solarwinds

eBOOK

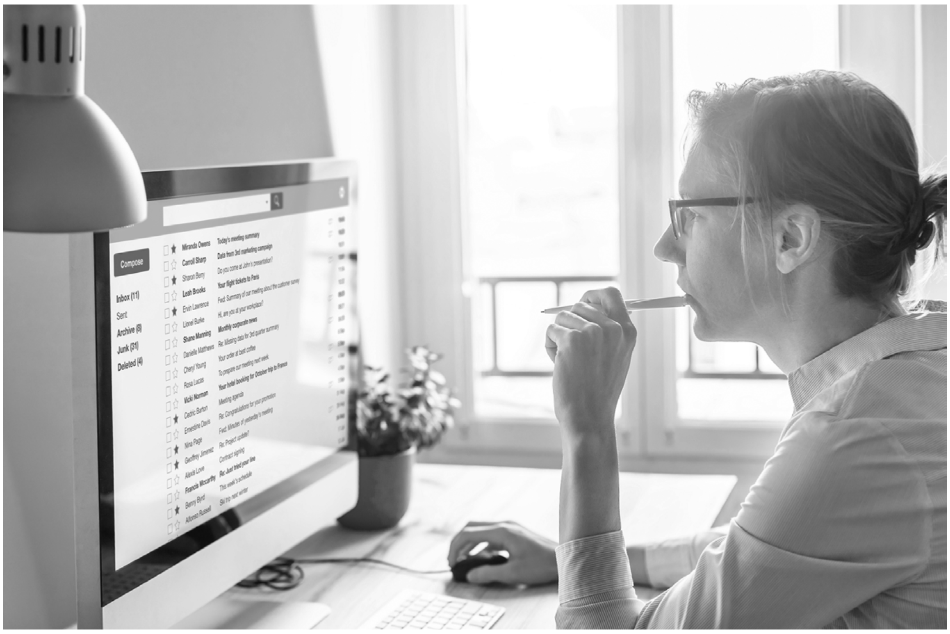
The MSP Email Security Guide: 2020 Edition

Introduction

Email remains one of the most fundamental and important elements of any security strategy. While cybercriminals launch many attacks via email, businesses can drastically reduce their risk by practicing stronger email security and putting in proper technical safeguards.

Email continues to be a vulnerability due to the human element. It's easy enough for cybercriminals to create convincing-looking fake messages that victims don't bat an eye at—particularly when they're tired, overworked, or distracted. Employees working from home often must balance competing priorities, including meeting deadlines, responding to emails, joining video conferences, and watching children. Unfortunately, watching for misspelled domain names that can indicate spam may not be as high on their priority list as it should be. At the time of this writing, cybercriminals are also using events and fears around COVID-19 to capture the attention of people seeking information on health, employment or financial resources, or stimulus checks.

As an MSP, your customers need you to protect them from this. Employees need to do their share as well, but you play a major role in keeping those employees and their companies protected. This eBook will cover some of the major email threats in the current environment, steps you can take to reduce your customers' risks, and the benefits to your MSP of providing email security to customers.



The State of Modern Email Threats

Cybercriminals love email—they deliver 94% of malware with it.[1] And based on data from SolarWinds MSP, we saw an increase of more than 80% of phishing and malware attacks in March 2020 alone.[2] Email provides easy access to victims, and cybercriminals can easily forge or fake them. Plus, some attacks require little-to-no programming knowledge, making the barrier to entry low for people looking to turn a quick profit. Here are just some common threats we see in today's market.

PHISHING

Phishing involves sending a fake but legitimate-looking email to a large group of people, hoping some percentage of recipients will take the bait and click a malicious link. This link will lead users to fake sites attempting to steal user credentials, banking information, or other personal information that could be valuable to the hacker.

Cybercriminals have multiple ways of hooking users' attention. Some may even use cyberbreaches themselves as lures by sending emails claiming to be a banking institution reporting a breach and asking you to change your credentials. Others use timely or relevant events as a lure. At the time of this report's writing, we've seen phishing scams claiming to come from government officials or medical professionals with advice on COVID-19. The US Federal Trade Commission (FTC) has issued guidelines on avoiding scams for emails concerning stimulus checks or emails coming from the Centers for Disease Control or the World Health Organization.[3]

While most people won't click the link in any given phishing campaign, the 2018 Verizon Data Breach Investigations Report found that 4% of people will.[4] While the percentage is small, it's enough for spammers to turn a profit and continue pursuing these attacks.

[1] "2019 Data Breach Investigations Report," Verizon. enterprise.verizon.com/resources/reports/2019-data-breach-investigations-report-emea.pdf (Accessed April 2020).

