



Vircom

Simplifying Security

Keeping Your Business Email
Safe with modusCloud



Table of Contents

What are the biggest threats to growing businesses?	3
How do attackers choose their targets?	7
Advanced Threat Protection and Benchmarking Growing Threats	10
Simplifying Security for the Long Term	13
About Vircom and modusCloud	17



What are the biggest threats to growing businesses?



There is no hiding from **1 Credential Phishing**, **2 Business Email Compromise** & **3 Ransomware**

The pace of change in today's market is breathtaking. Businesses are expanding, leaders are investing in people, processes and new ventures, and customers are always on the hunt for new products that give them an edge. In this burgeoning "4th Industrial Revolution", it is harder than ever to spot security threats and fraud – dangers we often don't notice until it's too late. For most IT leaders, while you may make ample investments in infrastructure and innovative tools, most networks and systems have fundamental flaws and loopholes inherent to how they work. These are what fraudsters and cyber criminals ultimately look to exploit.

While one may think that each systemic problem has a systemic solution, there's one vulnerability which most security systems can't account for: people. Your people, much as you love them, are busy, hardworking, mean well, and they can also (unfortunately) be easily influenced, targeted or manipulated by a frighteningly large number of bad actors with a malicious agenda. With LinkedIn, list services and the large mass of information available to anybody who goes digging, it's easier than ever for scammers and attackers to target people and groups within your company – no matter its size – than ever before.

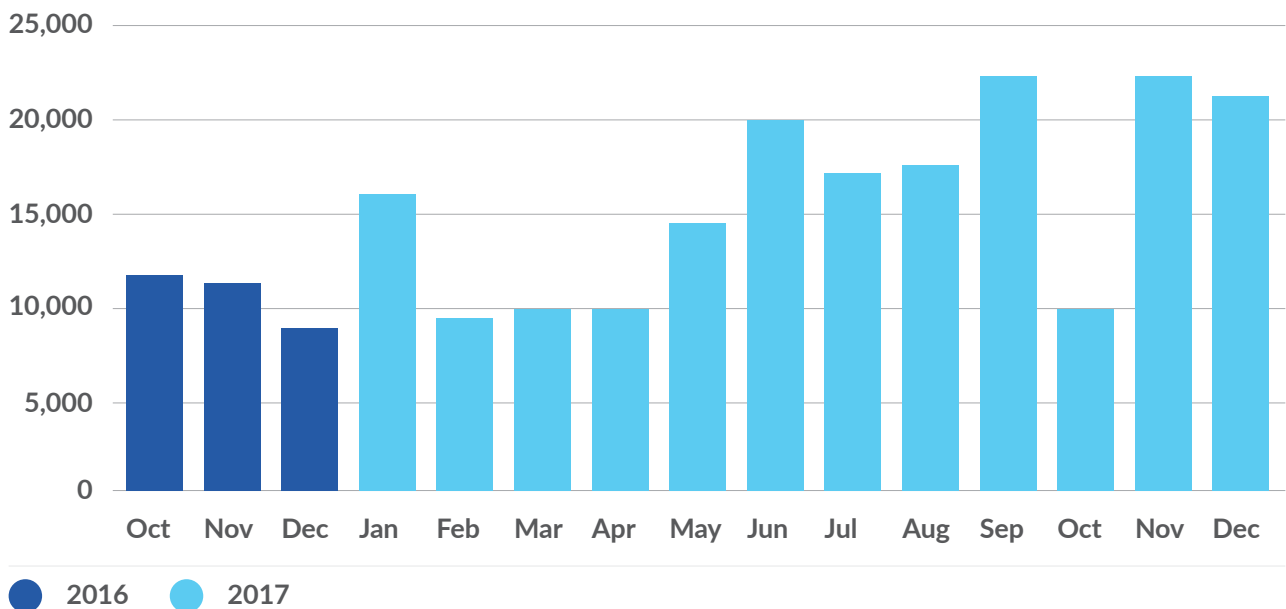


Human error and the risks it poses has led to the proliferation of three specific threats that put your company at significant risk, and they all arrive through email: 1) Credential Phishing, 2) Business Email Compromise (BEC) and 3) Ransomware.

1 In the first case, Credential Phishing is the sending of seemingly authentic support and password reset emails to unsuspecting users. This typically applies to personal accounts like iCloud and Gmail addresses, but, more and more, credential phishing is being used to target Office 365 users and get credentials for other business applications in order to compromise accounts, gather data or (in extreme cases) change wiring instructions to divert funds to accounts controlled by fraud artists.

