AREA 1

WHEN THE CLOUD RAINS PHISH

Understanding Office 365 and Gmail Security Threats

AREA 1

PHISHING– THE ULTIMATE "GOTCHA"

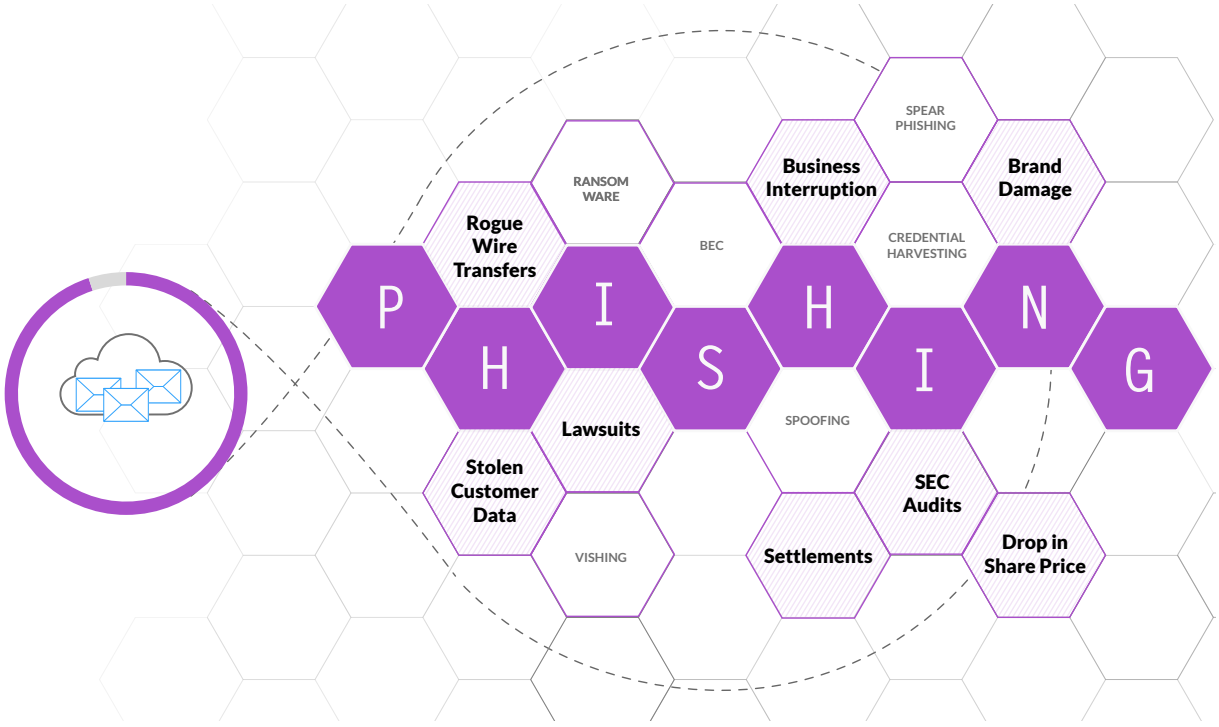
You've been phished! That sinking feeling in your gut comes from the realization that a cyberattack has breached your email security defenses. Even Office 365 and Gmail's world-class defenses aren't complete enough to protect against all modern phishing threats. Your organization's funds – and perhaps fate – could be at the mercy of some malicious fraudster or shadowy nation-state organization.

PHISH NEVER SLEEP

Our inboxes (which have increasingly transitioned to the cloud) are prime phishing targets, and hackers remain persistent in varying their attacks. Hackers have even cleverly adapted their methods to the cloud itself. For example, bad actors have used Microsoft's Azure cloud storage solutions to host their phishing landing pages, ultimately tricking some targets into thinking they're seeing an official Microsoft login page. And recently, Google had to fix a flaw that allowed malicious individuals to send unsolicited Calendar invites to Gmail users (since the invites can include URLs, attackers used Calendar as a Trojan Horse to get individuals onto a phishing website).

Even for organizations that have transitioned to the cloud, email is still the ideal vector for threat actors to warp protocols and technology to deliver spoofs, BEC, spear-phishing, whaling, ransomware, credential harvesting, watering hole attacks and more. The means, tactics and intent may differ, but these diverse attacks have a single commonality: they are all variants of phishing.

Here are some types of phishing campaigns commonly used by threat actors -- and a discussion of what's needed to defend you from this diversity of attacks.



