proofpoint

The Human Factor 2015

A Proofpoint Research Report

Most advanced attacks rely as much on exploiting human flaws as on exploiting system flaws. Proofpoint developed this report, The Human Factor, to explore this under-reported aspect of enterprise threats using data gathered from the Proofpoint Targeted Attack Protection product deployed in customer environments, tracking threats in email attachments, social media posts, and URLs.

This paper uses original field research to provide insight on who is clicking, and what they are clicking on, as well as when, where, and why they are clicking – because as the data show, the weakest link in security is all of us.

Contents

Executive Summary . . . 3

Key Insights . . . 4

Who . . . 7

- Who clicks on Malicious Messages? . . . 7
- Who Is Receiving Malicious Messages? . . . 8
- Who clicks on Malicious Messages: Execs or Staff? . . . 9
- Who clicks on Malicious Messages: IT or Sales? . . . 10

What . . . 11

- What Kind of Messages Are Users Clicking On? . . . 11

When . . . 13

- When Do Users Receive and Click Malicious Messages?: Time After Message Arrival . . . 13
- When Do Users Receive and Click Malicious Messages?: Time and Day . . . 14

Where . . . 16

- Where do users click from? . . . 16

Why . . . 17

- Why Are Users Clicking? . . . 17

Defending Against Attacks . . . 18

Executive Summary

In 2014, widespread end-user education succeeded in raising awareness of phishing as a threat, enabling end-users to recognize the most common phishing templates – such as social media invites – and become more wary of unsolicited messages in general. One result of this was a 94% year-over-year decrease in the effectiveness of social media invitation email lures.

In response, 2014 was the year attackers 'went corporate,' with explicit shifts in approach clearly designed to exploit middle-management and exfiltrate cash. By the end of 2014, cybercriminals were targeting subtly different user populations and employing tactics that looked very different from what users – and automated defenses – had adapted to recognize, specifically:

- Campaigns focused on businesses and financial access, with less reliance on social media invitations and other personal communication templates.
- Significant increases in attachment usage, disguised as e-fax, voicemail, or document formats
- Balanced attacks that mixed high-volume longline campaigns with strategic web compromises, attachment-based campaigns, and corporate communication and financial email lures.
- Changed time of distribution to blend in with business high mail-flow times.
- Designed campaigns that cut off the "long tail" of clickers in favor of more immediate payoff to get around faster-adapting defenses.
- Refocused on "traditional' endpoint platforms that predominate in business IT environments, such as PCs running Windows and Internet Explorer.

The result? It worked. Every company still clicks; every department and industry is still at risk (though financial industries and sales and marketing continue to be the top target areas); and attackers continue to shift tactics to play on human weaknesses as they siphon money and data from organizations.

The central lesson of 2014 for CISO's is that while user education may have an impact, attackers can always adapt and adjust their techniques more rapidly than end-users can be educated.

Key Insights

Who is clicking?

Every company clicks: On average **one of every twenty-five** malicious messages delivered are clicked by users. No organization observed was able to eliminate clicking on malicious links.

> ***Recommendation:*** User training is a necessary strategy and can pay dividends depending on the nature of the attack. Unfortunately, it is an insufficient strategy for dealing with threats that piggyback on valid messages or employ new, unfamiliar lures. Teams must explore technical and automated capabilities that minimize risk from user clicks.

All industries are being targeted with malicious messages, but a few stand out. Users in Banking & Finance **received 41% more malicious messages than the average across industries**. At the same time, there is no industry that does not receive email-borne advanced threats.

> ***Recommendation:*** All industries are targeted to a different extent, by different types of attackers, with different motives. It is vital to understand the specific nuances of an organization's specific situation, and monitor attack trends with appropriate threat intelligence and user monitoring, to understand whether some aspect of the organization is viewed as a lucrative target by cybercriminals.

All user roles are targeted, though Middle Management has become much more targeted. Managers and Staff clicked on links in malicious messages **two times more frequently than Executives**. Compared to last year, Managers also received more malicious emails and doubled their click rates.

> ***Recommendation:*** Information security policy and practices must pay special attention to non-executive employees, where most of the compromises will originate. Teams must use a set of tools that can give appropriate visibility into who is clicking, when, and how often, beyond just the malware forensics.

Every department is a target, even if some are better than others about clicking on malicious messages. While malicious messages were **targeted very evenly** across organizational departments, Sales, Finance and Procurement clicked on links in malicious messages **50-80% more** than the average departmental click rate. Attackers are targeting corporate financial users with access to payments and funds transfers, rather than trying to blanket all users.

> ***Recommendation:*** Organizations need a flexible defense against email-borne threats that can be deployed across all parts of the organization, protect on-site and global, remote or mobile employees, as well as support granular policies tailored to the needs of each department.

What are people clicking on?

The most clicked email lures were Communication Notification lures such as e-fax and voicemail messages alerts. The use of social media invitation and order confirmation lures – the most popular and effective email lures last year – decreased dramatically. Email lures that employ attachments rather than URLs, such as invoice and account statement lures, increased significantly as a vector, on some days driving a 1,000% increase in messages with malicious attachments over the normal volume.

> ***Recommendation:*** Attackers continually adjust their techniques to adapt to changing defenses, whether such defenses are technical or psychological. While an important tool, user education cannot be the last line of defense: organizations should deploy automated defenses capable of detecting and blocking threats that do not look or behave like previously known threats.

When do people click?

Clicks happen fast. The clock is ticking: organizations no longer have weeks or even days to find and stop malicious emails, because attackers are **luring 2-out-of-3 end users into clicking on the first day**, and by the end of the first week 96% of all clicks had occurred.

