Phishing Is No Longer Just Email: It’s Social
Executive Summary

Despite years of publicity and millions of dollars in employee training, phishing remains the largest insider threat that organizations face. As many as 93% of IT security breaches are the direct result of some form of phishing and 34% of all phishing attacks explicitly target enterprises. Employees unwittingly give up personal and corporate information to malicious actors every day.

And now, the attackers are widening their nets.

No longer limiting themselves to email, criminals are exploiting popular social media networks, instant messaging applications, and online file-sharing services. Facebook, Slack, Microsoft Teams, Dropbox, Google Docs, and other popular platforms are serving as the criminals’ initial point of penetration into the enterprise. These channels are much more personal; they invite sharing and widespread distribution, so phishing can propagate exponentially.

One set of stolen credentials is all a criminal needs to access the corporate network, where they can then move laterally to find and exfiltrate an enterprise’s crown jewels.

Traditional corporate security controls have limited ability to mitigate these risks. Employees are mobile and distributed. They may access personal email and social accounts from their work devices, with only marginal monitoring by IT departments. And when they access social apps on mobile devices, they’re outside the enterprise’s sphere of governance.

Vigilance, unfortunately, can only do so much. As soon as security professionals thwart one type of phishing attack, another comes along. It’s a cat and mouse game, and criminals are sophisticated, patient, and targeted. They persistently probe for ways to foil existing enterprise security defenses.

To make matters worse, malicious actors can easily buy off-the-shelf phishing kits on underground sites. These toolkits give scammers everything they need to rapidly create fake web pages and launch malignant campaigns via email and social channels – all with an eye toward corporate penetration.

More phishing emails, too, are getting through enterprise email security systems. Although most modern enterprises likely have protections in place, these gateways and filters are far from perfect. Regardless of their efficiency, relying on a single layer of defense against such rampant attacks isn’t best practice.
Phishing Is No Longer Just Email: It’s Social

Faced with these challenges, today’s businesses need a new approach to enterprise security. Namely, a Zero Trust mentality: Trust nothing, verify everything, and maintain consistent controls. Every access request must be authenticated and authorized, and then only granted on a transient basis.

Advanced, cloud-based, and real-time threat protection is pivotal to this security transformation. It will enable the enterprise to keep pace with today’s evolving threat landscape, including the social phishing phenomena we explore in this white paper.

## The Business Impact of Phishing

Organizations across the globe report that phishing schemes are the major source of enterprise security breaches. As many as 93% are the direct result of some form of phishing.⁵

The presence and effectiveness of phishing is staggering:

- 1 in every 99 emails is a phishing attack, using malicious links and attachments as the main vector⁶
- 52% of successful email attacks get their victims to click within an hour — and 30% within 10 minutes⁷
- Nearly 1.5 million new phishing sites are created each month⁸
- 83% of InfoSec professionals experienced phishing attacks in 2018⁹

This should surprise no one. If you’re a cybercriminal, it is far easier to log into the corporate network with an employee’s stolen information than it is to hack into an enterprise. Just one set of compromised credentials is all that an attacker requires to gain entry and establish a foothold. This initial ingress quickly leads to lateral movement, identification of the most valuable resources, and ultimate exfiltration.

And the impact is considerable:

- The average cost of a phishing attack for a midsize company is $1.6 million¹⁰
- 1 in 3 customers will stop doing business with a company that experiences a cybersecurity breach¹¹
Social Phishing: Casting a Wider Net

Social networking, messaging apps, and file-sharing services all rely on some level of trust. This makes social media ideal attack vectors. Bad actors capitalize on the perceived trust and community of these platforms, tricking users into spreading malicious content. The number of phishing scams on social media is up more than 70% over the first quarter of 2019.12

One common practice in the lifecycle of a phishing scam is to include a step where the victim must share a link – the fake or compromised website’s URL – across their social networks. As the link comes from a reputable or known contact, the victim’s social connections soon fall prey to the scheme themselves. And misplaced trust in a dangerous cyberdestination propagates.

In his white paper, “A New Era in Phishing: Games, Social, and Prizes,” Akamai security researcher Or Katz examined how social phishing campaigns leverage contests and rewards to deliver malicious links.13 Bogus prizes and fake promotions masquerading as legitimate opportunities further incentivize distribution, creating environments that lead targets to disclose personal and corporate information.

As social channels grow in number and popularity, threat actors have more ways to reach victims.

Forbes reports that criminals now use instant messaging services such as Slack, Skype, Microsoft Teams, and Facebook Messenger to acquire new victims and magnify their campaigns.14 These socially focused schemes use many of the same methods as email phishing – impersonation, capitalizing on implied trust, and malicious links – but are delivered through these next-generation communication platforms.