PHISHING HANDBOOK: HEADACHES AND REMEDIES

SOCIAL ENGINEERING SHARPENS THE SPEAR

Landing easily in the inbox, spear phishing attacks use social engineering to create trust and therefore, not surprisingly, have a high success rate in compromising systems and causing data and financial breaches. Because these phishing attacks are targeted, low in volume, and don't fit the conventional spam profile, they are often invisible to traditional security technologies – including Office 365 and Gmail spam filters – which rely on threat intelligence derived from active, high-volume campaigns.

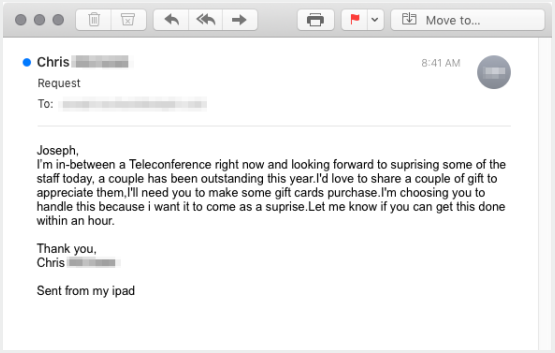
Effectively defending against spear phishing depends on early insight into phishing campaign infrastructure before an attack is launched, goes active, and does its damage. Setting up a phishing campaign infrastructure may take hackers months, although they then often launch the attack and take down the site within hours. Thus, a technology that proactively hunts for phishing campaigns and infrastructure – while under construction – has the critical early visibility needed to detect an attack and prevent a spear phishing email from landing in user inboxes.

> *"66% of IT professionals say security is their greatest concern in adopting an enterprise cloud computing strategy."*
>
> – Forbes.com

BEC ELUDES CLOUD DEFENSES AND EMPLOYEE TRAINING

BEC attacks rely on impersonation to trick victims into providing confidential information or transferring funds. A fake "CEO" request can damage a company more severely than a sophisticated technological attack. Outrageous BEC succeeds because fraudsters research and study the target company meticulously to gain deep knowledge and familiarity. Spoofing makes an email seem to come from a trusted organization, executive or supplier. File-less, link-less and easily validated by Office 365 and Gmail email authentication checks, BEC is positioned for jaw-dropping success.

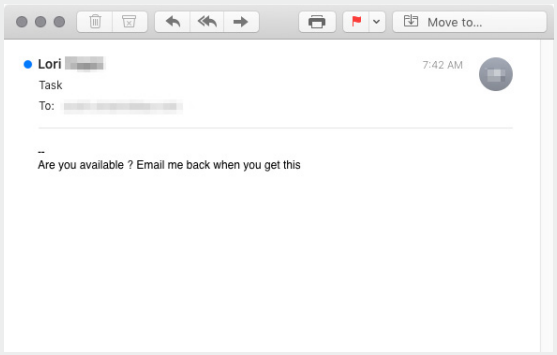
BEC example:



- Message to employee from impersonated CEO (using an AOL address)
- No technical call to actions (i.e., links or attachments)
- Message defeats SPF, DKIM, and DMARC because it came from an AOL account
- Delivered by O365

AREA 1

BEC example:



- Originated from Gmail (sender domain registered through Google Domains)
- No technical call to actions (i.e., links or attachments)
- Sender domain has MX records pointing back to Google
- Message passed all authentication mechanisms (no DMARC records published)

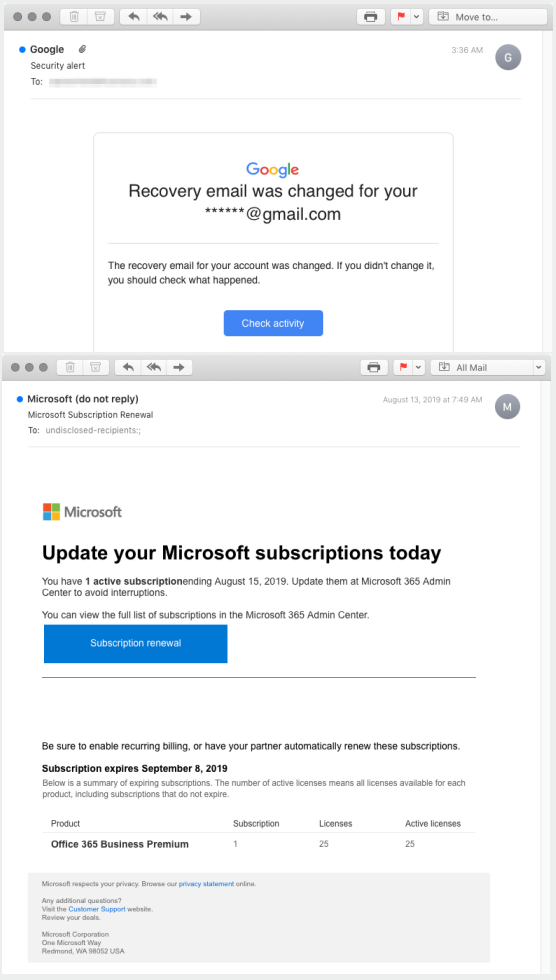
Protecting against these attacks requires advanced email analysis techniques that can look at the source and the sentiment of an email to detect BEC phish. Sophisticated matching models are needed to check that messages appearing to be from an executive or partner actually originate from known sending domains. In combination with language analysis of email subject and content, an effective defense must understand the message sentiment itself to detect BEC phish and prevent delivery of imposter email to employee inboxes. Only a technology defense using advanced email analysis and sender validation can expose the context and true sending domains of a BEC phish.