[2] "Email Security Education: Cybercriminals Capitalizing on Coronavirus and Work from Home Measures," SolarWinds MSP. solarwindsmsp.com/blog/email-security-education-cybercriminals-capitalizing-coronavirus-and-work-home-measures (Accessed April 2020).

[3] "Coronavirus Advice for Customers," US Federal Trade Commission. ftc.gov/coronavirus/scams-consumer-advice (Accessed April 2020).

[4] "2018 Data Breach Investigations Report: Executive Summary," Verizon. enterprise.verizon.com/resources/reports/DBIR_2018_Report_execsummary.pdf (Accessed April 2020).

SPEAR-PHISHING

Phishing is still common, but many email providers have improved their ability to detect bulk email. Cybercriminals, however, have adapted.

Enter spear-phishing. Spear-phishing involves targeting specific individuals within an organization to attack by using upfront reconnaissance to make their scam attempts more convincing. This requires more work but can increase the success rate of the attack.

Let's say your MSP handles IT and security for a 30-person accounting firm. The organization lists executives' names and corporate email addresses on the website. From here, the cybercriminal can use this small amount of information to perform some recon on members of the organization. They could check data breach dumps on the dark web for information on the victims—such as their names, addresses, social security numbers, or even their preferred bank. They could also check social media accounts on the victims for further information. Once they have this information, they can craft very convincing emails to executives requesting sensitive information, like customer data, or they can trick them into giving up their user credentials. According to research from Infosec, 30% of spear-phishing campaigns succeed.[5]

DISPLAY NAME SPOOFING

Display name spoofing involves forging a sender's name to make the message appear to originate from someone or somewhere other than the actual source. This technique is often used in phishing campaigns to obtain user credentials.

The security industry has successfully made it harder for attackers to forge domains due to authentication protocols like Sender Policy Framework (SPF), Domain Keys Identified Mail (DKIM), and Domain-based Message Authentication, Reporting, and Conformance (DMARC). To get around this, cybercriminals use display name spoofing to make their emails appear to come from an executive (c-level) in the targeted organization. For example, an attacker can register a free email account and use any email address. Sometimes the address contains the name of the executive they're trying to spoof, but even this isn't necessary. The attacker then sets their display name to match an executive's and launch targeted phishing campaigns. Cybercriminals hope recipients will look only at the display name and not the email address. Some recipients may even assume the sending email is the personal email of the executive and believe it's real.

[5] "The Trends in Spear Phishing Attacks," Infosec. resources.infosecinstitute.com/the-trends-in-spear-phishing-attacks/ (Accessed April 2020).

MALWARE AND OTHER ATTACKS

Cybercriminals often use email as a delivery mechanism for other malicious cyberattacks. All it takes is one click on a malicious link to download ransomware, illicit cryptomining software, or spyware onto an endpoint. These attacks could then propagate out to other machines or completely take down a network.

Beyond malware, cybercriminals often use email to deliver attacks that can slip past traditional antivirus (AV) solutions. For example, someone could download an excel spreadsheet that then launches a macro designed to create a new user account with admin privileges on the machine. Most AV solutions will only scan the original spreadsheet, and they won't catch the malicious behavior from the document macro. Unless you have a robust endpoint protection solution in place, the cybercriminal can have a field day with that endpoint.

Evasion techniques aren't limited to the endpoint either—many current attacks are built to bypass email security scanners (and their end users). For example, while the AV in many email programs will recognize executables or PDFs as potentially malicious, fewer think twice about HTML attachments. Cybercriminals frequently use HTML files to deliver malware via embedded JavaScript or send users to spam sites via URL redirects. Regardless, users and email security programs need to be on their guard against the latest attacks.

THE FOREST AROUND THE TREES

There's a common theme among all these threats—they're usually only one step in a larger attack. While large-scale attacks, like WannaCry, get most of the ink in the press, email threats remain common and often serve as the first infection point. If someone uses a phishing email to steal user credentials for a company, they can get access to other parts of the network and potentially do significant damage. While you need other defenses to prevent attacks, like patch management, endpoint protection, or information-and-event-management (SIEM) tools, email protection should still be a major part of any security stack.

Reducing Your Email Security Risks

To prevent email attacks, it helps to add multiple layers of protection to your email infrastructure. An email gateway designed for security can help reduce spam levels, catch phishing, prevent malware, and reduce the burden on employees trying to remain vigilant while facing competing priorities.