2 In the second case, Business Email Compromise is a sophisticated form of email fraud which involves a variety of means used primarily to divert funds. These include targeting high-authority users with requests for funds while masquerading as a foreign vendor or a user with higher authority than them, who is somehow inaccessible to execute on an urgent need (e.g. while flying between locations). Attackers can also execute BEC attacks through accounts compromised by credential phishing, impersonate attorneys or parties in large financial and real estate transactions, and also send unassuming emails that attempt to steal data, employee W-2s or other sensitive information. Some predictions have Business Email Compromise costing businesses more than \$9 Billion dollars in 2018 alone, with the average attack historically costing more than \$60,000.

Business Email Compromise attacks detected and blocked by modusCloud Threat Intelligence
 Q3 and Q4 2017 represented two of the three biggest quarters for volume of email fraud ever seen.



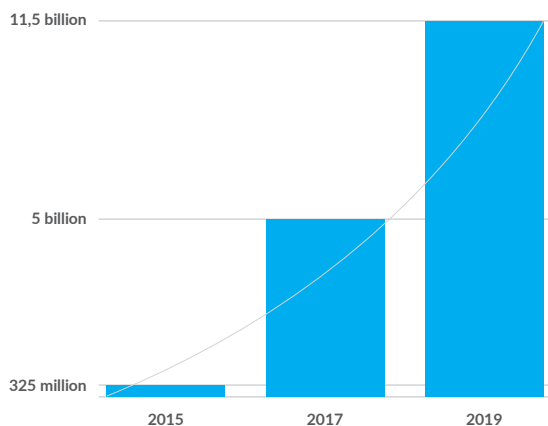
<https://www.proofpoint.com/sites/default/files/pfpt-us-tr-email-fraud-yir-180212.pdf>

<https://www.vircom.com/blog/business-email-compromise-2017/>



3 In the third case, Ransomware has been understood as a growing risk for businesses of all sizes, costing hundreds of millions and more to companies like Mondelez, Maersk and others. Ransomware is malicious software that, once downloaded or installed on a device, locks out access to a computer until a ransom is paid (typically in cryptocurrency). The FBI, as well as many other experts and organizations, generally recommend not paying ransoms, whether because there is not guarantee your data will be unlocked or that it encourages criminal behavior or, as is often the case, ransomware will simply delete data in order to lock it out – meaning there’s no data to recover. Overall, the biggest cost is usually not the ransom, but the damage caused to the data integrity and IT systems of its victims.

Cost of Ransomware Growing Exponentially



Ransomware is hard for employees to detect and, when delivered through malicious links disguised in emails, it can become a threat few businesses are prepared for. Out of curiosity or simple inattention, users often click links without examining them – a trend which has made ransomware delivered through malicious links in email a profoundly dangerous threat. Ransomware’s costs are expected to exceed \$11.5 Billion annually by 2019, when they cost businesses only \$325 million in the whole of 2015.

<https://cybersecurityventures.com/ransomware-damage-report-2017-part-2/>

Why are these three vectors so effective?

Because they are all complementary, they all take advantage of human nature and they all make a LOT of money.

These vectors of attack are so effective not only because they are often crafty, but because they are aimed at taking advantage of a user’s good intentions. When presented with unseemly options in face-to-face interactions, most people use non-verbal communication like body language, tone of voice and other things to discern untrustworthy or malevolent intentions. Through email, there are not only fewer cues to go on (and more common traits to make emails seem “official” and thus authentic), but also no perfect authentication mechanism to know that the person who messages you is who they claim to be.

This is even more risky when considering that practices like the reliance on Multi-Factor Authentication may be providing a fall sense of security. For instance, many BEC attackers are now following up emails with phone calls. This is because they know accounting employees are more likely to call vendors or superiors to validate transactions, so in order to prevent their attacks from being found out they try to head off any risk of being found out by a phone call – affirming the legitimacy of the transaction.