Preventing delivery in the first place saves an employee from being tested – and perhaps bested – by a crafty crook.

CREDENTIAL HARVESTERS MAKE A REASONABLE REQUEST

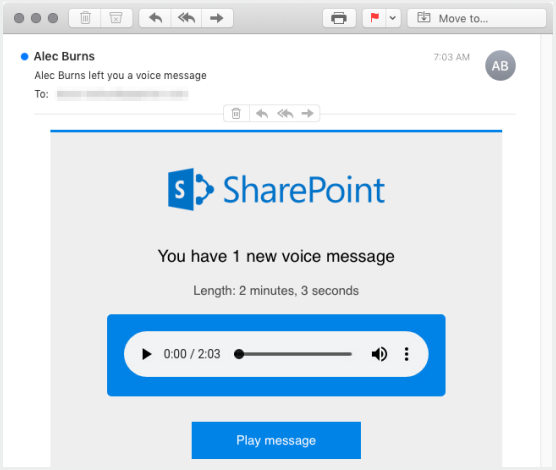
What could be more innocuous than merely logging into your own account? Stealing legitimate user IDs and passwords, credential-harvesting attacks often start with targeted phishing emails that request the victim to click on a link and log into their own account to change password or payment information. It sounds reasonable. But the link then directs the user instead to a spoofed site, allowing the hacker to harvest the valid credentials just entered by the victim. The hacker can then use those credentials to log into the victim's actual account.

Gmail and Microsoft credential harvester examples:



Another similar credential harvesting attack is a voicemail phish. It begins with an email informing the recipient of a missed call and voicemail. The message contains a link from the attacker to an authentic-looking site, prompting the recipient to enter his or her credentials.

Missed voicemail phish example:



Cybercriminals often launch phishing sites for a limited time only, taking them down quickly before threat researchers can amass the volume of threat activity data necessary to recognize the malicious nature of the site. Thus, newly launched credential harvesting sites go undetected by traditional email security technologies, including Office 365 and Gmail security defenses.

Thwarting these attacks demands muscular phishing defense: Google-like proactive web crawling, keen data analysis, brand detection – and speedy checks of associated infrastructure to detect imposter pages before credential-harvesting attacks launch. Advanced anti-phishing technical controls with early insight to malicious pages and instant-crawl of suspicious URLs, can detect and block emails containing links to credential-harvesting sites before they reach employee inboxes.

MALWARE, RANSOMWARE AND MORE: SPREADING THE MISERY

Installing malicious code on your system is the hacker holy grail, setting you up for ransomware, credential theft, crypto-mining and more. Once established, hackers can send your confidential and proprietary information elsewhere and gain entry to other systems and data on your network.

Threat actors use many techniques to slip malware-infected files past cyber defenses. They lure victims to click on a URL in an email or social post that downloads a malware-infected document. They also use URL shorteners and redirects to hide their malicious links and evade cyber defenses. They might also embed links to malware-infected documents in benign email file attachments. Hackers can easily attach password-protected or archived malicious files to emails, hiding their activities with techniques that evade Office 365 and Gmail signature- and sandbox-based malware-detection technologies.

