

5 Email Methods

Cybercriminals

Are Using

in 2021



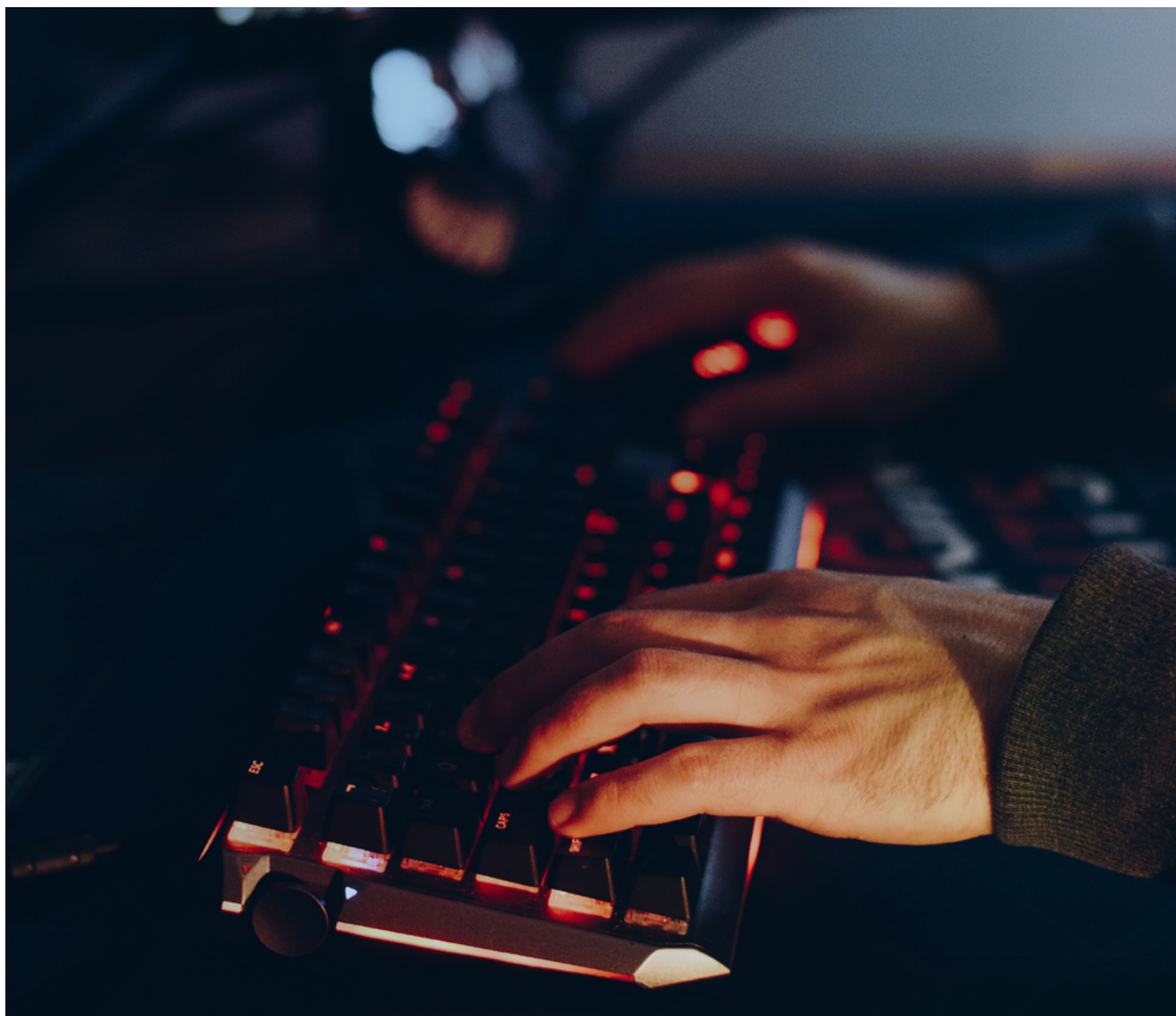
2020 was one of the most dangerous years ever in cybersecurity. The average cost of a data breach in the U.S. reached \$8.19 million. In 2021, cybersecurity threats are increasing by the day, with cybercriminals continuously updating their tactics and putting more companies at risk for both data and monetary losses.

### How widespread is the problem?

More than 80 percent of organizations have reported being the victim of some type of data breach, targeted email attack, successful phishing attack, or other security incident during the previous 12 months<sup>1</sup>.

Many of the most damaging attacks launch via emails designed to dupe unwitting employees. While non-email channels are becoming a larger avenue for cybercriminal activity, email is expected to remain the primary attack vector for the next several years.

Within this ever-changing security landscape, IT administrators and end-users alike are tasked with ensuring online security remains tight, and this especially applies to email. In this eBook, you'll learn about the latest email security trends and threats, as well as the best practices and tips to combat them.



<sup>1</sup>Source: Osterman Research

# The Latest Cybersecurity Techniques

Forms of email threats are constantly changing, making it difficult to protect an organization from attacks.

## What specific forms are these cyberthreats taking?

- 94% of malware is delivered through email.
- However, 86% of today's email attacks do not include malware; instead this type of increased activity works through tactics such as social engineering and email fraud.
- No matter the motive of cybercriminals, the truth is that 95% of security breaches are caused by human error.