“9%: *Of all simulated phishing emails, nearly one in ten were clicked”.*

<https://www.tripwire.com/state-of-security/security-data-protection/three-quarters-organizations-experienced-phishing-attacks-2017-report-uncovers/>

Furthermore, while a fraud involving state actors, malicious stock trading practices or corporate espionage may provide a strong incentive for phishing, the opportunities to execute these attacks on a large scale are relatively limited and exclusive. In general, fraud is the most profitable way to continually commit a crime and benefit from it (until the perpetrator gets caught, of course). Many email fraudsters are often located outside of the country their target is located in, meaning it is hard for local or even state and federal authorities to rein them in. If government is unable to protect businesses from international criminal attack, the onus is on businesses to provide for their own defense if they want to avoid the consequences of email attacks.

How much
are attackers
distributing,
and how
rapidly are they
growing?

As mentioned previously, the costs of ransomware will likely have multiplied by more than 35 times between 2015 and 2019. A similarly marked increase has occurred in BEC, which cost businesses \$740 million in late 2013, meaning that 2018's \$9 Billion cost figure represents a 12x increase in five years. Phishing has reached all time highs, with nearly 250 million phishing attempts taking place in 2017. There is no sign of any of these vectors slowing down. Considering the costs of an attack on the victim, every IT department needs to find the resources necessary to protect their users.

<https://securityintelligence.com/news/nearly-250-million-phishing-attempts-in-2017-study-shows/>

<https://www.fbi.gov/news/stories/business-e-mail-compromise>



How do attackers choose their targets?



Attackers choose their targets based on primary characteristics **like budget authority, access to information or systems, proximity to management.**

If you were an email scammer, who would you target?

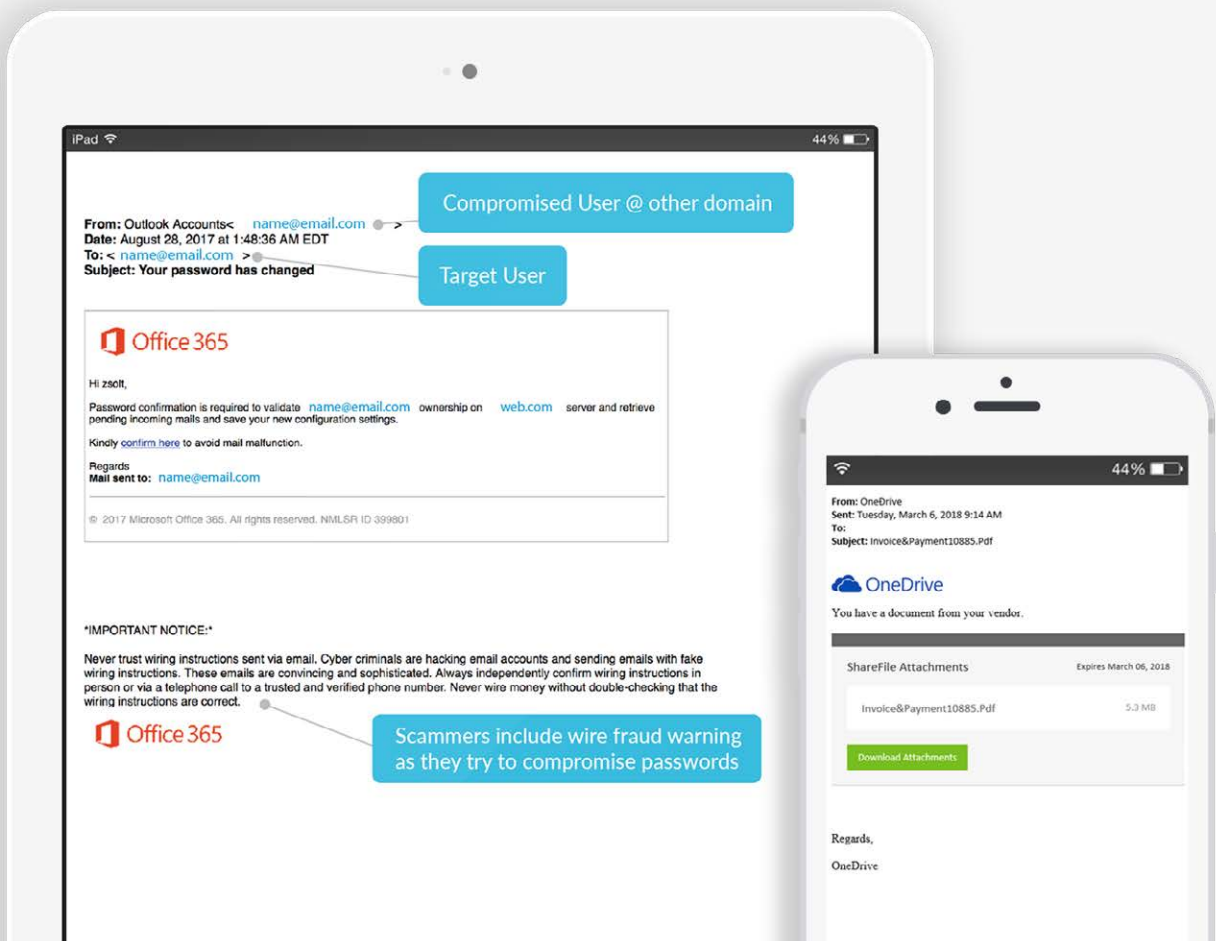
Think of it this way – almost like a hustler on a riverboat gambling trip – you would want a target that gives you a few things: 1) an easy, discreet method of approach, 2) a high-roller who isn't too loud (meaning someone with a lot of money who doesn't draw a lot of attention) and 3) a quick avenue of escape, so that by the time somebody knows they've been ripped off, you're already gone.