> ***Recommendation:*** With the majority of clicks on malicious URLs occurring within twenty-four hours after the message arrives, now more than ever time is of the essence for organizations. Best-of-breed detection of advanced and emerging threats and integrated incident response are must-haves to predictively block threats and mitigate infections.

Attacks are occurring mostly during business hours. The majority of malicious messages are delivered during business hours, **peaking on Tuesday and Thursday mornings**, and Tuesday is the most active day for clicking, with **17% more clicks than the other weekdays**. While the majority of clicking on malicious links still occurs during normal US business hours, significant clicking occurs still occurs outside business hours, showing that end-users are vulnerable to email-borne threats around the clock, regardless of whether they are on-site or remote.

> ***Recommendation:*** Users are no longer constrained by the temporal boundaries of the workday and workweek. Organizations must be able to protect their users around the clock as well, on weekends as well as weekdays, with protection that can follow them through their day. This protection capability must be seamless in order to integrate with their styles of working and accessing email at any time and across a range of platforms.

Where do people click?

On average, 1-in-5 clicks on malicious links still occur off the corporate network. Off-network click rates vary significantly by company and industry, but all experience some amount of off-network clicks.

> ***Recommendation:*** Consider technical solutions that provide a follow-me approach to protection against user clicks, regardless of device and regardless of whether the device is on or off the corporate network.

Why do people click?

Users clicked on phishing emails in 2014 because these evolved campaigns didn't match the characteristics users had been trained to look for in 2013. End-users had been trained to be wary of social media invites and other popular templates. When attackers changed their strategy to targeting corporate users with attachments in high-volume campaigns, while piggybacking on legitimate messages, such as email newsletters and opt-in marketing emails, end-users were faced with a large number of malicious email that they could not recognize as a threat. For example, there was a high volume of Microsoft Outlook Web Access (OWA) credential phish, as it is very easy to spoof these pages, and they produce high-value results.

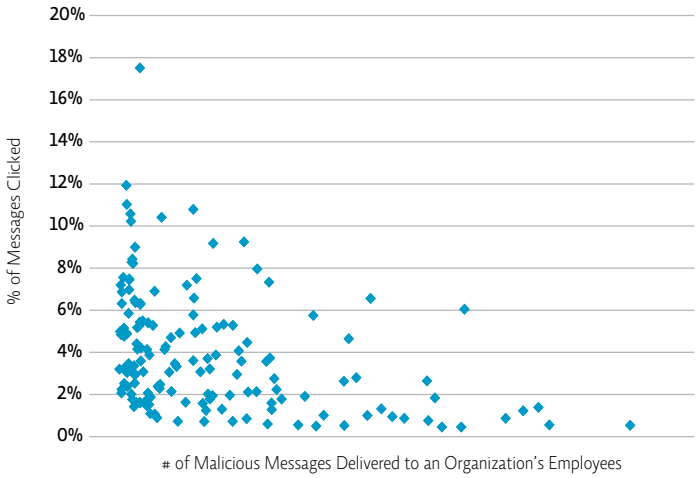
> ***Recommendation:*** Adaptive defense capable not only of protecting against attachments and URLs, but more importantly with integrated threat intelligence that enables early detection of emerging campaigns and threats, as well as big-data analytics that can detect unsolicited mail campaigns that include advanced threats or no apparent threat at all.

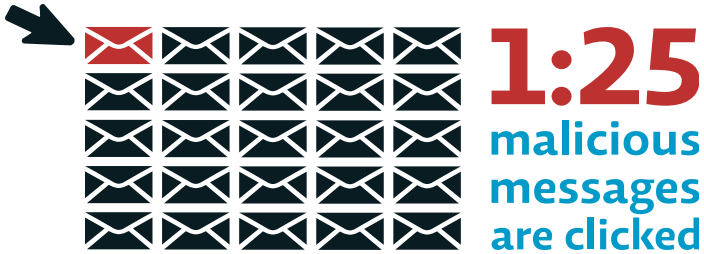
To read more of this and our other research, visit: www.proofpoint.com/threat-insight

This page was intentionally left blank.

Who clicks on Malicious Messages?

Percent click rate per customer



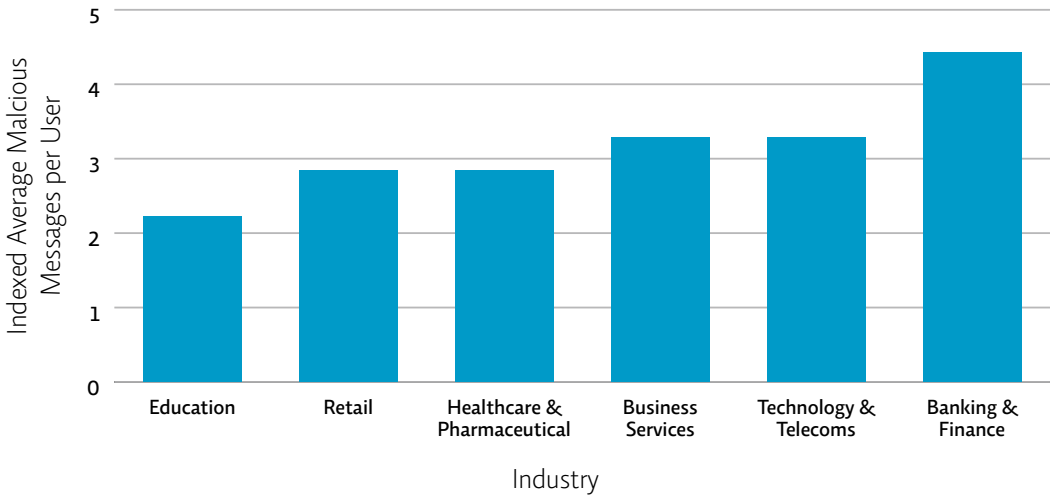


What this means

- The average click rate is just under 4% and remains relatively constant regardless of the number of messages received.
- The volume of messages an organization receives has little to no impact on the click rate: every organization clicks, and the rate of clicking for an organization is never zero.