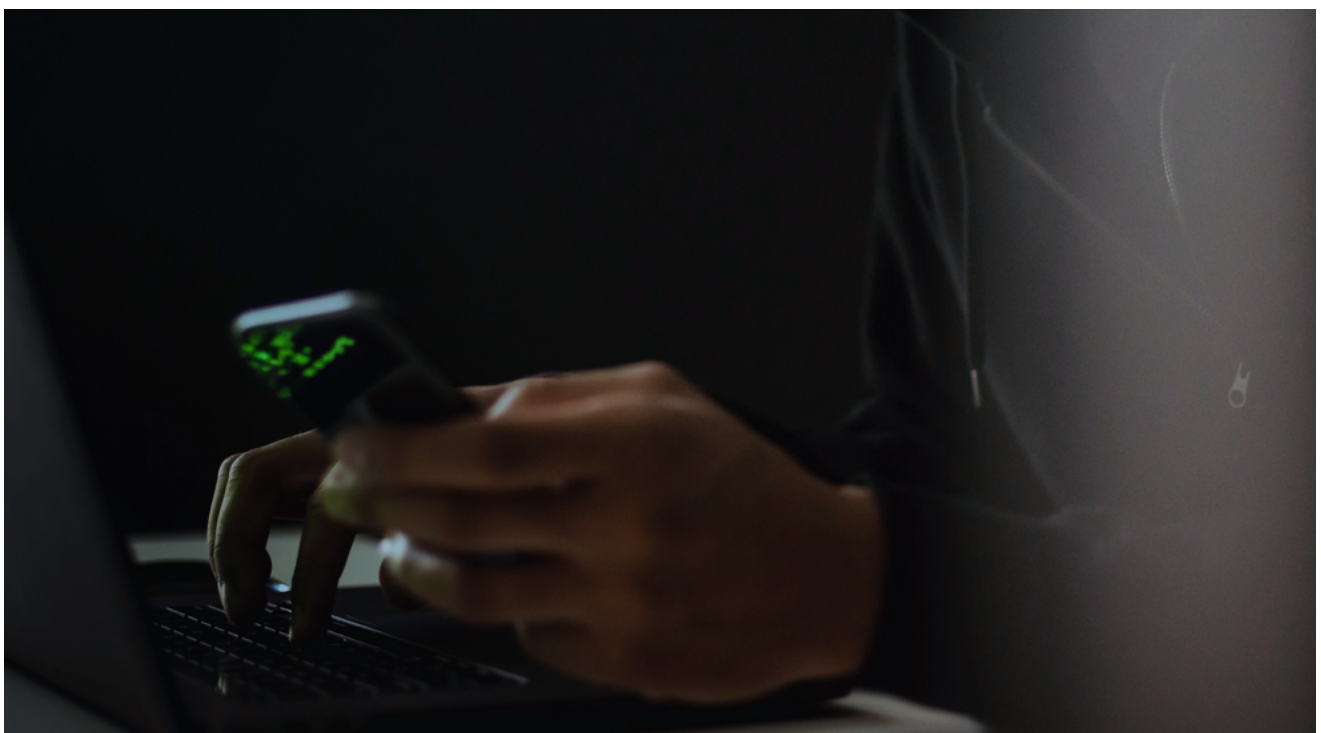
As "spam" email will continue to be a primary tool for cybercriminals, it's helpful to consider how many emails that could be. It's estimated that there were 4 billion email users in 2020, 244.5 million in the U.S. alone. It's estimated that between 60 and 107 billion spam emails will be sent each day through 2023.

Let's take a closer look at the potentially dangerous contents of your organization's email.

## Evolving Phishing Attacks

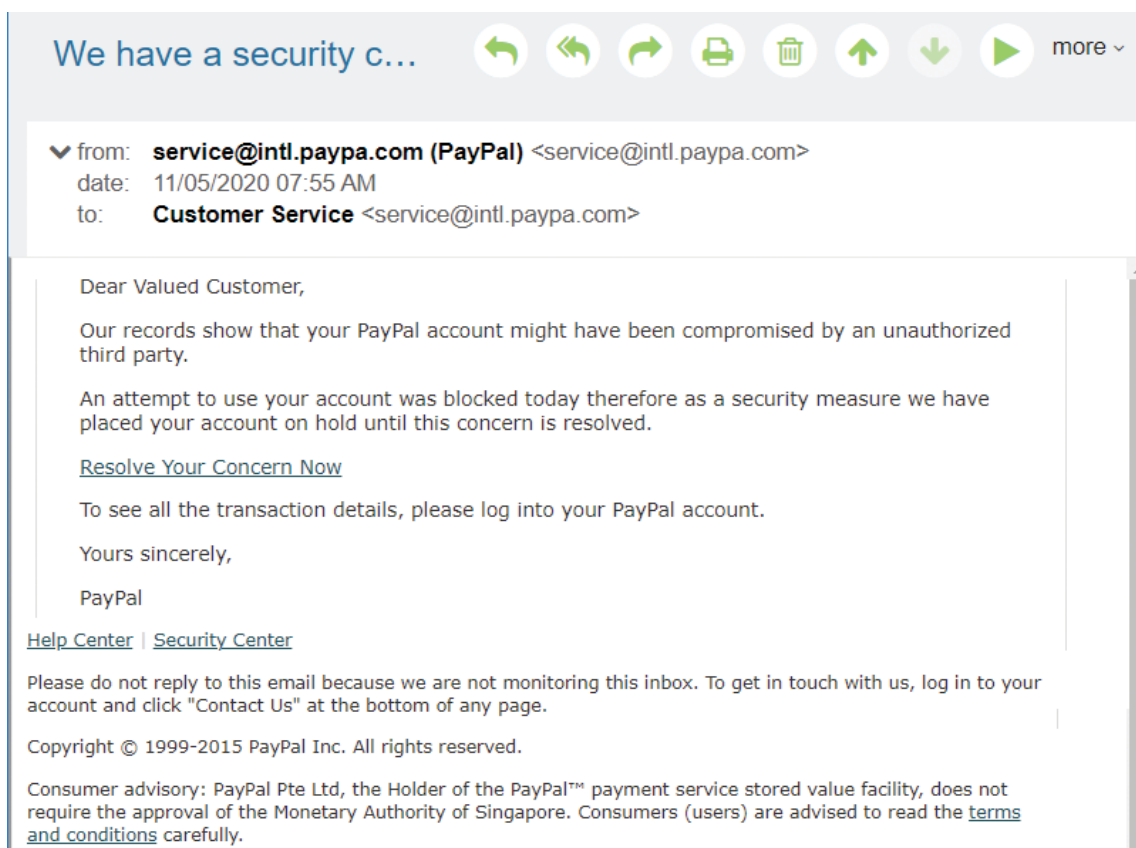
The word "phishing" denotes exactly how these email attacks work: Cybercriminals send fraudulent, malicious emails to a wide ocean of recipients, "phishing" for the few "bites" that will allow them to infiltrate an organization's network, obtain passwords, and burrow deeper into potentially damaging areas. It works so well that 95% of security breaches start with successful phishing attacks.

The version of phishing that most workers are aware of today is the traditional infiltration technique where the email encourages the recipients to click on a link or download an attachment. Taking this action gives the bad actor access to the recipient's computer or tricks the recipient into supplying critical identifying information such as passwords, social security numbers, etc.



## Phishing Survival Tips

MDaemon Technologies has been publishing [phishing survival tips](#) for years. Phishing attempts continue to make headlines, and hackers love [to impersonate large corporations \(e.g. PayPal\)](#) to take advantage of their more vulnerable users.