Not that you would think like that, but these are the techniques and tactics the fraudsters look for. This applies almost everywhere, whether it's in a casino, a riverboat or through email. In all cases, these kinds of malicious, manipulative actors are looking for a target that meets their criteria. They are looking for a system or set of tactics that applies well to this target, which displays an inherent weakness or otherwise lacks the defense to thwart an attack like what they may be planning.



As it turns out, if you're looking for 1) discreet methods of approach, 2) high-value targets who are rarely boisterous and 3) quick getaways, going through email could be considered one of the best ways to achieve that. That's why attackers will target high-level and C-suite employees, impersonate those employees and even external vendors (through simple tricks with email headers and more) to send data requests, wire transfer requests and other valuable transactions to any employee with the authority to give them what they're looking for.

Play **"Spot the Phish"**! Ok, maybe you already have the answers, and we had to cover up domains for privacy, but these are real examples of the most basic attacks your employees might face – and what gets through most security filters (like those offered with Office 365).





The tactics that these attackers use, time and time again, involve using compromised accounts to phish for the credentials of accounts they want to gain access to. They often target high-authority individuals with requests that often require little attention relative to the work they have to do. They impersonate high-authority individuals by modifying email headers and reply-to's, while also distributing malicious content through links and attachments – whether ransomware, spyware, other forms of malware. The attachment may even be something as benign as a forged invoice. This is the bread and butter of a scammer, and it's no wonder why their business has been so good of late – especially considering that a majority of businesses have little protection against any of these approaches.

Ultimately, for phishing, grooming and gaining access, every user can become an entry point for attackers to learn more and find vulnerabilities within an organization.

The more sophisticated scams get, the more legitimate they need to appear – that means more niche targets, better grooming and bigger end goals – whether it's the pursuit of information for the ends of espionage, multi-million-dollar payoffs, or social “hacktivism” that is intent on exposing trade secrets in the name of the public interest.

What's worse is that attackers are continually realizing the value present in targeting smaller businesses, mainly because they have less protection, fewer organizational hoops to jump through, and there are, simply put, many more of them, making it easier to develop a repeatable and profitable fraud scheme over time. Worse yet, many don't devote the resources necessary to protect against attacks until it's too late.



Advanced Threat Protection & Benchmarking Growing Threats.



Advanced Threat protection, where it's from and what it does, and how to protect against Credential Phishing, Ransomware and BEC.

While fraud is a growing threat, it doesn't need to keep businesses up at night. There are solutions that are purpose-built to protect against the tactics that email fraudsters love to use against businesses small and large alike. It ultimately comes down to four main problems, each with their own solution: Imposter attacks, Phishing attempts, Malicious Attachments and Malicious URLs.

In each of these cases, tactics can be detected and countered by an email gateway using Advanced Threat Protection features. To summarize:



Imposter Protection: The most common tactic in BEC attacks, imposter emails are used to impersonate high-authority users within a company, or important partners, attorneys and external vendors. Typically done by masking or impersonating who an email is from, or simply copying display names and sneaking in a different reply-to address that leads to a continued conversation under false pretenses. Imposter Protection protects against these tactics and by filtering inconsistent or inauthentic structures out at the gateway level.



Phishing Protection: Phishing messages have common markers that make them effective – whether it's using lookalike domains or imitating the support messages and password reset emails that come from major email and cloud application platforms. Phishing protection uses fuzzy matching, along with other techniques, to identify whether an email that could seem legitimate at a glance is actually phishing for credentials or attempting to compromise accounts.