Who Is Receiving Malicious Messages?

Malicious messages per user per industry

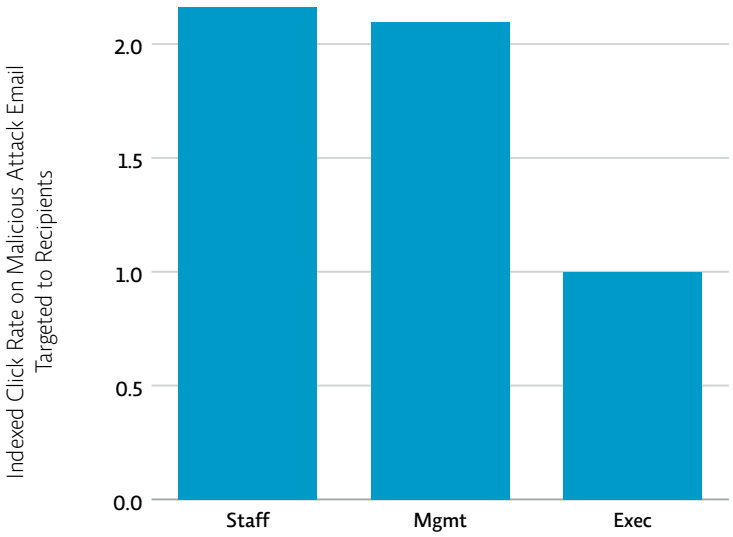


What this means

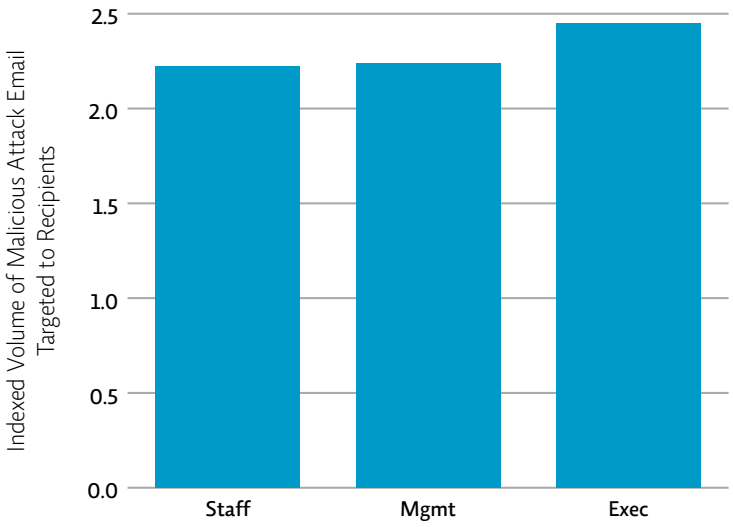
- Users in the most targeted industry, Banking & Finance, received 41% more malicious messages than the average across industries.
- All industries are being targeted with malicious messages. While attackers favor some industries due to the value of the data they hold, every industry receives email–borne advanced threats.
- Cybercriminals no longer focus exclusively on stealing user and account information from banks, and all organizations are now at risk from attacks. While credit card data theft has shifted to any organization of any size that might accept or process credit card payments, the higher value of personal health records (PHR) and insurance cards on the black market are driving attackers to target large and small organizations in health care and insurance. Meanwhile, intellectual property (IP) theft and the opportunity for direct financial transfers means cybercriminals are attacking previously 'uninteresting' sectors such as manufacturing, shipping, energy, utilities, and even construction.

Who clicks on Malicious Messages: Execs or Staff?

Click rate by role



Malicious messages by role

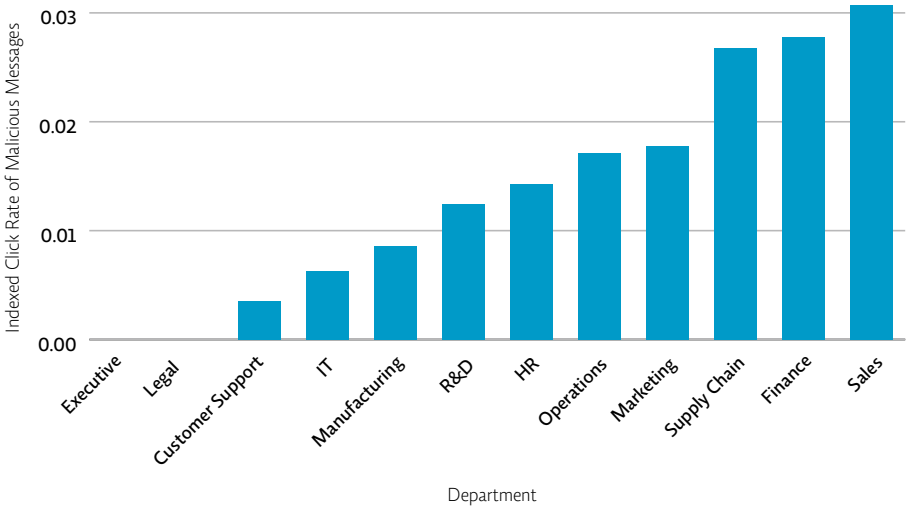


What this means

- All user roles are targeted: every role receives malicious messages. Job functions in 2014 were almost equally targeted by malicious messages, with executives being slightly more targeted than Management and Staff.
- Managers effectively doubled their click rates compared to the previous year. This represents a marked change from 2013 for Managers, who were much less frequently targeted by malicious emails in 2013 than in 2014.
- Staff continued to click by a ratio of 2–to–1 over executives, and in 2014 were joined by Managers.
- This change reflects a shift in the cybercriminal attack campaign landscape: large–scale attack campaigns shifted from embedding malicious URLs to using attachments or URLs linked to compromised sites in legitimate Web marketing messages, such as newsletters and opt–in marketing emails.

