The Human Factor

How attacks exploit people as the weakest link in security

A Proofpoint White Paper

Most advanced attacks rely as much on exploiting human flaws as they do 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.

This paper uses original field research to provide insight on who's clicking, what they're clicking on, and when, where, and why the weakest link in security is all of us.

Executive Summary

In the last 12 months, 76% of IT security and operations staff stated that their organization had been impacted by malware that had evaded their existing Intrusion Detection and Antivirus solutions[i]. Another report found that 95% of targeted and APT-driven threats began with an email-based spear phishing attack[ii]. Socially-engineered, targeted, and more sophisticated email-borne attacks on organizations are now the dominant form of cyber-attack execution, and increasing in volume.

Most advanced attacks rely as much on exploiting human flaws as they do system flaws. They work because people click – and because Information Security teams typically lack sufficient real-time insight into who's being targeted and how, and thus can't effectively act to protect the organization.

Some percent of these attacks will be caught using secure email gateways, sandboxing, and other technologies. However, given the coordinated and distributed nature of modern attack techniques, such as Longlining, some threats will get through – and understanding the forensics of malware isn't enough to protect the organization.

In a longline attack, end user information about who is really being targeted, how frequently, who is clicking on threats, and what exactly are they clicking on is more crucial than forensics data in constructing effective defensive strategies. Yet few current security solutions provide such data (real-time or delayed), and IT has often been forced to rely on 'conventional beliefs' and reports from users which may be inaccurate or unreliable.

Proofpoint developed this report, **The Human Factor**, to explore this under-reported human aspect of threats and the risk InfoSec teams are dealing with based on data from our global enterprise customer base that are using Proofpoint Targeted Attack Protection.

The key insights are summarized here:

Who's Clicking

- **Every company clicks. On average, 10% of users are responsible for 100% of clicks within any given wave of malicious attacks on a given company. Industry best-in-breed companies are still clicking at over 1%.**

  Some organizations spend a significant effort on training their users and implementing best-of-breed traditional security defenses. These investments pay dividends in helping combat threats; however due to the unpredictable nature of users, and constantly changing landscape, things will typically get through and someone will click. Our data showed that click-rates for all companies observed were non-zero.

  Recommendation: User training is a necessary strategy and can pay dividends depending on the nature of the attack can pay dividends. But it is an insufficient strategy for dealing with such threats; technical and automated capabilities to minimize risk from user clicks must be explored.

- **Everybody makes mistakes. While repeat-clickers account for the majority of clicks on malicious links, 40% of clicks are typically from one-off clickers.**

  Conventional belief has been that dealing with repeat clickers is the key approach to maximum mitigation of enterprise risk. However, our analyses indicated that this still means a large number of clicks, 40% on average, still remain at large.

  Recommendation: Enterprises should invest in training users, especially repeat clickers. However, since the one-off clickers can vary with each wave and account for a large quantity of risk, solutions with technical capabilities to predict and detect threats, as early as possible, are critical.

- **It's everybody's problem. Staff is targeted 2x as much as Middle Management, 1.3x as much as Executives. Further, Staff is 2x more likely to click on threats they receive.**

  Phishing attacks on executives and C-level employees of organizations receive a lot of attention, and conventional belief is that targeting them makes sense as executives have more keys to the enterprise kingdom. However, given attackers can penetrate an organization's defenses anywhere and then attempt to move laterally to achieve their goals, it seems they tend to target non-executives much more given the higher chances of receiving clicks.

  Recommendation: InfoSec security posture needs to pay special attention to non-executive employees where most of the compromises will originate, and must use a set of tools that can give appropriate visibility into who is clicking, when, and how often, besides just the malware forensics.

- **Everybody gets attacked. While the top most targeted industries included Pharmaceuticals, Hospitality, and Insurance when measured on an average attacks per user basis, even the least-targeted industries received a significant volume of attacks.**

  Traditionally Finance and Healthcare are believed to be the most attacked industries. However, our research showed that in terms of volume of threats received other industries seem to experience a higher attack volume. Additionally, within each industry, the variance based on, size of company is minimal, debunking the notion that size of company results in more average number of attacks experienced per user.

  Recommendation: All industries are targeted to a different extent, by different types of attackers, with different motives. It is key to understand the specific nuances of an organization's specific situation, and monitor trends as it relates to specific user insight.

What are people clicking on

- **Social Connectivity Drives Clicks. Top lures include Social Networking communications, Financial Warnings, and Order Confirmations but the LinkedIn Connection Invitation gets 2x more clicks that any other template.**

  Users can tell-apart spam annoyances from useful email, however, it is getting more and more difficult for users to tell apart phishing email as unsolicited email and notifications from popular services are common. Given the nature of professional social networking, and specifically the popularity and trust enjoyed by the LinkedIn brand, it is frequently used as a malware campaign template and serves its purpose in enticing users to click.

  Recommendation: Since LinkedIn is the prominent social network that users typically allow into their corporate email account, users must be made more aware of the possibility of threats masquerading as accounts notifications from LinkedIn and others, and to look for tell-tale phishing signs before clicking on notifications. Additionally, using security solutions that predictively seek out anomalies in email and sandbox URL destinations is key to minimizing risk.