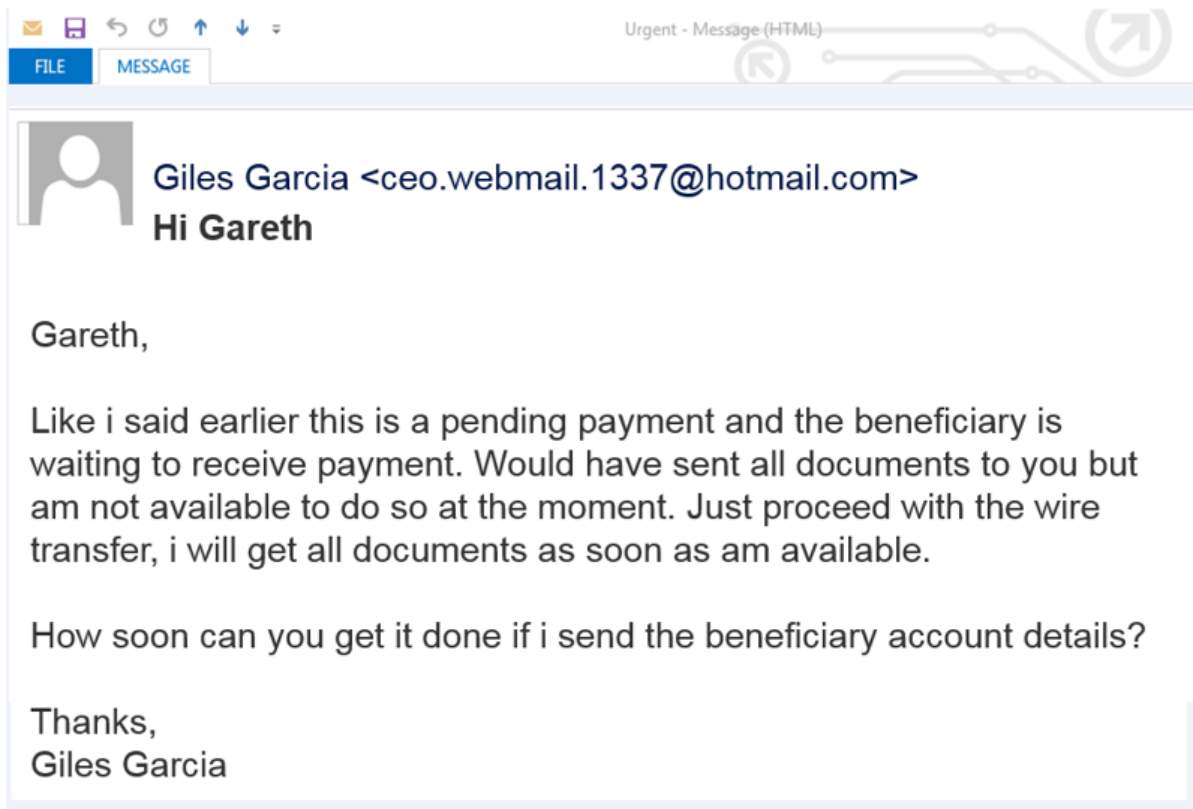
Recent email attacks are much more subtle and therefore more difficult to identify as dangerous. Here are a couple of the latest trends email administrators and employees must be on the lookout for.

## Business Email Compromise (BEC)

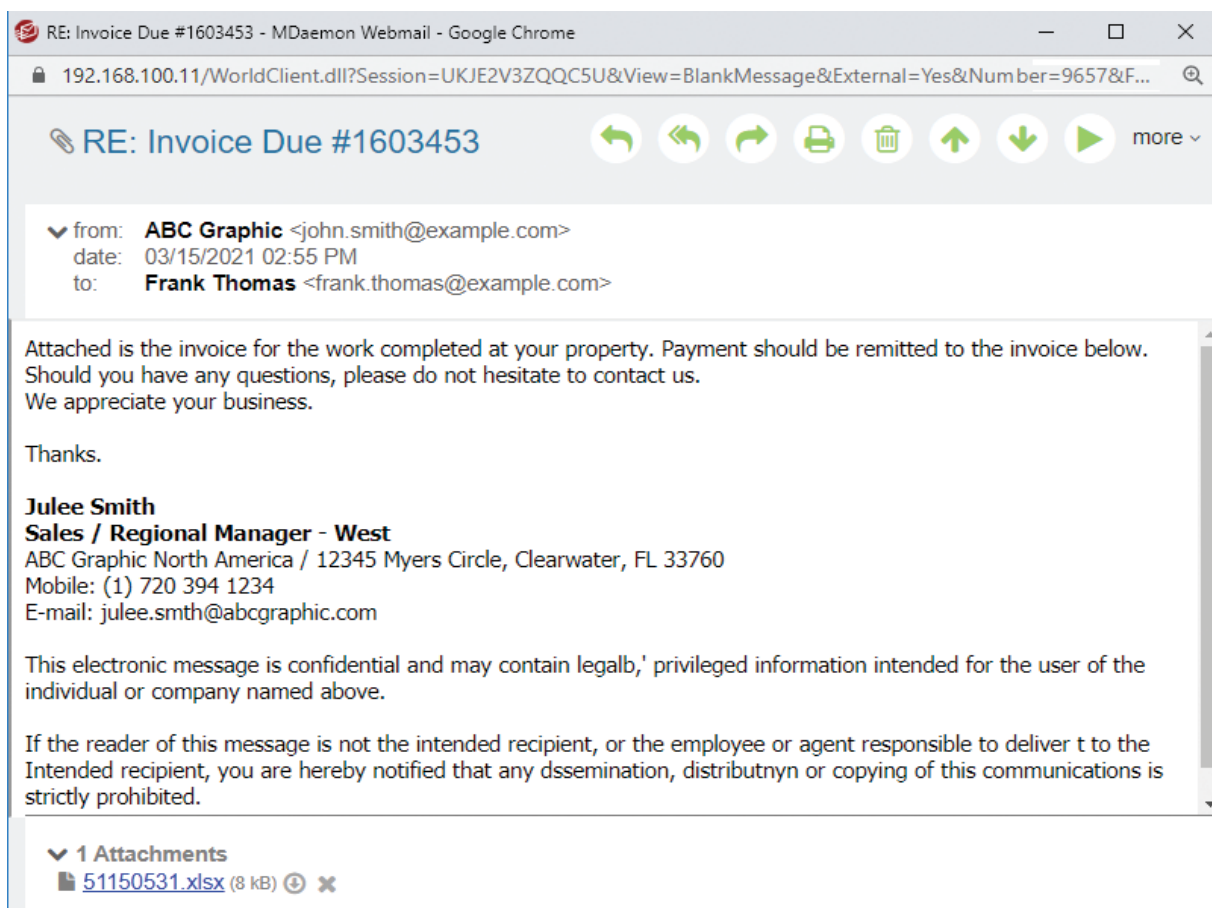
These attacks don't phish by sending the same message to untold numbers of recipients. Business Email Compromise begins when cybercriminals take the time to gather information on company personnel through company websites and social media, and then use this information to send emails impersonating actual employees and asking the recipients to perform normal business functions. Because these emails don't include malicious links or attachments, they are able to bypass traditional secure email gateway protections. Once the criminals gain access, they often lurk undetected for weeks or months, learning privileged information and communication patterns they can later exploit.