According to CSO, bad actors increasingly stage phishing attacks through online file sharing and collaboration tools, such as Microsoft OneDrive, Google Docs, SharePoint, WeTransfer, Dropbox, and ShareFile.15 Sometimes files contain the malware. Sometimes they are part of a broader phishing scheme meant to transport and house images, documents, and additional materials that might help legitimize the scheme to its targets and corporate email scanners.

Fictitious social media users add yet another element in these attacks. They appear on a website as an integrated plugin for social networks, often providing testimonials. The target is actually seeing embedded JavaScript code on a spoofed phishing site that presents pre-generated social accounts. These fake people become proof that others have won (nonexistent) prizes. This encourages participation and further sells the scheme.
Social phishing campaigns launched specifically via mobile devices are especially tricky to mitigate. In addition to the acknowledged security shortcomings of mobile devices, the mobile user interface does not have the depth of detail needed to identify phishing attacks, such as hovering over hyperlinks to show the destination. As a result, mobile users are three times more likely to fall for phishing scams.16

**Attackers Continue to Evolve Phishing Tactics**

Modern criminals are persistent and use multifarious, targeted activities to bypass enterprise security defenses. Protecting against their phishing campaigns is an ever-evolving arms race. As soon as security practitioners thwart one assault, malicious actors pivot and adjust their technique.

A recent example: Attackers found a vulnerability that allowed them to bypass Microsoft Office 365’s existing email security protocols. They obfuscated the phishing URL by embedding zero-width characters into it. This allowed the compromised emails to evade Microsoft’s URL reputation check and Safe Links URL protection.17 Users received the email with the phishing link intact, instead of the Microsoft-hosted link that should have replaced it.

In their recent *Phishing Activity Trends Report*, the Anti-Phishing Working Group noted a growth in the use of URL redirection. Attackers place redirectors both prior to the phishing site landing page and following the submission of the credentials. This helps hide the phishing URL from detection via web server log referrer field monitoring.18 Additional examples of evolved and inventive phishing include:

- The industrialization of phishing through the increasing popularity of off-the-shelf phishing kits
- Using Google Translate to obfuscate a URL that is linked to a fake Google credential scraping site19
- Employing SSL encryption on a phishing web page to lend credibility to a phishing email20

Business email compromise (BEC) schemes are also on the rise. Criminals send phishing emails from compromised reputable accounts – often Microsoft Office 365 accounts. Because the senders are real, filters don’t block these communications. Such scams increased by 476% between Q4 2017 and Q4 2018,21 leading to $1.2 billion in losses in 2018.22
Phishing Kits: The Industrialization of Phishing

Templated, mass-produced phishing kits make it easier than ever to quickly create and launch malicious campaigns. Sold on the underground Internet, these kits typically give scammers everything they need to mount damaging attacks: graphics and web design tools, placeholder content, and mass emailing or other distribution software.

Steve Ragan, an Akamai security researcher, describes these toolkits in his article for CSO:

“They’re the web component, or the back-end to a phishing attack. It’s the final step in most cases, where the criminal has replicated a known brand or organization. Once loaded, the kit is designed to mirror legitimate websites, such as those maintained by Microsoft, Apple, or Google.”

Tens of thousands of such kits are currently available. Criminals develop them using a mix of basic HTML and PHP, and store them on compromised web servers. The programs usually live for just 36 hours before they are detected and removed.

Cybercriminals originally offered phishing kits for sale, but they are now increasingly offered free of charge. These “free” phishing kits, however, often hide the toolkits’ authors as implicit recipients, meaning that phished information is not only captured by the toolkit buyer, but also by the original creator. As the saying goes, there is no honor among thieves.

Akamai researchers recently tracked the activity of more than 300 phishing campaigns that all use the same phishing kit to abuse over 40 commercial brands. Each scam begins with a three-question quiz related to a recognized brand. Regardless of their selected answer, the victim always “wins.”

Because these phishing campaigns are based on the same toolkit, they share functionality and features, as shown to the right.
These toolkit-based campaigns capitalize on the trusted reputation of known brands. Although they have similar origins and characteristics, each was easily customized to contain different quiz questions in a variety of languages. Many of the victimized brands were airlines, but abuse is widespread. Criminals also commonly spoof retail, home decor, amusement park, fast food, restaurant, and coffeehouse brands.

Many of these fake, phishing kit-produced pages target consumers who then inadvertently transport the compromise onto their corporate network. And kits that explicitly target enterprise users are widely available as well. Such toolkits were used to create these imitation Microsoft Office 365 and SharePoint login pages:

![Microsoft Office 365 and SharePoint login pages](image)

**What About Email Filters and Gateways?**

Enterprises generally have some form of email filtering in place, either as a dedicated service or as an addition to Microsoft Office 365 or Google G Suite. These products do a decent job of keeping traditional spam, phishing, and malicious emails from users. But they are far from perfect.