Attachment Defense: Malicious attachments come in a variety of forms, as anything from easily identifiable virus executables to Ransomware to unique threats with varied signatures to fake invoices that may have been drafted by real legal and accounting professionals are all used by attackers. Based on a unique scoring system, Attachment Defense protects against content threat might pass through as legitimate invoices and more, leveraging cloud visibility to stop threats and stymie trends as they emerge.



URL Defense: Businesses don't just need filtering and protection against malicious URLs at their email gateway, but perpetual protection no matter when that URL might turn malicious. Rewriting URLs at the gateway is one way to do this, essentially routing the email through a time-of-click scan that keeps your users from falling victim to hosted malware or malicious content - even if it is uploaded after they first receive a link.

Why mixed tactics are more likely to come from attackers.

This is the general matrix of practices that fraudsters are using today in order to “put daylight” between users and safe email, along with what can protect against them. Without complete protection from all the common points of vulnerability within your email (and accounting for the latest tactics through both machine-learning updates and up-to-the-minute cloud protection), attackers will be incentivized to layer and mix strategies in order to take advantage of human nature.

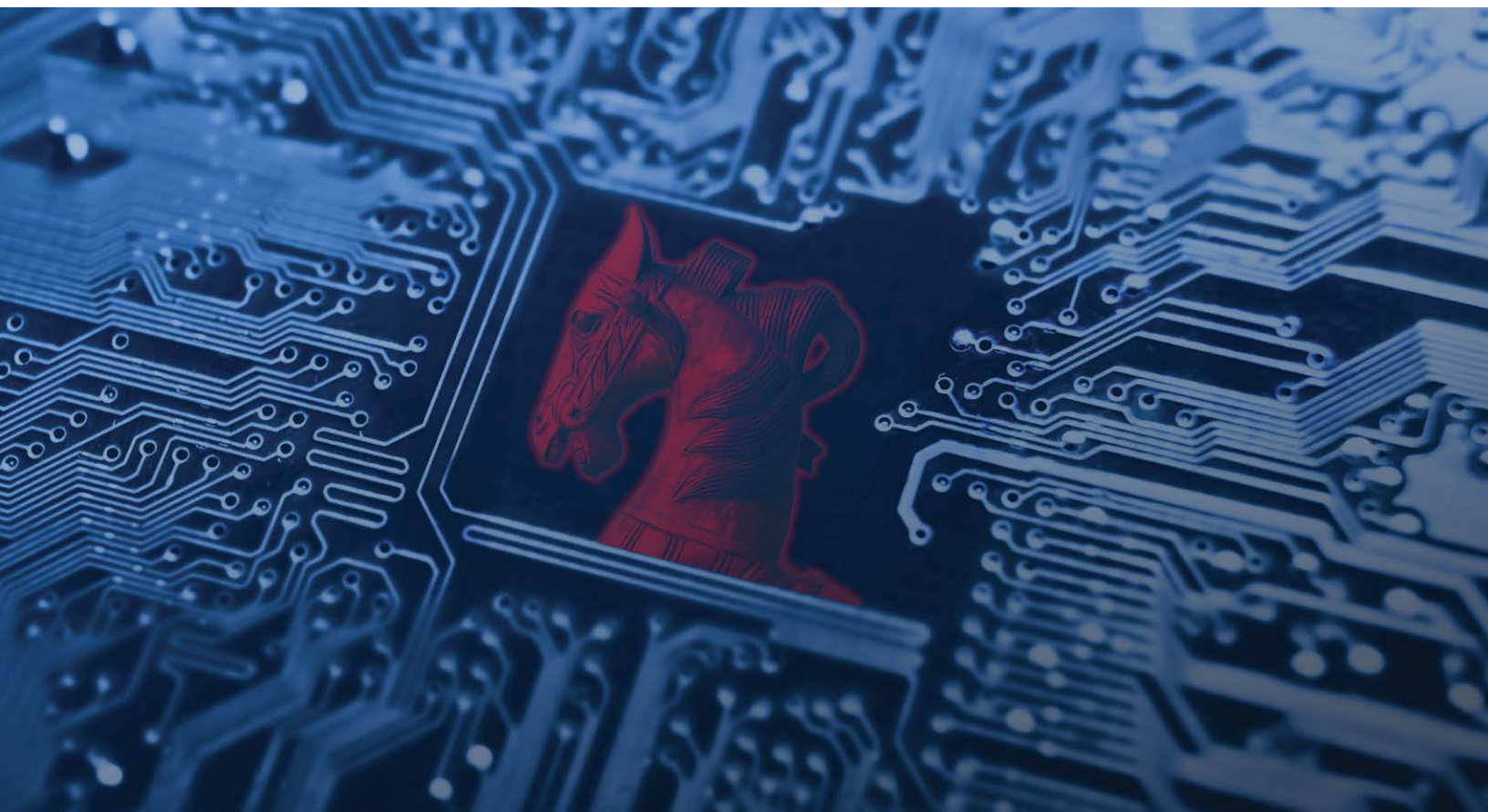
For instance, protection against viruses in attachments is essential to safe email, but what if attackers use automated processes to change virus signatures between each individual send? Or what if they send a malicious attachment containing a link to hosted malware, or simply a fake invoice without any “programmatic” malicious content? There are a variety of possible tactics that can be used together to defraud your organization, so using protection that stops all manner and iteration of attacks gives you the best chance to anticipate what attackers may attempt.