BEC is so successful that, during the third quarter of 2020, the median number of BEC attacks received per company each week rose by 15%, quarter over quarter. A recent Anti-Phishing Working Group (APWG) report found that the average loss from a wire transfer BEC attack was \$80,183 in the second quarter of 2020 — a 32% increase over the first quarter. Here are some specific forms of BEC attacks:

- CEO fraud: Attackers impersonate a company CEO or other executive through fake emails in an attempt to get any employee to execute unauthorized wire transfers or turn over confidential tax information.

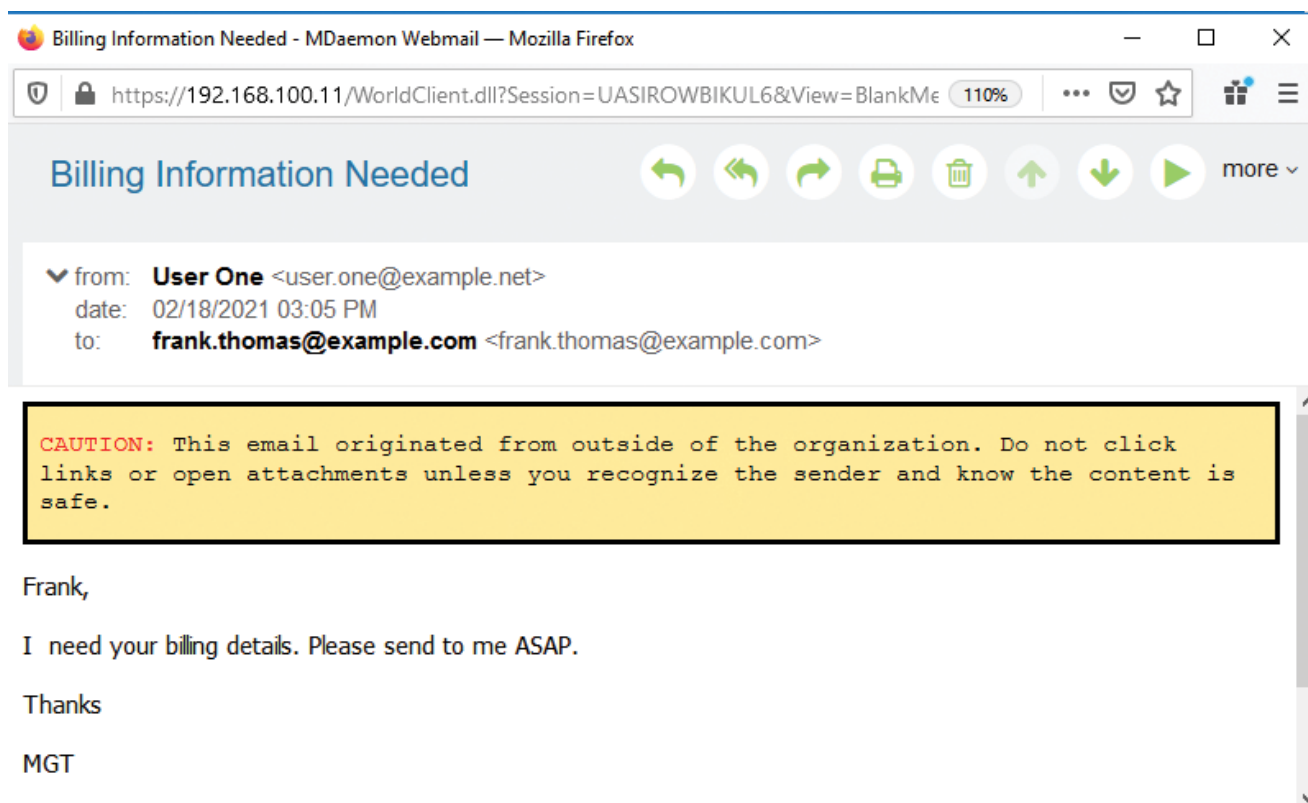


- Account compromise: Attackers hack a relevant employee's account and then use those qualifications to request invoice payments.
- Vendor email compromise: Instead of targeting client companies, attackers use BEC techniques to infiltrate vendors and wait for opportunities to, for instance, re-route ACH payments by impersonating the vendor in accounts-payable emails.
- False invoice scheme: In an attack that combines the ideas presented above, this scheme commonly targets someone in a company's financial department to receive a legitimate invoice that includes fraudulent charges to bank account numbers and other information like payment amounts.



## BEC Survival Tips

The social-engineering aspects of BEC attacks can be implemented in ever-increasing ways, limited only by attackers' ingenuity and motivation. Your company's best defense is to educate and encourage all employees to stay continually vigilant about the potential dangers of social-engineering attacks.



[Learn more about MDaemon Technologies' techniques and tips for BEC vigilance.](#)

To help users more easily identify suspicious emails, MDaemon administrators can enable a content filter rule that adds a warning header to the top of emails originating from external sources.

## Ransomware

Ransomware is exactly what it sounds like: Cybercriminals use email to gain access to company data and then "hold" this data for ransom. Specifically, they often use social engineering to trick the email recipient into opening a malicious attachment or clicking on a malicious link, which then installs the ransomware onto their system and locks their files until they pay up.

A ransomware attack can encrypt a user's files without actually granting cybercriminals access to the data. However, in recent years the business entities most targeted in these attacks have the potent combination of cash on hand, a vast bank of sensitive information, and plenty of motivation to pay quickly to recover their data – and that has most often translated to healthcare organizations and public-sector entities like city and county governments. By November 2020, these organizations were facing an average of 626 attacks per week – nearly 90 attacks every day. Ransomware attacks against healthcare organizations alone jumped 45 percent in November 2020 and 71 percent in October 2020, when healthcare entities were the number-one target. An average ransom payment? \$110,000, with an annual haul of more than \$150 million overall.

### Ransomware Survival Tips

Because ransomware is another email-security risk, the best way to avoid becoming a victim is to develop and reinforce strong email security practices, such as regularly changing and using strong

passwords, never opening attachments or clicking on email links from untrusted or unknown sources, and encouraging employees to never post email address or work information on social media sites.