Most email security solutions include AV and anti-spam engines. These supplement the native AV and anti-spam filtering in most email products, like Microsoft 365™ (formerly Office 365®), Microsoft Exchange™, or Google® G Suite®. However, to deal with modern threats, email security solutions need to go further both in terms of the quality of their AV and anti-spam protection and the breadth of the features they offer. When you're considering an email security solution, look for the following features.

ACCURATE EMAIL FILTERING

Businesses can't afford to miss important emails. While they should stay protected from email threats, some email security solutions can get too aggressive, filtering out important communications the business needs to operate. The last thing you want is someone losing a potential sales deal because their email landed in the junk folder. Ask the vendor about both their detection and false positive rates. Although, don't just take their word for it—test the system during your trial period. If you miss vital emails or receive too many suspicious messages, you should continue looking for a different solution.

Additionally, you may want to look for a solution that uses near real-time pattern recognition, collective intelligence, and machine learning to better detect threats and reduce false positives.

SUPPORT FOR SPF, DKIM, AND DMARC

We mentioned earlier how some authentication protocols have helped prevent a multitude of email threats. To protect yourself, make sure to enable SPF, DKIM, and DMARC to further clamp down on domain-based spoofing emails.

SPF restricts which mail servers can send email for a specific domain name. This framework helps detect and block domain-based email spoofing. DKIM signs outgoing messages with a digital signature so the recipient can verify the email came from the domain it claims to be. DKIM not only helps reduce spoofing attacks, particularly when used in combination with SPF, it also reduces the chances of legitimate emails being identified as spam. DMARC is an email protocol designed to help prevent email spoofing when used in conjunction with SPF or DKIM. It helps extend and strengthen both SPF and DKIM.

VISIBILITY AND CONTROL OVER EMAIL FLOW

When looking for an email protection solution, look for one that lets users train the system themselves by marking something as "spam" or "not spam." Your technicians don't have time to babysit this portion of email management. Instead, a solution that offers a self-service portal where end users can mark emails as "spam," release legitimate emails from their quarantine, and blacklist or whitelist senders on their own frees your technicians to work on other projects.

BUSINESS CONTINUITY PROTECTION

When email stops, business stops. Sales can't communicate with customers. Account managers can't continue providing strong service. Internally, project deadlines get missed because people don't receive messages on time.

Your email security solution should allow customers to continue writing, sending, and receiving email, even if the primary email service goes offline. Vendors should provide a cloud-based web console that users can log into to continue working during an outage. The console should be backed by redundant servers in multiple locations to both maximize uptime and meet geographic storage requirements.

EMAIL ARCHIVING

Too often, businesses end up losing important emails. Someone may accidentally delete an email or even a full folder, or their email provider may store email for a relatively short period of time. The real challenge here is that many regulated industries require businesses to preserve most or all data, including emails, for a specific amount of time. If you can't keep email for the long haul, then you (or your customers) could end up facing severe fines. Beyond that, an archive can help if you simply need to retrieve an email (or series of emails).

Your email security solution should include an email archive that stores emails for the long haul. Look for one that lets you set custom retention periods, so you can meet varying customer needs. Finally, grill salespeople on how they keep the archive secure. You may need to demonstrate this in the event of audit, so upfront research is a must.

COMPATIBILITY AND FLEXIBILITY

As an MSP, your customers have varying needs. Many want to stick with their in-house email solution, so it's critical you choose an email security gateway that works with nearly any email service. However, this goes beyond landing new customers—it also helps in keeping customers around. For example, if a customer decides to switch their service, the right email security platform can make for a seamless transition without a dip in security performance.

INTEGRATION WITH MICROSOFT 365

With the shift to move more resources to the cloud and adopt SaaS applications, businesses of all sizes widely use Microsoft 365. While Microsoft 365 includes built-in security, it does have limitations. Adding an email security solution that integrates easily with Microsoft 365 and lets you onboard customers quickly and easily is important.

Additionally, to increase efficiency across your business, look for an email security solution that synchronizes with your Microsoft 365 account to automatically add new Microsoft 365 mailboxes, distribution lists, shared mailboxes, and mailbox aliases so you don't have to go back and manually add those mailboxes one by one. Microsoft 365 will likely only grow in adoption—so make sure you have additional layers of protection to help protect your customers' data.

SECURITY TRAINING

While an email security solution is essential, teaching users to be on guard against potential threats also makes a major difference. Make sure to hold regular security trainings with your customers to emphasize what to look for in a potentially malicious email. Additionally, it's worth sending periodic refreshers on the training to your customers. Not only can this help them stay secure, it's an additional method of reminding them of the value your IT business provides.