How attackers vary their strategies, between months or even years, to take advantage of gaps in protection.

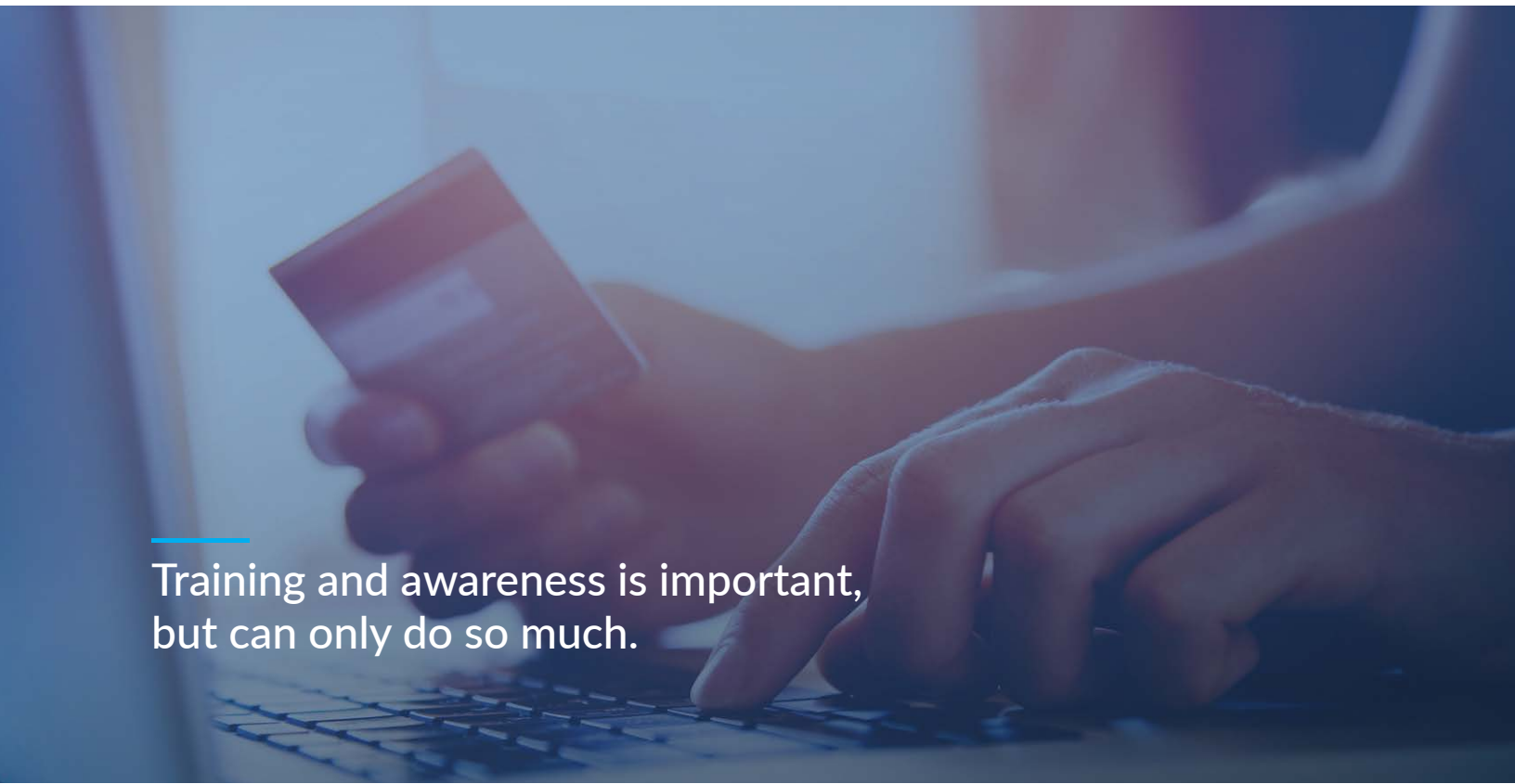
Very often, the prevalence of attacks and the variety of strategies used will fluctuate. For instance, over the course of 2016, malicious link attacks grew significantly, but 2017 seemed to be the year of ransomware – except for the fact that between Q3 2016 and Q3 2017, malicious links directing to hosted malware (mostly ransomware) grew by 2200%. What is to stop attackers from targeting high-level employees – or any employee for that matter – with an imposter attack holding a malicious link that installed hosted malware, which could be directed at anything from locking out a computer, to exposing sensitive data, to targeting other devices on a network like industrial control systems?