In its latest *Email Security Risk Assessment*, email management company Mimecast reports that compromised communications are increasingly getting through current email security systems. They detected 463,546 malicious URLs contained in 28,407,664 delivered emails. In other words, 1 of every 61 phishing emails reaches the intended recipient.26

The ease and cost effectiveness of phishing kits, as well as the proliferation provided by social networks mean that cybercriminals can create and circulate short-lived phishing campaigns with great success. The Akamai threat research team has determined that such short-lived attacks pose a unique set of challenges.
Traffic must reach the phishing domain and show a change of behavior in order to be flagged. By the
time security teams observe this rogue traffic, analyze the URL, add the URL to a threat list, and push
the updated threat list out to customers, the phishing campaign is over. It has run its course and the
malicious URL has been deactivated, likely by the criminals or perhaps by the legitimate owner of the
site that hosted the compromised URL.

This detection gap presents a significant threat to enterprises.

The era of roaming corporate devices and BYOD (bring your own device) creates yet another
weakness. A distributed and mobile workforce means that traditional corporate security mechanisms
are increasingly insufficient. Personal devices that move in and out of the organization’s perimeter may
access private email accounts not protected by the enterprise’s email gateways and filters. As the line
between professional and personal devices and access continues to blur, this threat will only worsen.

Employees who fall for phishing or other attacker scams
are the most dangerous insider threat.27

42% Innocent employees getting duped

26% Employees blending work and personal use

Phishing Is No Longer Just Email: It’s Social
And, as discussed previously, email isn’t the only way to launch a phishing attack and distribute malicious links.

To detect, block, and mitigate these sophisticated phishing attacks, organizations need an additional layer of defense – one that looks into all traffic from all of the devices on the network.

**Conclusion**

The phishing landscape has evolved. Industrialized phishing kits, as well as the use of social networks and other non-email distribution channels are the new normal. Further exacerbating this alarming trend, devices are roaming and users generally access social network and messaging apps through mobile devices, which are typically the weakest link in an enterprise’s security structure.

To successfully fight back, modern enterprises must adopt a Zero Trust model. The corporate security motto should be: Trust nothing, verify everything, and maintain consistent controls. Enterprises need to authenticate and authorize every single access request, and then only grant access on a transient basis.

Cloud-based security solutions are uniquely positioned to implement a Zero Trust framework because they can monitor all enterprise network activity, regardless of device type or the origin of a request. They have crowdsourced visibility – they aggregate disparate, limited-scope traffic and build global, real-time insights. These solutions use Internet-wide patterns to achieve more complete threat awareness.

By observing the impact of phishing campaigns across multiple enterprises, cloud-based protection can identify trends that a single enterprise may not be able to detect.

**Akamai Enterprise Threat Protector**

Akamai’s Enterprise Threat Protector proactively identifies, blocks, and mitigates targeted threats arising from phishing campaigns, phishing kits, malware, ransomware, DNS data exfiltration, and advanced zero-day attacks. Enterprise Threat Protector is a Secure Internet Gateway that enables security teams to ensure that users and devices can safely connect to the Internet, regardless of where they are connecting from – and without the complexity associated with legacy approaches.

For additional information on Enterprise Threat Protector and a free trial, visit akamai.com/etp.
Phishing Is No Longer Just Email: It’s Social

Akamai secures and delivers digital experiences for the world’s largest companies. Akamai’s intelligent edge platform surrounds everything, from the enterprise to the cloud, so customers and their businesses can be fast, smart, and secure. Top brands globally rely on Akamai to help them realize competitive advantage through agile solutions that extend the power of their multi-cloud architectures. Akamai keeps decisions, apps, and experiences closer to users than anyone — and attacks and threats far away. Akamai’s portfolio of edge security, web and mobile performance, enterprise access, and video delivery solutions is supported by unmatched customer service, analytics, and 24/7/365 monitoring. To learn why the world’s top brands trust Akamai, visit akamai.com, blogs.akamai.com, or @Akamai on Twitter. You can find our global contact information at akamai.com/locations. Published 08/19.

SOURCES
3) Internal Akamai research
12) https://betanews.com/2019/05/02/social-media-phishing/
15) “Cybercriminals Impersonate Popular File Sharing Services to Take Over Email Accounts” by Asaf Cidon, CSO. https://www.csoonline.com/article/3274546/cybercriminals impersonate popular file-sharing services to take over email accounts.html
24) Internal Akamai research