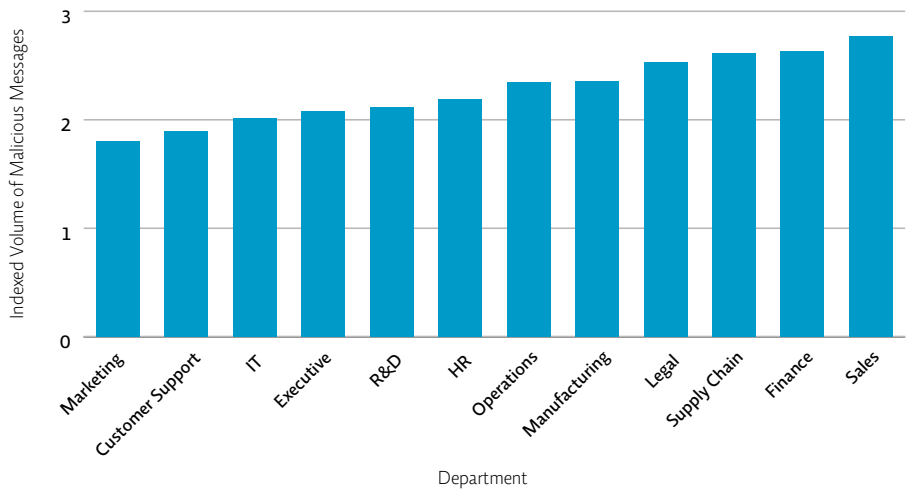
Who clicks on Malicious Messages: IT or Sales?

Click rate by department



3x more likely to click than IT

Indexed volume of malicious messages by department

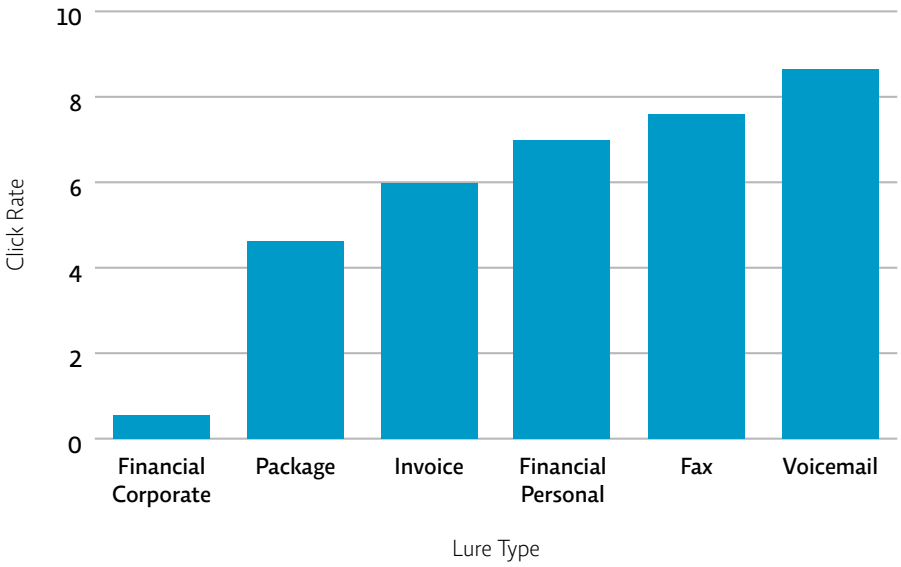


What this means

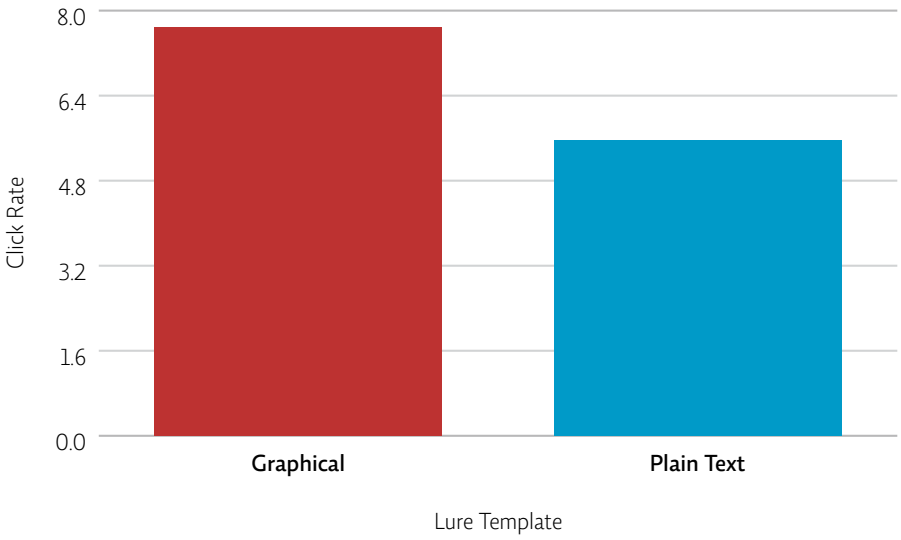
- Sales, Finance and Procurement (Supply Chain) were the worst offenders when it came to clicking links in malicious messages, clicking on links in malicious messages 50–80% more frequently than the average departmental click rate. This would be expected, since these functions have a higher amount of email-based interaction with external senders.
- Technical organizations still click on links in malicious messages. For example, research and development (R&D) placed in the middle of the department rankings, clicking less frequently than marketing and human resources (HR), but more frequently than customer support and IT. Customer support and IT were the least frequent clickers of malicious messages.
- In contrast to click rates by department, which showed broad range and distinct leaders, malicious messages were targeted very evenly across organizational departments. Every department is a target, but some are better than others about clicking on malicious messages.