At the same time, Malicious Attachments with no visible malicious content could be sent in waves, only to hold links directed to the same hosted malware that has given so many companies trouble. The mix of the variety of email tactics used by advanced threat actors, from imposter emails, phishing attempts, and malicious attachments and URLs, give a variety of iterated opportunities to gain access, compromise accounts and even divert funds. A solution that doesn't account for these or is otherwise incomplete is one that only leaves a matter of time before attackers uncover a real vulnerability and find the best way to profit from exploiting it.





Simplifying Security for the Long Term.



Training and awareness is important, but can only do so much.

With Advanced Threat Protection you can significantly reduce the risk to your users being exposed to risks. The last mile requires basic training and awareness to complement your software and tech-side solutions. You can't build every member of your team into a cybersecurity expert, but you can take fundamental steps to improve internal awareness of cybersecurity risks in the long term. These include a variety of the following issues, including:



Password Practices: Along with never giving out passwords, employees need to ensure that their devices and accounts are all protected by sufficiently strong and yet still memorable phrases that use nuances of both letters and numbers, capitalization and symbols while being based on memorable or personally relevant phrases. If you prefer not to use this technique, then using a password generation and storage tool is highly recommended.



Installing Software: Employees need to know that software installations need to be validated by IT, while some companies enforce specific policies that require sufficient permissions for any device to have software installed, updates also need to be initiated regularly to ensure that security vulnerabilities are always patched before they can be taken advantage of.



Being Able to Identify Malicious Content: When an unexpected and malicious email, attachment or executable ends up in a user's hands, it's important that they don't click out of curiosity, but think twice and ask whoever gave it to them directly (whether over the phone or in person) what the relevance and purpose of the content is. If that person hasn't heard of it, it's probably malicious. (A good email gateway should filter out emails with executable files.)



Using Public Wifi: While this is a trend for mobile and remote workers, public wifi should be avoided at all costs (and where it must be used, a VPN should be employed). Users should additionally avoid entering any passwords, particular those to websites that hold or manage financial information wherever public wifi is involved. Furthermore, at hotels, convention centers and other common sites for doing business, "imposter networks" can be present that appear to be legitimate wifi, but are actually operated by malicious actors that are attempting to observe activity and steal information.



Multi-Factor Authentication: As with learning to think twice about malicious content, employees should always double-check with their colleagues whenever they are presented with an unexpected, odd or rushed transaction – even if it's of basic information. There are endless avenues of attack that fraudsters use, not necessarily to steal funds or data, but to work up to attacks that have a major payoff, either by getting essential information that helps them piece their scam together or by grooming individual employees as targets for large future attacks.

In the matrix of all these simple habits that can help you keep your team safe, you still need to deploy purpose-built solutions for anti-virus protection, network security and – of course – email filtering that keeps your users safe.

An iterated solution responds to threats as they emerge, protecting against advanced threats while accounting for human error.

modusCloud is a powerful, machine-learning driven email security gateway that fulfills the requirements you need to meet and protect against the sorts of attacks and risks discussed in this paper. With powerful spam and content filtering, Advanced Threat Protection, Email Continuity, Email Encryption and Email Archiving, you can fulfill all the needs your organization has in preventing and managing malicious email threats, even as their perpetrators work harder and harder to target your users.