When do people click

- **Long-tail of Clicks Past Delivery. Most malicious messages are sent to users during working hours, and more than 1 in 15 user clicks on malicious links are seen more than a month after the threat was delivered.**

  Conventional belief is that attackers target users at specific times such as late evenings, right before weekends, or even during weekends. The logical explanation is that this is when users are less alert or are likely to be caught checking email while not on the corporate network and under on-premise security scrutiny. Our analyses of the data suggest the opposite, i.e. that most attacks are aimed at enterprise users during all times within working hours. Additionally, there is a long-tail of risk for enterprises where users are still clicking on threats, even more than 30 days after delivery.

  Recommendation: Enterprises must ensure that a retroactive and longer-term protection technique is used which can extend to the entire threat lifecycle, regardless of when a threat is delivered and when a user clicks.

Where do people click

- **Mobility matters, Mobile Devices less so. 90% of total clicks on malicious URLs come from user's computers; 20% of those clicks happen when those computers are outside of the corporate firewall. Only 10% of total clicks from mobile devices.**

  Recent estimates have indicated that 65% of email is accessed first on a mobile device[iii], and intuition suggests this would mean higher click-rates on URLs within emails coming from mobile devices. However, this doesn't seem true for the enterprise users specifically, and mobile device-related threats are still an emerging issue in comparison. Additionally, with 1 in 5 clicks coming from off-VPN devices[iv] this further complicates the security issues of dealing with clicks from personal computers.

  Recommendation: The significant number of clicks from personal computers compared to mobile devices should help guide security investment strategy. Consider technical solutions that provide a follow-me approach to protection, regardless of device and regardless of whether the device is on or off the corporate network.

Why do people click

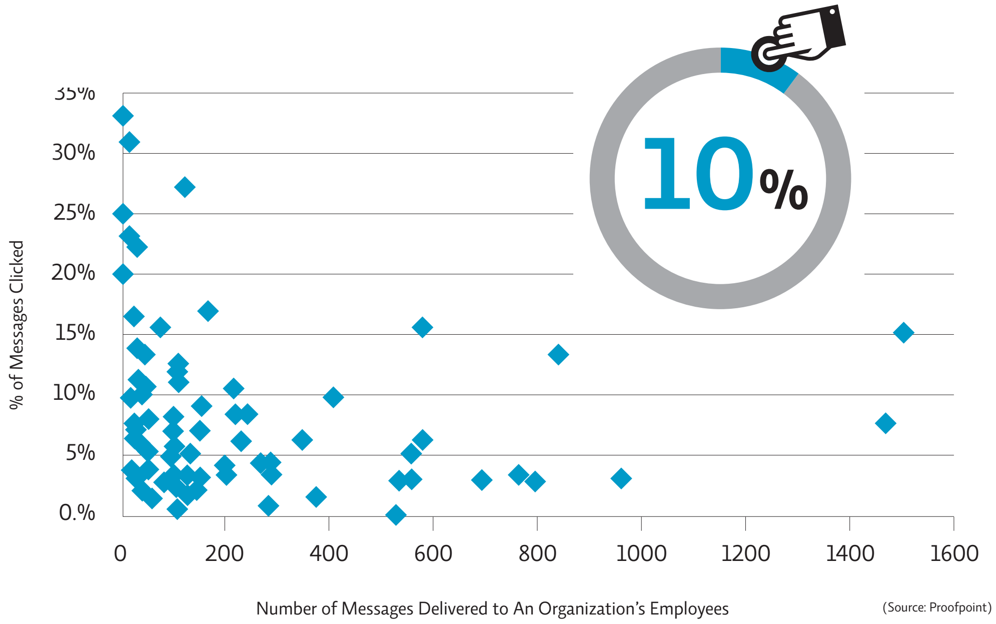
- **Email volume conditions humans. Receiving too few or too many malicious threats results in a higher user click-rate. After 100 malicious messages odds of clicking level-off at 60% likelihood.**

  IT teams have been trained typically to assume that users never learn from mistakes. That is, users will be users. However, the data suggested that there is in fact a clear relationship between the number of malicious messages a user receives and how many of those messages he or she clicks, implying some element of user learning and awareness.

  Recommendation: Since users are conditioned to click, the focus of enterprises should be on security controls that can provide visibility into those situations for proactive action and quicker incident response.