To learn more ransomware survival tips, read [Avoid Being a Victim in New Massive Ransomware Outbreak](#) which covers the eight best practices for email administrators.

## Smishing

Apply the fraudulent principles of phishing to SMS messages on mobile devices, and the result is the meteoric rise of “smishing” scams. They get special mention here because, not only do the attacks impersonate package delivery and streaming services, online retailers, and other common service providers – they also claim to be from internet and email providers. The scheme tries to get recipients to provide sensitive information either through SMS or at a spoofed website, or to even download and install malware.

### Smishing Survival Tips

Waste no time adding warnings about smishing to your employee education efforts. Let them know the circumstances under which your business would ever text them on private devices – and that no one will ever text them privately about their work email. Just as they should be with emails, your employees should always be wary of unsolicited texts and should confirm any content directly with the supposed sender, without providing any response to the text.

## Security Breaches from Within: The Challenge of Data Leaks

The goal of the cybercriminal is to gain access to, or leakage of, proprietary or financial data, and as noted above, the real scare is that 95% of security breaches are caused by human action. If an employee unintentionally sends confidential data, or worse, a cybercriminal manages to breach an employee account to gain access to that data & expose it, your company could be held liable for violating data privacy and compliance regulations.

Data leaks have become such a threat that:

- Nearly one-third of organizations have experienced an accidental leak of sensitive or confidential information.
- 53 percent of security teams are at least somewhat concerned about accidental breaches of sensitive or confidential data by employees.

Your organization should take the potential for data leaks seriously – and protection doesn't have to be complicated or expensive. In addition to your employee training activities, MDaemon Technologies' Security Gateway provides clear and specific administrative steps for [taking control of data leaks](#). Security Gateway includes over 60 data leak prevention rules, along with options for creating your own custom rules to suit your specific business environment. Messages containing Social Security numbers, bank account numbers, healthcare terms, and other sensitive data can be quarantined for administrator review, encrypted, or rejected, among other options.

# The Latest Changes On the Business Landscape

Now that we've defined the latest types of attacks targeting email, let's take a closer look at the current events exacerbating the explosion of email security threats.

## The Pandemic

Email security is only one of a myriad of processes that are changing as a result of the coronavirus pandemic. As noted above, cybercriminals have had a field day targeting healthcare organizations of all kinds around the world; they've also exploited fears surrounding the virus to spread malware and misinformation, both among business employees and the general public. Finally, as vaccines started rolling out, the number of web application attacks against healthcare organizations spiked by 51 percent – to the extent that healthcare organizations experienced 187 million attacks in total, or roughly 500 per organization.

### Pandemic Survival Tips

In response to the spike in pandemic-related online scams, MDaemon Technologies compiled a list of information and resources, including their own [best practices](#) to avoid email scams and to administratively tighten email security.

## Targeting Remote Workers

More employees are now working remotely than at any time in history. This provides a wide range of targets for cybercriminals, who try to exploit weaknesses in endpoint devices like personally owned desktop and laptop computers, and even mobile devices that are now regularly used to access proprietary business systems.

### Remote Work Survival Tips

Part of criminals' efforts here go toward "spoofing" email domain names and other tactics to look authentic enough to fool those working from home in a potentially distracted state. It's even easier on mobile devices where domains are hidden completely. MDaemon Technologies has published best practices for [securing work devices at home](#) and [improving work-from-home security](#).





## Cloud Migration

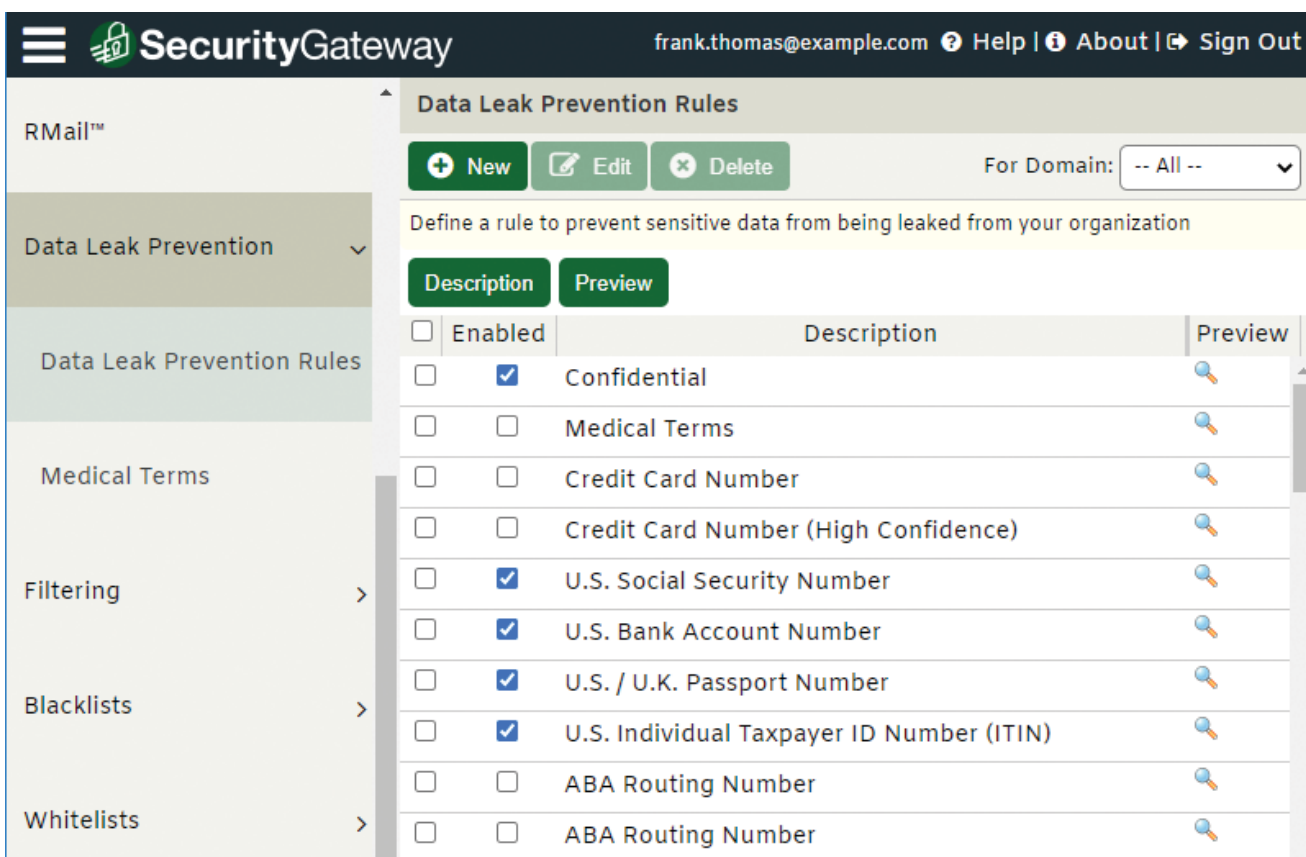
Due to the nature of the cloud, securing this type of deployment platform comes with its own constant challenges.