At its core, modusCloud offers powerful email filtering against spam, phishing, viruses, bulk mail, gray mail, along with protection against imposter attacks, targeted phishing and malicious attachments and URLs. modusCloud's Imposter Protection, Phishing Protection, Attachment Defense and URL Defense all fulfill the key requirements that growing businesses need to protect against threats as they emerge.

Using Continuity, Encryption and Archiving to close your gaps.

Filtering and protection isn't the only thing that can be done at the gateway level, and by adding more value at the gateway, you can create a broader reach of security, continuity and compliance for your organization



Email Continuity: modusCloud displays all spooled mail in the Emergency Inbox through a web-based user interface. 30-day spooling provides always-on SMTP deferral, failover & queue protection, thus allowing users to read, reply to and send new emails via the Emergency Inbox. This instantly deploys as soon as a spooling threshold is surpassed, meaning your organization can still use email even when a primary server or cloud service is down. When delivery is restored, email will automatically flow to the downstream mail server along with any replies and new emails that have been sent while delivery was unavailable.



Email Encryption: By allowing employees to send encrypted messages within and without your organizations, all made accessible through a secure hosted portal, stakeholders within your organizations can share sensitive information securely across public networks and through their mobile devices. Using this sort of technology removes your employees from the path of various malicious actors, making secure email simple as ever.



Email Archiving: Archiving on modusCloud also offers your organization an unlimited storage volume for 10 years at a fixed cost per user, featuring company-wide search, individual user search and a user-friendly web interface. Built for Microsoft Exchange, Office 365 and more, modusCloud Archiving ensures compliance and retrievability for legal, financial and other businesses while also allowing any company to fully own and understand their email data. With 55% of organizations being ordered to produce email by court and regulatory bodies, archiving can be a critical functionality that prevents both lost time and resources. As a failsafe, an archive ensures you can get up and running quickly in the event of an attack.



modusCloud is a powerful solution that assures compliance and keeps your organization running smoothly at all times, while limiting the possibility for compromise of both accounts and sensitive information. The services you provide to your organization are no longer simply a “cost of doing business”, but play a proactive role in the function, protection and improved efficiency of all your colleagues around you.

Registering to a service with great support gives you peace of mind.

modusCloud was developed to be powerful technology, but always with the realities of the IT world in mind. Our support team is also staffed with IT experts, who are always focused on finding you solution to problems as soon as you call.

The fact is, Vircom has been in the business of email and security for more than 20 years because of the compelling support experience it provides. Many customers have chosen us over other providers on the basis of our quality onboarding along with ongoing efforts to go above and beyond the call of duty – that means that even as you get a demo or start a trial, you’ll begin to see where Vircom offers you a service advantage that other vendors simply can’t match. We combine a high-quality product, informed staff and swift responsiveness to ensure that you get the most value possible out of our security offering, without wasting time dealing with inexperienced support technicians or losing productivity due to an inferior filtering product. With Vircom, you’ll have found attentive security expertise that actually listens, and that you can actually trust.

Learn more about email threats

The Rise of URL Defense

Cyber Criminals: Who They Are and Why They Do It

How Bad Was Business Email Compromise in 2017?

Cloud Email Archiving Solutions Explained: What You Need To Know

Why is Targeted Phishing Hammering the Real Estate Market?

Setting Up A Cyber and Email Security Awareness and Training Program

Cyber Security Training Practices for Everyday Business Safety

moduscloud Your Complete Cloud Email Security Solution

How to create a strong password in 3 easy steps



About Vircom and modusCloud

With more than 2 decades of award-winning experience, Vircom has always been at the cutting edge of developments in email and securing your business's communications. With modusCloud, Vircom offers powerful, AI-driven filtering with Advanced Threat Protection, Email Continuity, Email Encryption and Email Archiving, along with the great customer service and partner benefits that those who know us have always loved. A free 30-day trial on all offers means you're able to discover all the benefits Vircom gives you, from easy management and implementation to powerful protection and services that keep your business running smoothly, no matter the threats that are out there.

Contact Vircom for a technical demo

Get a live look at what attackers are doing, the heights they've scaled and how you can stop them with modusCloud.



Toll Free: 1.888.484.7266



Local: 1.514.845.1666



info@vircom.com



Vircom