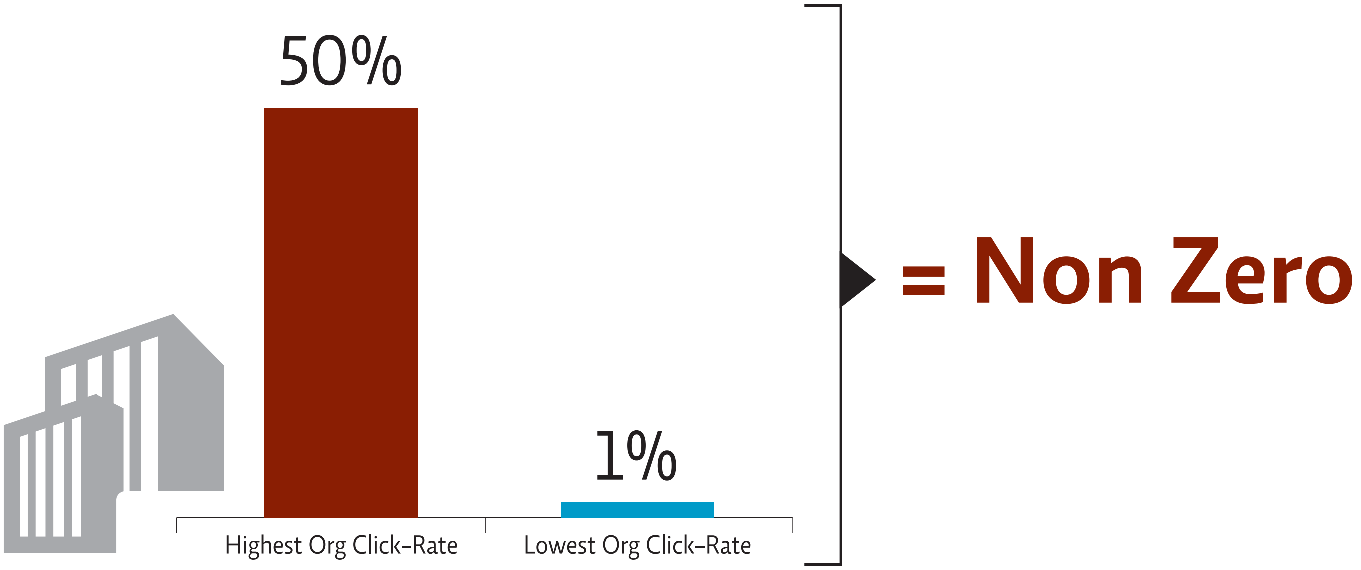
To read more in-depth details and methodology of this and all our other research, visit: www.proofpoint.com/threatinsight

Who Clicks on Malicious Messages: Some or All Organizations?



(Source: Proofpoint)

10 in every 100 users attacked at a given organization clicked on the malicious URLs in the messages received as part of a typical campaign.



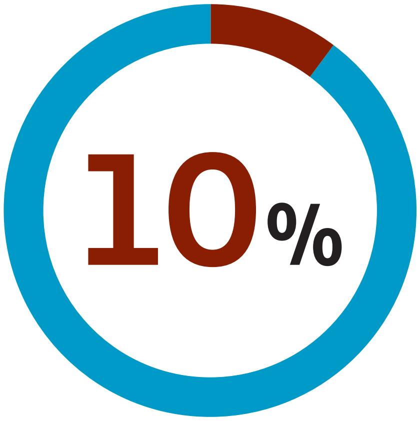
(Source: Proofpoint)

What this means

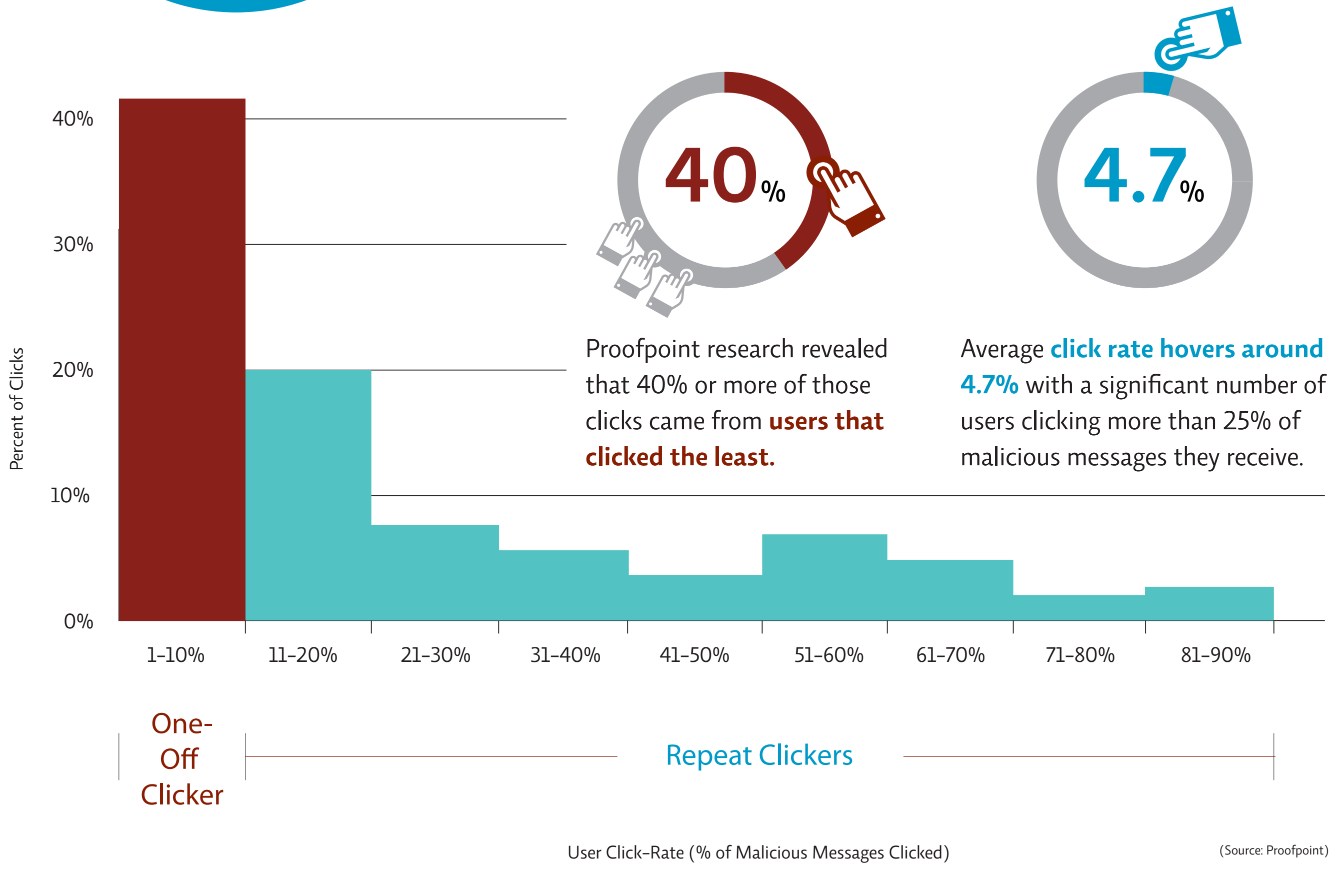
1. Even the best-in-class organizations had a non-zero click rate = everyone clicks.
2. An atypical campaign can see even more varied results across companies.
3. User training is a necessary but insufficient strategy to dealing with such threats; technical and automated capabilities to minimize risk from user clicks must be explored.