What Kind of Messages Are Users Clicking On?

Click rate by email lure



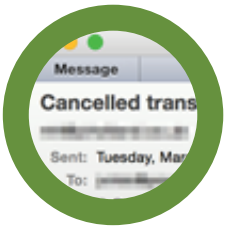
Click rate by lure template type, graphical vs textual



Top 3 Most Clicked Email Lures

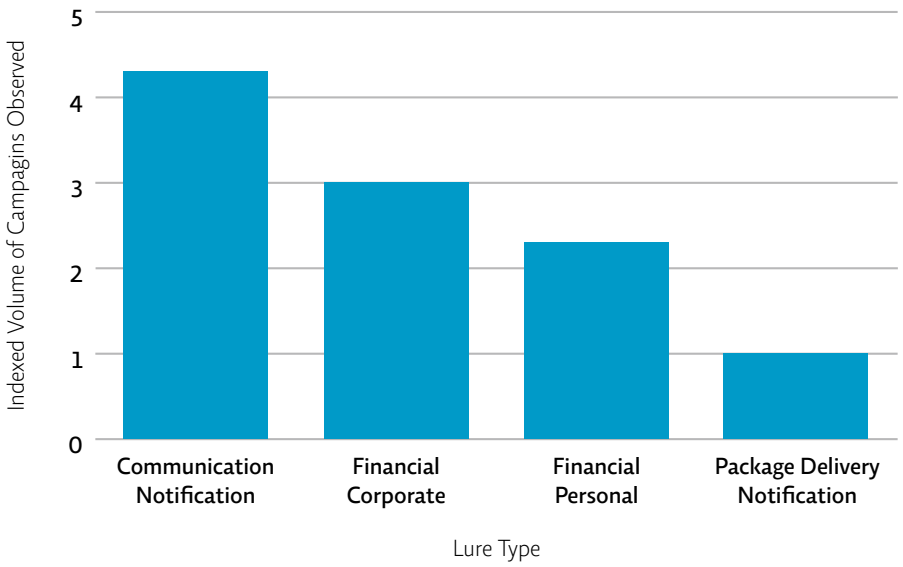
Voicemail

Fax



Financial Personal

Most common email lures in 2014

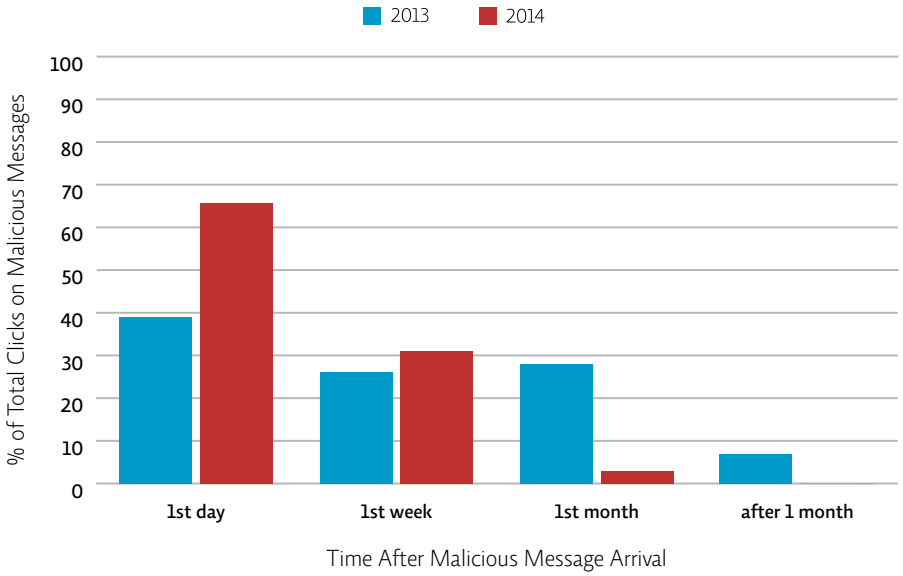


What this means

- The most popular email lures in 2014 were Communication (i.e., "You have a voicemail") and Corporate Financial messages, such as ACH and wire transfer fraud emails.
- The last twelve months saw a 94% decrease in the use of social media invitation and order confirmation lures, which were the most common and most effective email lures in 2013.
- Despite a major shift in 2014 to target corporate financial credentials (such as banking passwords) by volume of attacks sent, the Corporate Financial lure ranked the lowest as measured by click-through rate. However, such lures also deliver the highest yield: each successful wire transfer fraud can net hundreds of thousands or even millions of dollars. Similar to venture capitalists, movie studios or pharmaceutical companies who invest to deliver one "blockbuster" out of many candidates, attackers are performing a basic expected-value calculation (that is, delivery rate x payoff – cost of delivery) and counting on the high value of a click to compensate for the lower overall click-through rate of this lure.