Cloud apps and accounts are just as susceptible to being compromised – maybe more so. Cloud attacks have steadily increased along with the growth of the remote workforce. Credential theft through password guessing and spraying techniques is a common goal, which makes the organization more susceptible to BEC, social engineering, and similar scams that run inside the organization's network. Criminals can even use their access to internal accounts to encourage the installation of malware.

### Cloud Survival Tips

The truth is that online security threats will get worse as more businesses move their applications to the cloud. Businesses have to secure their cloud accounts through better visibility and detection capabilities to spot, for instance, suspicious logins or email activity, while continuing to adhere to privacy and compliance policies.

MDaemon Technologies' Security Gateway includes more than [60 data leak prevention rules](#) that protect against transmission of a wide variety of sensitive data such as passport numbers, driver's license numbers, bank account numbers, and much more. It also combines many other email security features with archiving and compliance capabilities.



The screenshot displays the SecurityGateway web interface. The top navigation bar includes the MDaemon logo, the text "SecurityGateway", and user information "frank.thomas@example.com" with links for "Help", "About", and "Sign Out". The left sidebar contains a menu with items: "RMail™", "Data Leak Prevention", "Data Leak Prevention Rules", "Medical Terms", "Filtering", "Blacklists", and "Whitelists". The main content area is titled "Data Leak Prevention Rules" and features buttons for "New", "Edit", and "Delete", along with a "For Domain:" dropdown menu set to "-- All --". Below this is a yellow instruction box: "Define a rule to prevent sensitive data from being leaked from your organization". There are "Description" and "Preview" buttons. A table lists various rules with checkboxes for "Enabled" and "Preview" icons.

<input type="checkbox"/>	Enabled	Description	Preview
<input type="checkbox"/>	<input checked="" type="checkbox"/>	Confidential	
<input type="checkbox"/>	<input type="checkbox"/>	Medical Terms	
<input type="checkbox"/>	<input type="checkbox"/>	Credit Card Number	
<input type="checkbox"/>	<input type="checkbox"/>	Credit Card Number (High Confidence)	
<input type="checkbox"/>	<input checked="" type="checkbox"/>	U.S. Social Security Number	
<input type="checkbox"/>	<input checked="" type="checkbox"/>	U.S. Bank Account Number	
<input type="checkbox"/>	<input checked="" type="checkbox"/>	U.S. / U.K. Passport Number	
<input type="checkbox"/>	<input checked="" type="checkbox"/>	U.S. Individual Taxpayer ID Number (ITIN)	
<input type="checkbox"/>	<input type="checkbox"/>	ABA Routing Number	
<input type="checkbox"/>	<input type="checkbox"/>	ABA Routing Number	

## Microsoft Is a Target

The more popular a hosted email provider or other cloud-based service is, the more likely it is to attract hackers. It's no surprise, then, that Microsoft has often been in the news in recent months as the victim of cyberattacks.

In one recent instance, a sophisticated threat actor compromised a Mimecast certificate used to authenticate several of the company's products to Microsoft 365 Exchange Web Services. These products included Internal Email Protect (IEP). This affected approximately [10 percent of Mimecast's customers](#).

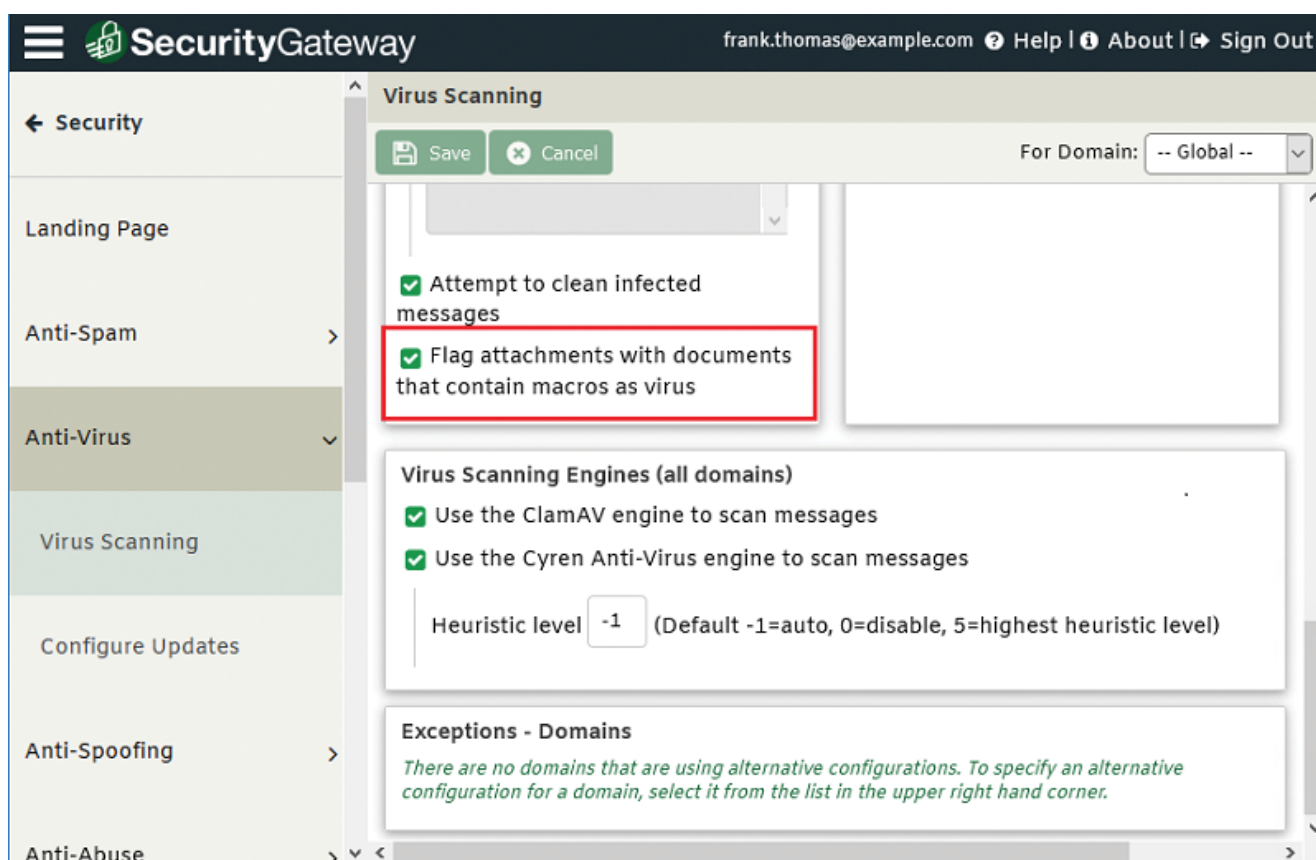
In another instance ripped from the headlines, Russian hackers have collected victim information by compromising the Security Assertion Markup Language (SAML) signing certificate using highly privileged – and hacked -- Microsoft Active Directory domain accounts.