For more details on this analysis: www.proofpoint.com/threatinsight/humanfactor1

Who Clicks on Malicious Messages: One-Off or Repeat Clickers?



The share of users that are responsible for **100% of all clicks** and incidents.



Proofpoint research revealed that 40% or more of those clicks came from **users that clicked the least.**

Average **click rate hovers around 4.7%** with a significant number of users clicking more than 25% of malicious messages they receive.

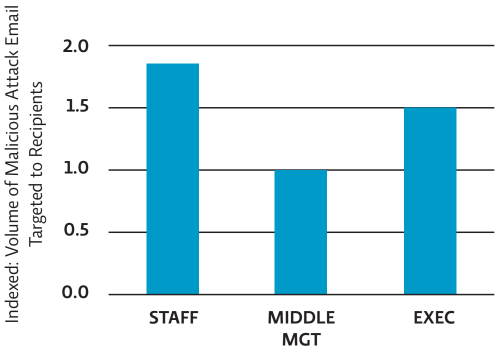
(Source: Proofpoint)

What this means

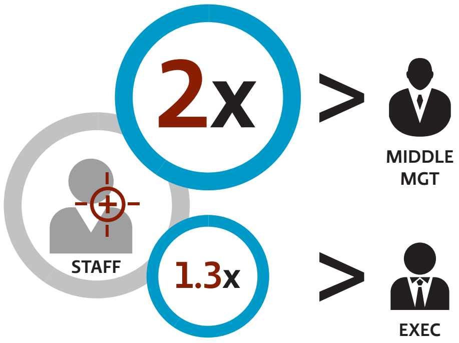
1. Attackers are opportunistic in who they go after to achieve their end goal – there are frequent clickers, but even those less frequent need predictive defenses.
2. Repeat Clickers aren't the most significant problem for InfoSec; training or disciplinary action against them is not an effective strategy to solve the problem.
3. No employee is immune – Eventually, everyone clicks. Having visibility of who is clicking, when, and on what is key to identifying at-risk users.

For more details on this analysis: www.proofpoint.com/threatinsight/humanfactor2

Who Clicks on Malicious Messages: Executives or Staff?

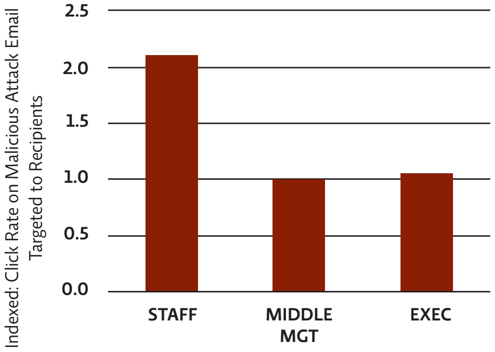


(Source: Proofpoint)

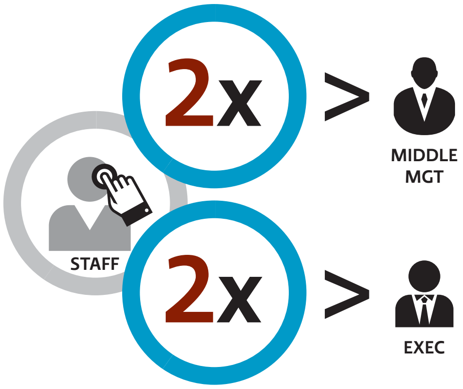


TARGETED MALICIOUS MESSAGES

Staff is typically targeted with malicious messages at almost twice as much as Middle Management; 1.3 times as much as Executives.