When Do Users Receive and Click Malicious Messages?: Time After Message Arrival

User clicks after threat arrival

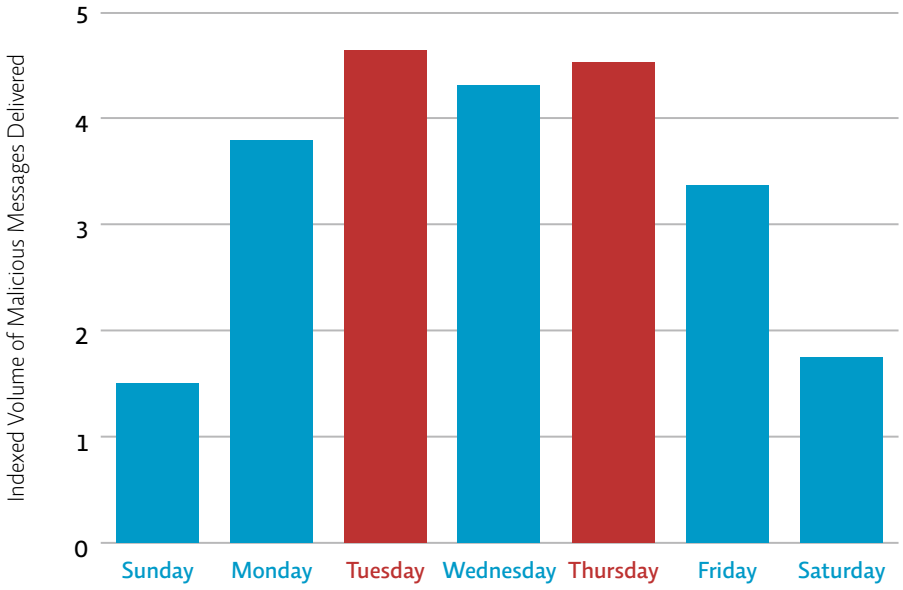


What this means

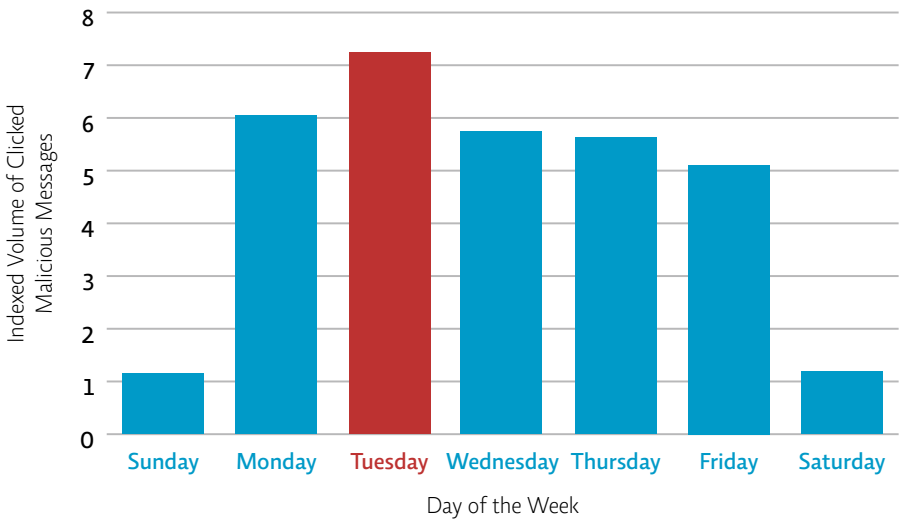
- Attackers are luring 2-out-of-3 (66%) end users into clicking on the first day after a malicious message is received
- By the end of the first week 96% of all clicks had occurred.
- This behavior represents a significant change in malicious URL lifespan compared to last year, when only 39% of malicious links were clicked in the first twenty-four hours after they arrived, and even after one week only 65% of clicks had occurred.
- The 'long tail' observed last year seems to have fallen off, with the percentage of clicks after 30 days effectively falling to zero.

When Do Users Receive and Click Malicious Messages?: Time and Day

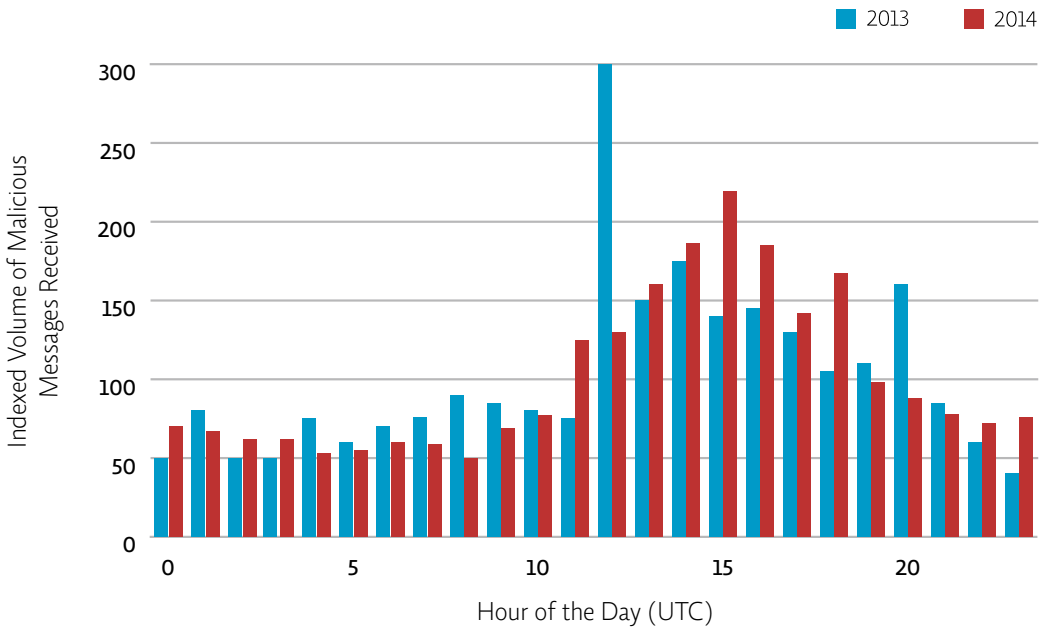
Malicious messages received by day of the week