Other security challenges in Microsoft's products include:

- A long-recognized ability for cybercriminals to embed macro-based attacks into Office® documents.
- Exchange Online Protection (EOP), the default security solution in Office 365®, allows users to access their junk email folder and move any message back into their inbox without disabling or warning of any potentially dangerous links or attachments within the message.
- EOP's poor recognition of phishing attempts, including attacks that impersonate other Microsoft products like Office 365, Outlook and SharePoint. In fact, a leading email security vendor has discovered a 16-percent false negative rate in spam and phishing detection within Office 365's native security over testing that included more than 100 million emails.

### Office 365 Survival Tips

Many Office 365 users address these security weaknesses by employing a third-party email security solution. Among its [stronger protections against email-borne threats](#), MDaemon Technologies Security Gateway includes [macro detection](#) and [better identification](#) of phishing attempts.



# The Route to Better Security Today

So far we've looked at many specific attacks and trends that threaten your business today. But what general steps should you be taking to establish better security throughout your network?

And what options are easy to use and cost-effective while still providing administrative control?

## History Lessons

Today's security professionals say their list of top concerns includes phishing attempts, employees' inability to recognize phishing and social engineering attacks, and zero-day exploits. Further, a key takeaway of cybersecurity in 2020 was that prevention efforts are likely to fail at some point; your security systems must be able to successfully identify and disrupt attacks in real time.

The U.S. Cybersecurity & Infrastructure Security Agency's [insights on email and web security](#) include the following at-a-glance recommendations:

- Adopt a minimum DMARC policy of "p=quarantine" or "p=reject". For more information, please see the "Deployment Strategy" section on page 3 of [this guide](#).
- Implement HTTPS with HTTP Strict Transport Security (HSTS) across all external-facing domains, as well as email servers and gateways; it functions similarly to MTA Strict Transport Security (MTA-STS) as explained [here](#).
- Disable weak encryption standards for web and email.
- Maintain ongoing visibility of DMARC findings and reports to ensure anti-spoofing measures (SPF & DKIM) have been properly deployed to protect your domain.

As referenced earlier, there are three parts to better email security: Developing an informed and vigilant workforce, building and reinforcing the best possible protections, and using an active security solution that monitors your organization's email in real time. Let's take a closer look at these.

## Improving User Training

Considering that 38% of users fail phishing tests, it's no surprise that, among security teams:

- 74% are at least somewhat concerned about phishing attempts making their way to end users.
- 72% are at least somewhat concerned about employees failing to spot phishing and social engineering attacks.
- 51% are at least somewhat concerned about CEO fraud/business email compromise attempts making their way to end users.

The solution to this problem is both obvious and incredibly meticulous: Train your employees and test them through simulated email attacks; then retrain them and test them again on a quarterly cycle. They must understand how to identify phishing attempts and be hyper-aware of the basic rules of email safety, such as never opening an email attachment from someone they don't know and always double-checking credentials before engaging with suspicious messages.

**DHL -AWB Shipment Has Arrived**

from: **DHL Customer Support** <dhl@lupendis.com>  
 date: 09/25/2020 10:58 AM  
 to: **Recipients** <dhl@lupendis.com>

Not a DHL Domain (MDaemon Webmail displays the actual sender in brackets to help users identify spoofing)

Generic "To" Header

**REMINDER!!!** — False Urgency

Dear Customer, — Generic Greeting

We attempted to deliver your item at 2:30pm on 24th May, 2019. (Read enclosed file details)  
 The delivery attempt failed because you were not present at the shipping address, so this notification has been automatically sent.

If the parcel is not scheduled for re-delivery or picked up within 72 hours, it will be returned to the sender

Label Number: (Read enclosed file details)  
 Class Package Services  
 Service(s): (Read enclosed file details)  
 Status: e-Notification sent

Attempt to Convince Recipient to Open Attachment

Read the enclosed file for details.

DHL Customer Service.  
 2019 DHL International GmbH All rights reserved.

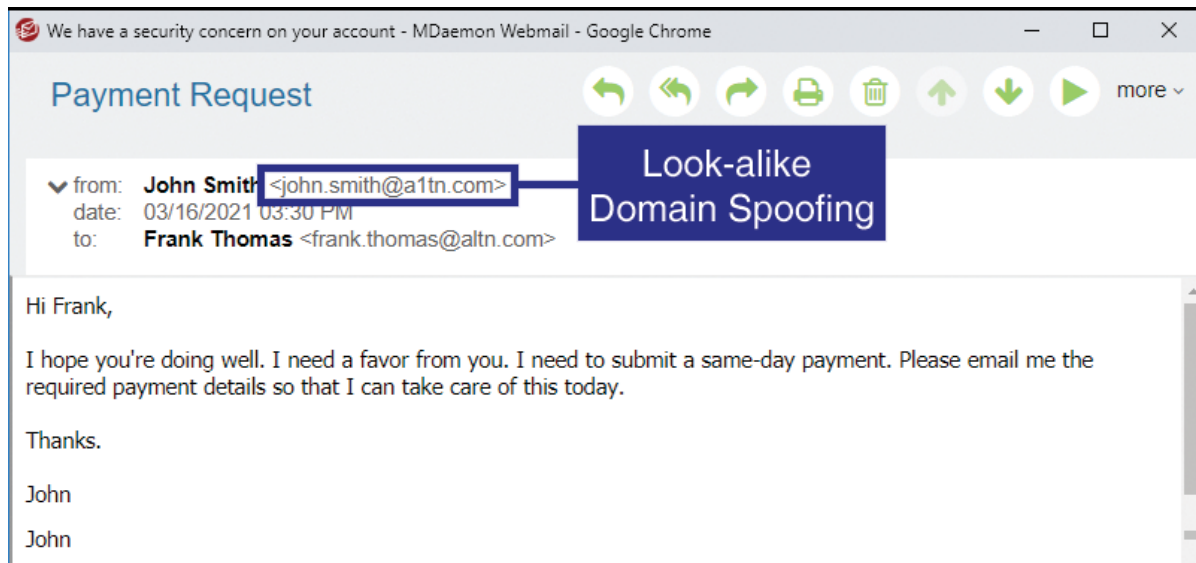
### Administrator Recommendations

There are also plenty of steps email administrators can take to erect layers of protection within your email system:

- Review Active Directory sign-in logs and unified audit logs for anomalous activity.
- Enforce multifactor authentication to drastically reduce data theft.
- Review user-created email forwarding rules and alerts or restrict forwarding.
- Determine when, how and why to reset passwords and to revoke session tokens.
- Resolve client site requests internal to the network.
- Consider restricting users from forwarding emails to accounts outside of the organization's domain.
- Use tools such as firewalls and threat monitoring to block attacks on your infrastructure.
- Implement a layered approach to [email security](#), along with [email encryption](#) for safely sending emails and attachments.

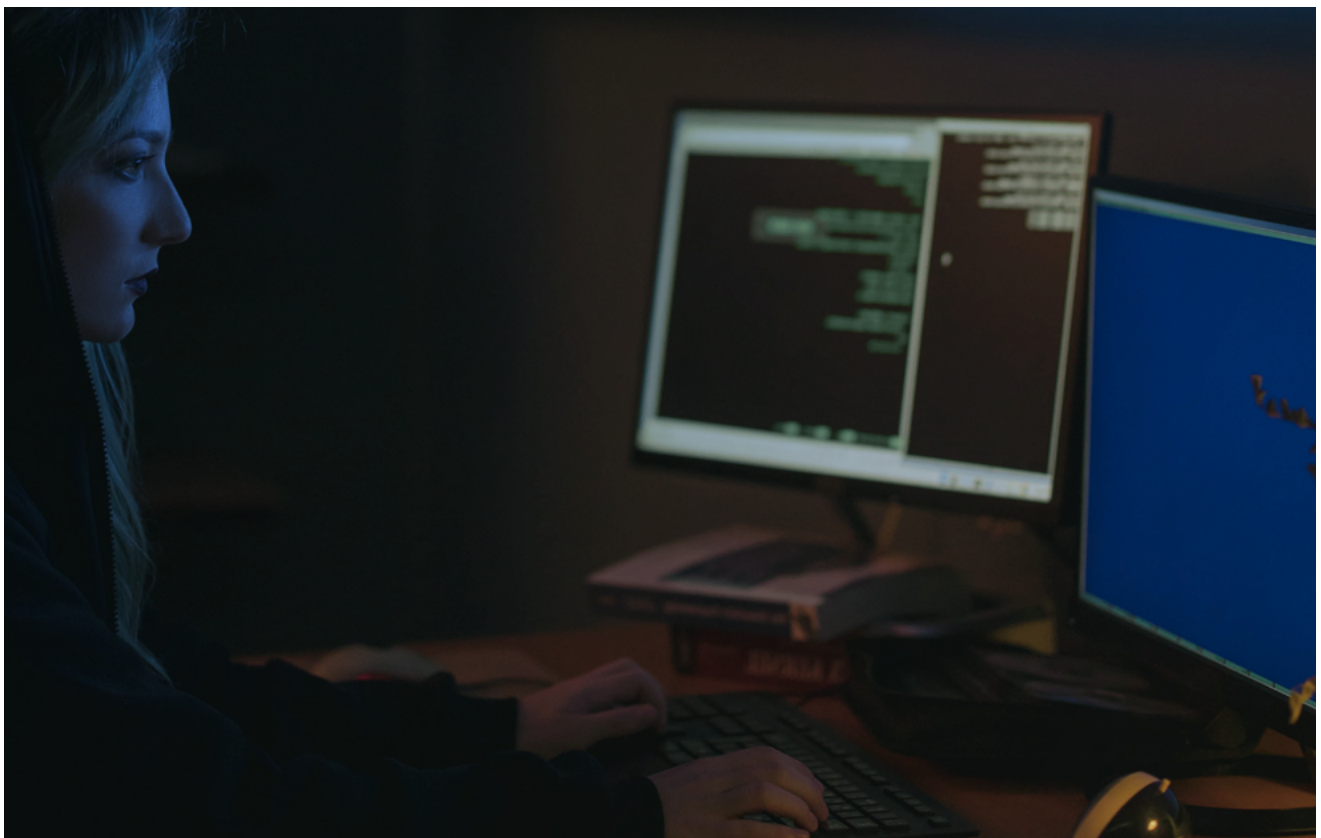
## Blocking Dangerous Email

As we've noted above, "spoofed" threats are becoming ever more dangerous. Your email security solution must be sensitive to these threats while also recognizing near-match spoofing of domain names and other fraud attempts.



## Establishing Zero Trust

So how can employees verify internal requests for information, or how can administrators know web addresses included in emails or visited on remote devices are secure? The emerging answer is zero trust access, based on the idea of "never trust; always verify." The goal is to reduce risk by allowing administrators to control what communications are permitted between different access points on the network. This prevents attackers from entering the infrastructure and acting laterally, whether they came in from the cloud, an on-premises device, or a mix of both.



# Step Up the Security of Your Organization's Email and Keep Cybercriminals Out

Think your business doesn't need to worry about cybersecurity just yet? It's time to think again. Recent surveys have found that:

- While only 7% of respondents believe that account takeovers are a key risk for their organization, in reality, account takeover activity is implicated in 42% of security risks.
- 33% of organizations have been impacted by account takeover threats during the past 12 months.

Strong email security isn't just for the largest corporations. Since 1996, MDAemon Technologies has developed email and email security software for the global small and medium enterprise business market. Our flagship products, MDAemon Email Server and Security Gateway for Email, can be deployed in virtual, hosted cloud or private on-premise environments. Our solutions require minimal support and administration to operate and maintain – and our clients are very satisfied with their savings over other well-known solutions.

One of the best practices you can implement in 2021 is adding MDAemon Technologies to your email security processes. Want to learn more about how **MDaemon Technologies' Security Gateway for Email** can help protect your employees? [Visit us](#) to learn about our hosted or on-premise email protection across your entire organization.



[SecurityGatewayForEmail.com](https://www.SecurityGatewayForEmail.com)

2021 © Mdaemon Technologies. All rights reserved.