Why Email Security Matters to MSPs

Cybercriminals have become more coordinated and sophisticated in their attacks. And small- and medium-sized businesses (SMBs) have increasingly become targets. A report from Ponemon and Keeper Security claims 67% of SMBs have faced a cyberattack.[6] SMBs are enticing to cybercriminals because they often have lower levels of security than bigger companies, yet still have valuable data to steal or encrypt.

This places MSPs squarely on the front lines of this fight. MSPs must keep their customers secure if they want to keep their business, as many SMBs don't distinguish between IT and security services. If their computer stops working and they can't access documents required to do their jobs, you don't want to have to tell them it was their fault for opening an email with ransomware attached to it. Additionally, over the past year, we've seen an increasing number of attacks focus on MSPs themselves. This means you'll need to make sure your own in-house security practices—from email security to patching to password practices—meets the highest standards. If criminals can breach your MSP, they can seriously harm your business and your customers.

Ultimately, stronger email security can help you:

- **Retain customers:** When times are uncertain, businesses need to know their IT providers have their backs. Especially with the rise in phishing attacks , having strong email security in place can reassure customers they're in good hands and help them stay with your company longer.
- **Stand out in a crowded marketplace:** Imagine this scenario—someone leaves their MSP because of a data breach. Suddenly, they've become very security-conscious in a way they haven't before. Showing how you offer strong email security could help bolster your case and win you the sale. As more MSPs offer security services, email protection in your security stack becomes a must to maintain.
- **Expand your service offerings:** Adding email security into the mix lets you offer more value and charge more in your service packages. Plus, if you use a solution that offers email continuity, you can leverage this as part of an overall business continuity package. As people increasingly work from home, being able to access email even during an outage can be a lifesaver.

[6] "2018 State of Cybersecurity in Small & Medium Size Businesses," Ponemon and Keeper Security. start.keeper.io/2018-ponemon-report (Accessed July 2019).

- **Improve compliance:** Many regulations require businesses to keep data for a long period of time. If critical emails get lost, this can lead to fines or other punishments. Having a good email security solution that includes optional archive storage can help you better meet these compliance requirements.
- **Drive profitability:** When you reduce the time technicians spend managing email and quarantines, you free them up to work on other projects. This increases your efficiency, which can potentially reduce your overall labor costs or help you chase earn revenue by moving techs onto new, higher-value services. Plus, with stronger email security, you'll spend less time remedying security issues.

Browse Our Other Security Resources

Email security is critical for IT services providers. Yet, it's only one piece of the puzzle. A strong security strategy requires multiple technologies and sound processes and policies to truly minimize risk. SolarWinds MSP offers multiple free resources on everything from helping secure networks and devices, protecting user credentials and accounts, fighting social engineering scams, and thinking strategically about risk and security postures.

Get free security eBooks, infographics, case studies, and white papers by visiting our resource library.

We also publish frequent updates on all things security on our blog. Learn more by browsing the articles today.

ABOUT SOLARWINDS

SolarWinds (NYSE:SWI) is a leading provider of powerful and affordable IT infrastructure management software. Our products give organizations worldwide, regardless of type, size, or IT infrastructure complexity, the power to monitor and manage the performance of their IT environments, whether on-prem, in the cloud, or in hybrid models. We continuously engage with all types of technology professionals—IT operations professionals, DevOps professionals, and managed service providers (MSPs)—to understand the challenges they face maintaining high-performing and highly available IT infrastructures. The insights we gain from engaging with them, in places like our THWACK online community, allow us to build products that solve well-understood IT management challenges in ways that technology professionals want them solved. This focus on the user and commitment to excellence in end-to-end hybrid IT performance management has established SolarWinds as a worldwide leader in network management software and MSP solutions. Learn more today at www.solarwinds.com.

solarwinds

For additional information, please contact SolarWinds at 866.530.8100 or email sales@solarwinds.com. To locate an international reseller near you, visit http://www.solarwinds.com/partners/reseller_locator.aspx

SOLARWINDS DISCLAIMS ALL WARRANTIES, CONDITIONS, OR OTHER TERMS, EXPRESS OR IMPLIED, STATUTORY OR OTHERWISE, ON THE DOCUMENTATION, INCLUDING WITHOUT LIMITATION NONINFRINGEMENT, ACCURACY, COMPLETENESS, OR USEFULNESS OF ANY INFORMATION CONTAINED HEREIN. IN NO EVENT SHALL SOLARWINDS, ITS SUPPLIERS, NOR ITS LICENSORS BE LIABLE FOR ANY DAMAGES, WHETHER ARISING IN TORT, CONTRACT OR ANY OTHER LEGAL THEORY, EVEN IF SOLARWINDS HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.