Malicious messages clicked by day of the week



Malicious messages clicked by hour of the day (UTC)



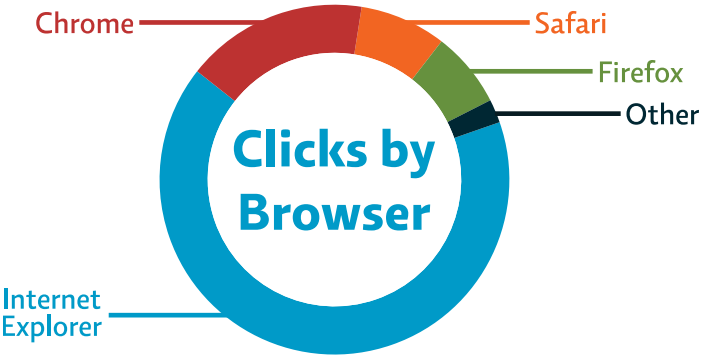
Malicious Message Peak Click Time

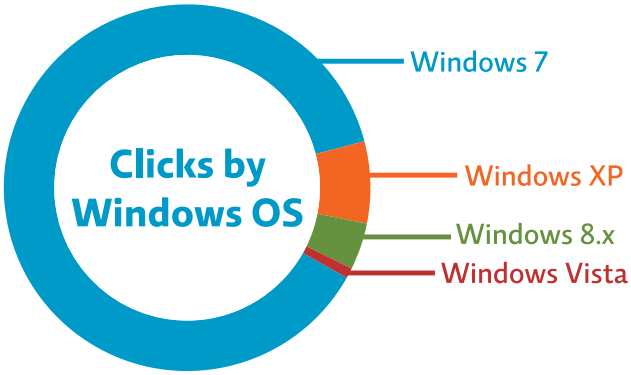
10:00am to 3:00pm ET

What this means

- Peak hours for end-users clicking on malicious links are 10am-6pm ET, which shows that many employees are clicking as part of their daily tasks, and end-users click 17% more on Tuesdays than the other weekdays. This is consistent with attackers' shift to attachments and whitelisted web marketing emails linked to watering holes; the attacks are now significantly more focused on business managers.
- Saturday and Sunday clicks are occurring steadily, which means that end-users are still clicking on malicious links over the weekend when they are (presumably) off-site and probably working from a mobile device.
- In 2015, Tuesday and Thursday emerged as significant leaders in volume of malicious messages, with biggest relative year-over-year drop hitting Monday and Friday. Last year, email lures such as order confirmations were designed to hit at low points: Thursday and Friday, before work. In 2014, lures such as communication notifications and newsletters need to blend in with email flow and points of highest volume: midday Tuesday and Thursday.
- A significant amount of clicking on malicious links still occurs outside of normal US business hours, demonstrating that end-users are vulnerable to email-borne threats around the clock, regardless of whether they are on-site or remote.

Where do users click from?



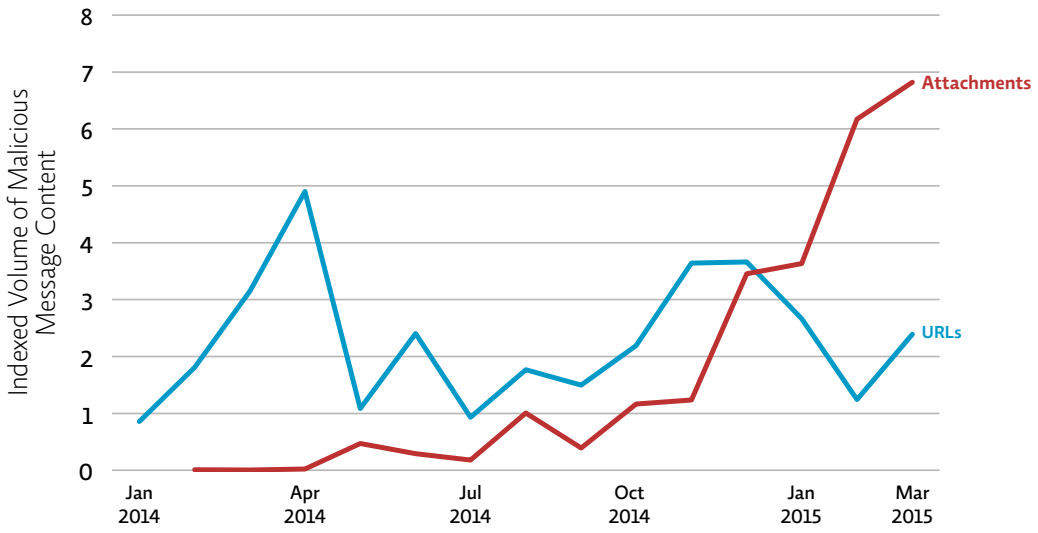


What this means

- On average 1-in-5 clicks (20%) on malicious links still occur off the corporate network. Off-network click rates vary significantly by company and industry, but all experience some amount of off-network clicks.
- 91% of clicks came from PC's in 2014, a slight increase from the 90% we observed in 2013.
- Clicking from Microsoft-based platforms increased across the board: there were more clicks from PCs, from Windows-based operating systems, and from Internet Explorer.
- However, 5% of clicks (1-in-20) on Windows clients come from systems for which patches are no longer available from Microsoft.