(Source: Proofpoint)



CLICKS ON MALICIOUS MESSAGES

Staff clicks on malicious messages almost twice as much as Middle Management and Executives.

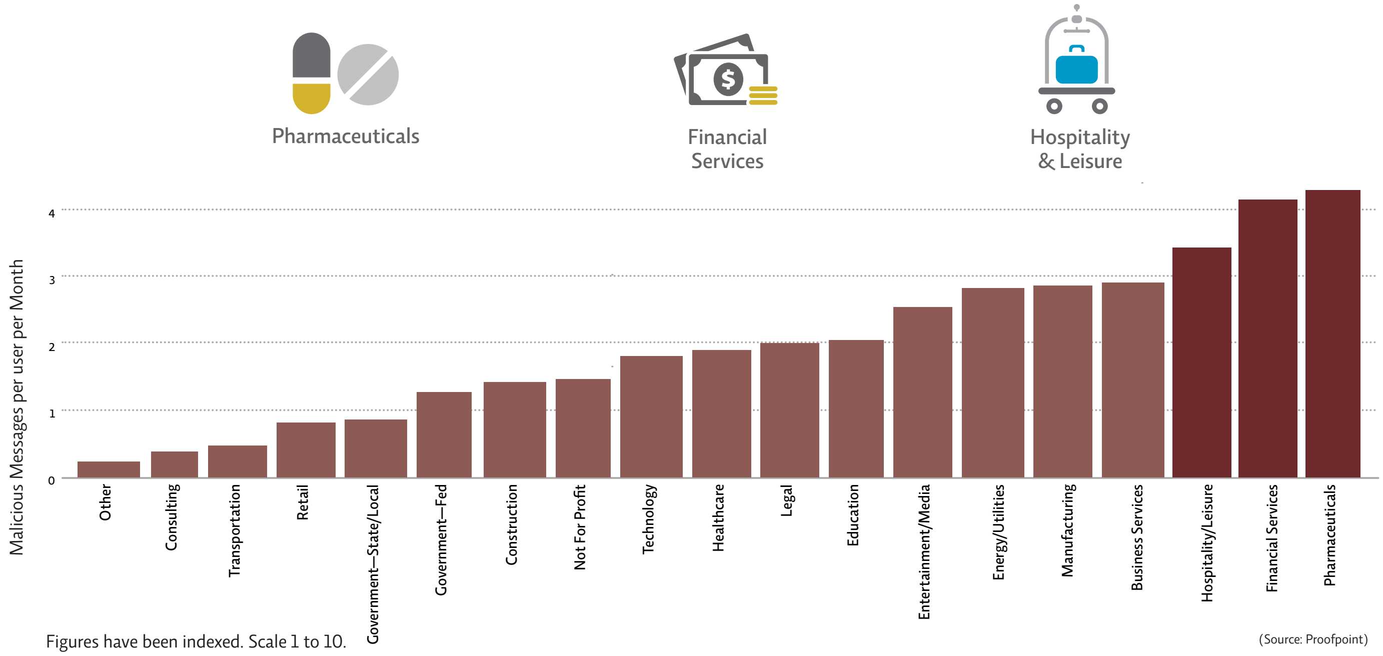
What this means

1. Staff seems to be targeted due to higher susceptibility to threats. Attacker are likely able to move laterally within the organization from that user's machine to achieve their objectives.
2. Given numbers of Staff-level employees typically, IT faces 2x likelihood they'll receive malicious email, times 2x likelihood they'll click = potentially hundreds of breaches
3. Strong indication that additional defenses to protect Staff are necessary, and to build security models using Big Data that can detect risky emails and predictively catch-before-click.

For more details on this analysis: www.proofpoint.com/threatinsight/humanfactor3

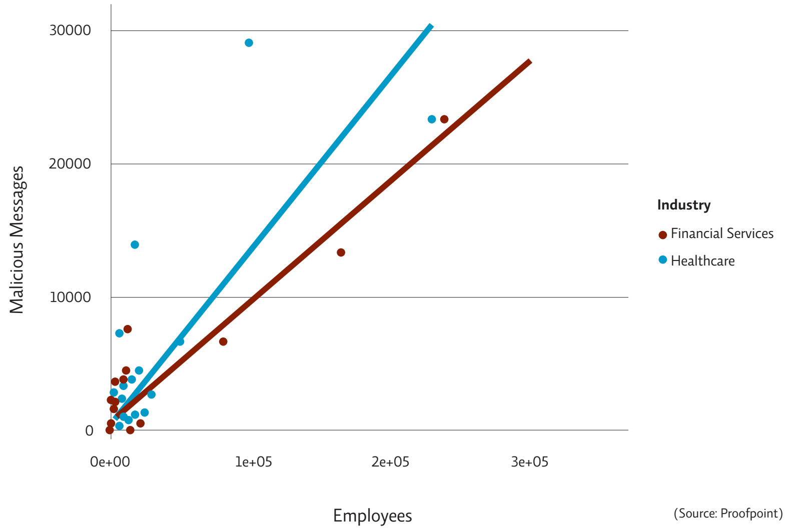
Who Clicks on Malicious Messages: Specific Industries or Specific Company Size?

