure Leaders." Susan Moore, April 2018.

26. Gartner. "Gartner Top 10 Strategic Technology Trends for 2018." Kasey Panetta, October 2017.

27. GreatHorn. "Trends, Challenges and Benchmarks in Email Security," July 2018.

28. InfoSecurity Magazine. "Chain Phishing Attack Against Office 365." Ryan Campbell, October 2017.

29. Gartner. "The Gartner IT Security Approach for the Digital Age." Kasey Panetta, June 2017.