Why Are Users Clicking?

Malicious messages trend, Attachments vs URLs, January 2014–March 2015



Volume of messages with malicious attachments increased

17x in 6 months

What this means

- As efforts to educate employees about the dangers of phishing emails that used fake social media invites and financial account notifications began to reduce the effectiveness of those lures, attackers changed tactics and focused on lures types designed to elicit more response from corporate users, such as financial fraud messages, or credential phish and wire-transfer phish. At the same time, broad-based phishing campaigns using malicious attachments grew rapidly in late 2014, taking over much of the volume previously occupied by URL-based longline phishing campaigns.
- Emails with malicious URLs are being sent by trusted third parties (e.g., newsletter or opt-in marketing email with a link to a compromised legitimate site); instead of directly malicious URLs, cybercriminals are sending attachments instead.
- High volume of OWA credential phish: very easy to spoof these pages, and they give high-value results, can be broad-based or targeted.

Defending Against Attacks

Clearly, traditional defenses cannot keep up with attackers' continually evolving techniques. Links are arriving in messages that do not look like the messages that end users have been trained to recognize as phish, and existing defenses are not as effective at stopping them from getting to end-users.

So what is the answer? An axiom in American football is that it is more tiring to play defense than offense: the offense knows where he ball is going to go, while the defense is always reacting and chasing the ball. Rather than relying on your end-users to recognize and protect your organization from last year's attacks, use threat intelligence and Big-Data analytics to gain more insight into where the ball is likely to go and defend accordingly, conserving energy and resources.

To keep pace with these threats, organizations must also adopt defensive capabilities that can protect from campaigns using multiple tactics over multiple vectors, from email to social media and URLs, using malicious URLs, malicious attachments, and even text-based messages that carry neither a link nor an attachment. Advanced threat intelligence driven from a cloud-based global platform provides visibility into rapidly evolving threats and techniques, and can be effective as a defensive strategy when coupled with integrated threat management capabilities to mitigate the damage of new and emerging threats.

For CISOs, this means:

- Continue to emphasize the importance of email security and social media security
- Deploy defenses that use multiple, contextual big data and threat intelligence-based detection techniques including static, predictive, and browser path analysis as well as dynamic behavioral analysis
- Ensure layered security that incorporates automated threat response systems content control systems as well as next-generation detection, because someone will always click (and it only takes one).

An appropriate modern security solution must be able to provide the following:

- **Next-generation detection:** Advanced malware can evade antivirus and reputation filters to deliver banking Trojans, ransomware, and other malware. In order to detect advanced malware effectively—whether spread via spear-phishing emails containing a malicious attachment, watering hole URLs over email, or longline phishing campaigns — organizations need a malware analysis technology that employs a combination of sophisticated techniques to evaluate advanced threats.
- **Predictive defense:** Organizations should deploy solutions that leverage cloud-based Big Data analytics to predictively detect malicious URLs in unsolicited emails and block user clicks before they can lead to a compromise. These capabilities combine machine-learning heuristics to model email flow at a per-user level, and at a cloud-level across all traffic in order to block URLs even before they host active malware; with kill chain analysis and preemptive sandboxing to predictively determine what could likely be malicious—and take preemptive steps before any user has a chance to click and have their machine compromised.
- **"Follow-me protection":** Users are clicking everywhere, all the time, so organizations need comprehensive security whenever or wherever the user clicks by following email and checking for the URL destination's safety in real-time. The ideal solution leverages an agentless, cloud-based service with URL intelligence to protect users from malicious links in emails no matter when or where they click on that URL– while working remotely, BYOD, and more.
- **End-to-end insight:** Insight and actionable intelligence are essential to mitigating the impact of advanced threats. Organizations must have the ability to detect compromises and speed response and remediation of phishing and web compromise attacks by quickly identifying campaigns, targeted users, and potentially infected systems. Details of attacks, the size of the threat, specific users that were affected, and real-time notifications for potential incidents that require investigation should be available via a single pane of glass for Incident Response teams, enabling them to instantly verify, prioritize and contain advanced threats and targeted attacks detected by industry-leading security vendors, including situational awareness based on actionable threat intelligence and the ability to automate infection verification, threat containment.

To learn more about Proofpoint's specific solution, Proofpoint Targeted Attack protection, and how it can provide specific insights to you about your organization, please visit www.proofpoint.com/TAP or contact us at +1 (877) 634-7660.

More of our research at www.proofpoint.com/threat-insight

About Proofpoint

Proofpoint Inc. (NASDAQ:PFPT) is a leading next-generation security and compliance company that provides cloud-based solutions for comprehensive threat protection, incident response, secure communications, social media security, compliance, archiving and governance. Organizations around the world depend on Proofpoint's expertise, patented technologies and on-demand delivery system. Proofpoint protects against phishing, malware and spam, while safeguarding privacy, encrypting sensitive information, and archiving and governing messages and critical enterprise information. More information is available at www.proofpoint.com.

892 Ross Drive
Sunnyvale, CA 94089

1.408.517.4710
www.proofpoint.com