TOP ATTACKED INDUSTRIES:



Figures have been indexed. Scale 1 to 10.

(Source: Proofpoint)



(Source: Proofpoint)

Significantly more linearity in terms of attacks seen by industry.

Less differentiation by size of company than by industry.

What this means

1. Certain industries are targeted more often than others; however the industries that see higher volume of threats are different than conventional opinion.
2. Number of employees tends to matter much less than industry of an enterprise when it comes to number of threats seen per employee.
3. Users across companies in different verticals are the targets that attackers use to drive success of their attacks – it is key to understand the nuances of the organization's specific situation, and monitor trends as it relates to specific user insight.

For more details on this analysis: www.proofpoint.com/threatinsight/humanfactor4

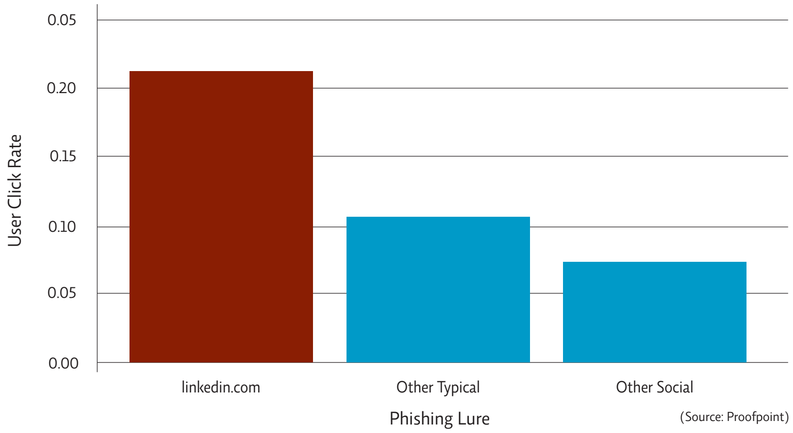
What Are Users Clicking On?

Most Effective Attacker Templates That Get Users to Click

SOCIAL NETWORK COMMUNICATION

FINANCIAL ACCOUNT WARNINGS

ORDER CONFIRMATION



(Source: Proofpoint)

2X CLICK RATE

Click-rates on malicious campaigns using **LinkedIn templates are ~2x that of any other seen by Proofpoint in the recent past.**

4X CLICK RATE

Click-rates on malicious campaigns using **LinkedIn templates are ~4x that of campaigns that used other social network brands**.

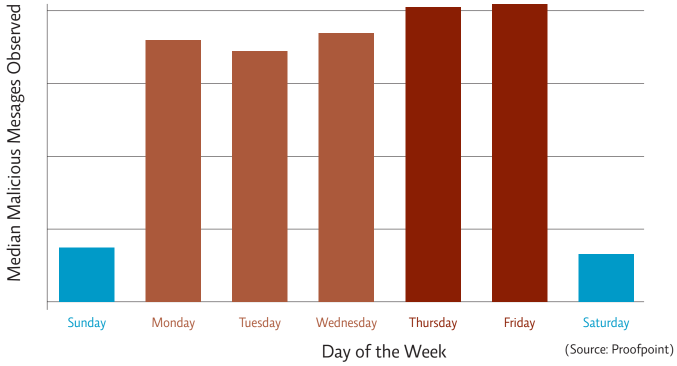
Users click on malicious LinkedIn invitation templates **8x more than they click on all types of LinkedIn emails and notification templates.**

What this means

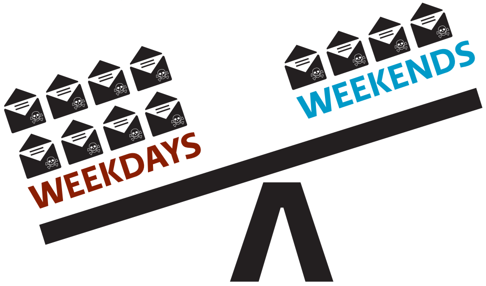
1. Attackers are familiar with brands that drive user clicks, and evolve them as necessary. LinkedIn is one such selection.
2. Attackers are able to get 50+% of corresponding legitimate click-through rates.
3. It's becoming increasingly difficult for users to distinguish good from bad – training is necessary, but not sufficient. Detection techniques that don't rely on users are key.

For more details on this analysis: www.proofpoint.com/threatinsight/humanfactor5

When Do Users Get Attacked & Click?