> *"Despite Google's and Microsoft's continued investment in G Suite and Office 365 security improvements, some Gartner clients report dissatisfaction with natively available capabilities and are, therefore, choosing to supplement with third-party products..."*
>
> – Gartner

PHISHING ATTACKS: THE BAD, THE WORSE, AND THE WORST

Breaches and thefts like these are taking place under the watchful guard of technology giants. How? According to Gartner, ***"Not all email and SEG vendors include best-of-breed protection. Should this be the case for your solution, consider complementing it for additional protection."***

BEC: 'Arrivederci' to corporate millions

Early in 2019, Chinese hackers stole $18.6 million from an Italian engineering company, through an elaborate cyber fraud scheme that included impersonating the firm's chief executive. Hackers convinced a corporate officer to transfer that amount in three batches: $5.6 million, $9.4 million and $3.6 million to banks in Hong Kong. Withdrawn within minutes, naturally.

Spear-Phishing: Sony's North Korean hackers three-peat

The same hackers who laid waste to Sony in 2014 three-peated by stealing $81 million from Bangladesh Bank and creating the malware used in the 2017 WannaCry ransomware attack. Damages amounted to billions of dollars according to the FBI. Right now, the group is homing in on defense contractors, university faculties, technology companies, virtual currency exchanges, and US electric utilities. Look sharp!

Ransomware: Hackers Demand $1M in Grays Harbor Ransomware Attack

Healthcare providers are in a uniquely painful bind when it comes to ransomware: the very lives of patients may depend on the availability of the vital information the hackers take hostage. Greed in the attack on Washington-based Grays Harbor Community Hospital and Harbor Medical Group exceeded all prior bounds when hackers demanded $1 million from the cash-strapped organization to unlock patient files. Not surprisingly, the ransomware had invaded via a phishing email clicked on by an employee. When the staff initially treated the attack as an IT issue, the ransomware seized the opportunity to spread to clinics and take down medical records, prescriptions and other key data. The clinics were forced to revert to paper and pen for communications—inflicting not just inconvenience and cost-inefficiency, but heightened risk as well.

The devastation wrought by ransomware has jumped 184 percent during the second quarter of 2019, with average downtime of nearly 10 days. Without phishing emails as their primary tool, ransomware would be hard-pressed to do the damage it does. It's a vivid example of the extraordinary harm that can come from something as simple as an email.

> *"With companies such as Google and Microsoft commonly sending users alerts when unusual activity has been discovered on their account, users may feel its normal to receive them and would then click on the enclosed link. Attackers are capitalizing on this by sending emails that pretend to be 'Microsoft account unusual sign-in activity' alerts from Microsoft..."*
>
> – Bleeping Computer

WIN THE CLOUD PHISHING WARS

As cloud email attacks proliferate, phishing has also spawned more cybersecurity solutions. Nevertheless, the black hats keep setting the pace because successful attacks and damages keep soaring. It's a truism but worth restating that defenders must win every encounter, while the attackers need to breach only once in order to wreak their havoc.

Protecting your cloud email from modern phishing sites requires aggressive detection techniques, including proactive and real-time web crawling, to discover malicious locations. These strategies, used in combination with sophisticated ML models, can quickly detect criminal websites and prevent download of malicious code.

GARTNER: PRIORITIZE A MULTI-TIERED ANTI-PHISHING APPROACH

While traditional cybersecurity solutions can detect and protect against known phishing sites and downloads, they lack critical early awareness of newly established or previously unknown malicious sites and payloads. Against a fierce criminal headwind, a layered or multi-tiered approach is key to keeping your mailbox from being weaponized against you.

In its foundational paper, How to Build an Effective Email Security Architecture, Gartner recommends priority establishment of anti-phishing technology controls to reduce cyber risk.

The paper notes Verizon's statistic that phishing and pretexting encompass 98 percent of social incidents and 93 percent of breaches. The report recommends designing an email security architecture that addresses the severity of modern email threats such as malware, malicious URLs, credential phishing and BEC. Gartner refers to Area 1's ability to protect the inbox with:

- Pre-emptive crawling
- Machine learning models
- Cousin domain detection
- Anomaly detection—among other resources

To learn more about how Area 1 Security stops the phishing threats that other defenses miss, read the Area 1 report Phishing: Top Threats Missed by Existing Defenses.

AREA 1

About Area 1 Security

Area 1 Security offers the only pay-for-performance solution in the cybersecurity industry - and the only technology that comprehensively blocks phishing attacks before they damage your business. Phishing is the root cause of 95 percent of security breaches, according to Gartner.

Area 1 Security works with some of the most sophisticated organizations in the world, including Fortune 500 banks, insurance companies, and healthcare providers to preempt and stop targeted phishing attacks at the outset, improve their cybersecurity posture and change outcomes.

Learn more at www.area1security.com, join the conversation at @area1security or follow the blog for the latest industry news and insights on how to deal with phishing.

▸ Learn More INFO@AREA1SECURITY.COM