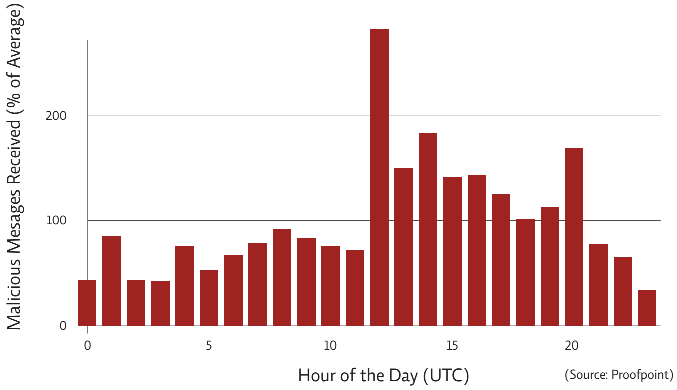


(Source: Proofpoint)



Most malware threats come into enterprises during the weekdays Vs. weekends.

Thursdays and Fridays are nearly tied for the **most malicious days of the week**

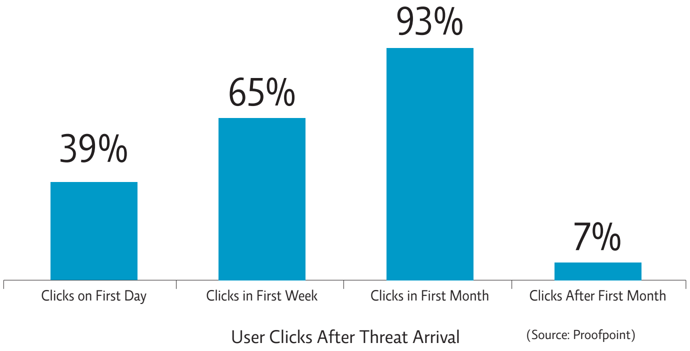


(Source: Proofpoint)

8AM –4PM EST PEAK

Most malicious messages that are part of a campaign are during working hours.

For US enterprises, these threats **peak from 8am Eastern Time to 4pm Eastern Time.**



(Source: Proofpoint)

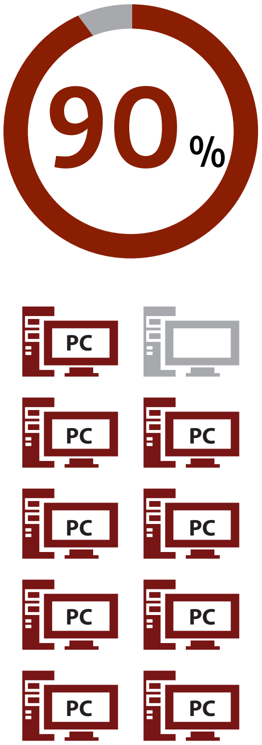
7% of user clicks are observed months after delivery of threats

What this means

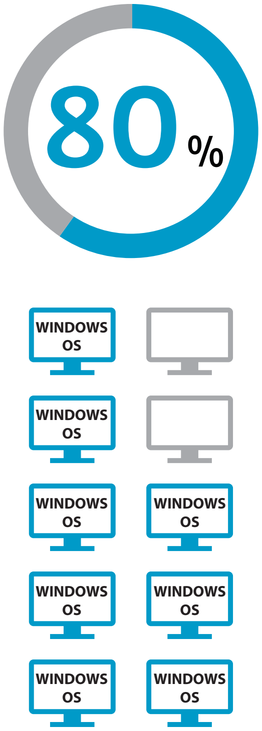
1. Threats arrive around the clock, all days of the week, all hours of the day.
2. Campaign-based threats do have a pattern, but targeted threats do not.
3. Half-life for a threat can be quite long, as users can click months after delivery – this fact creates a need for retroactive and long-term protection that extends to the entire threat lifecycle.

For more details on this analysis: www.proofpoint.com/threatinsight/humanfactor6
www.proofpoint.com/threatinsight/humanfactor6a

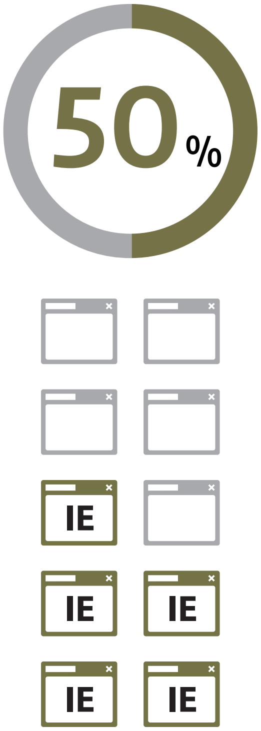
Where Do Users Click From?



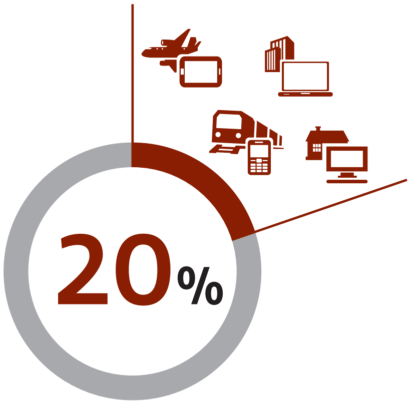
90% – Of user clicks on malicious links come from **personal computers and laptops.**



80% – Of user clicks on malicious links are from **Windows OS** specifically.



50% – Of user clicks on malicious links are from users that are using **Internet Explorer**.



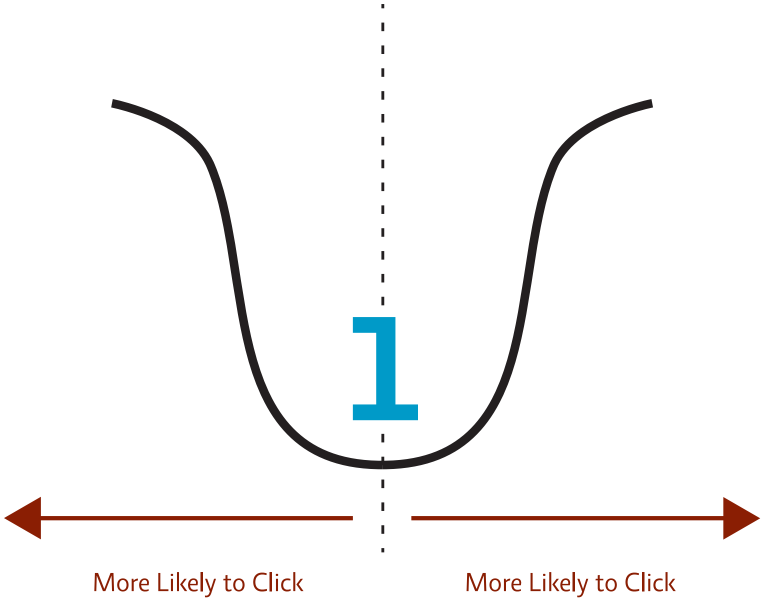
20% of Clicks Come From Off-Network Devices

What this means

1. Majority of clicks on threats today come from personal computers, not mobile devices.
2. Mobile is still an emerging problem from a user-behavior perspective, but requires coverage through a follow-me security approach to combat advanced threats regardless of device used for access.
3. Windows and Internet Explorer on PCs are still the dominant enterprise user preference; next generation threat detection to reveal these threats predictively (eg, to detect pre-click) can mitigate risks.

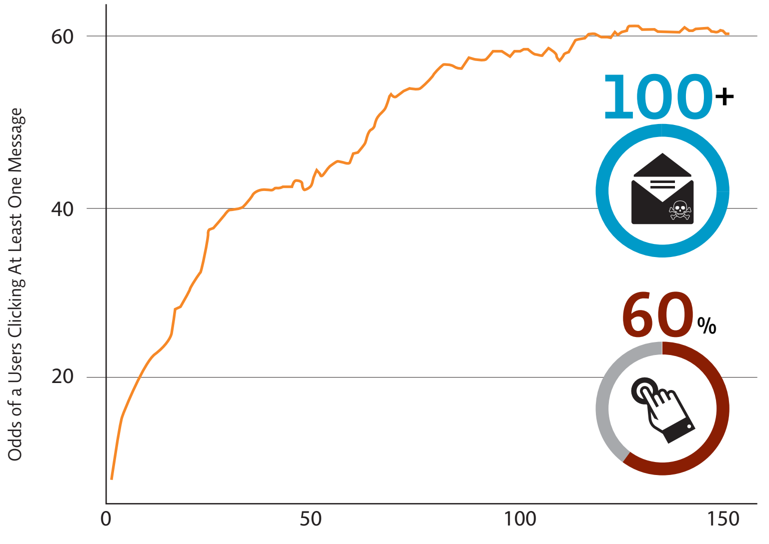
For more details on this analysis: www.proofpoint.com/threatinsight/humanfactor7

Why Are Users Clicking In Spite of Training?



Users in companies that receive on average 1 malicious message per user per month are less likely to click.

Anything received more or less than 1 on average = more likely to click!



(Source: Proofpoint)

As users receive **100 malicious messages or more**... the **odds of the user clicking a message increases to 60%**, and stays at that level regardless of more messages received.

What this means

1. There is an inherent learning curve for employees who receive phishing messages.
2. Too many phishing messages is too bad, too few is too bad as well when it comes to 'user learning' – some enterprises have statistics where high click-rate users cause just as many incidents as low-click rate users
3. User behavior is not consistent and predictable; security architecture needs to account for this through cloud-based scale and malware analysis techniques that can cover everything and everyone.

For more details on this analysis: www.proofpoint.com/threatinsight/humanfactor8

Defending Against Attacks

Security is an ever-shifting challenge – and thus never perfect. Attackers constantly change their tactics to bypass traditional and on-premise signature-based solutions. With the help of polymorphic malware, traffic distribution systems, and other methods that incorporate cryto-tools and next-generation exploit kits, attackers have recently had some increased success bypassing antivirus, IDS/IPS, secure email gateways, secure web gateways, and more active technologies. Even at the height of effectiveness, a 99.99% effective filter still lets through some of these threats. In Longlining attacks consisting of millions of emails, that volume of threats getting through in a short amount of time can be significant.

Based on Proofpoint's experiences with enterprise customers of all sizes, even the best companies with large investments in security and training have their users clicking on malicious messages both on and off the corporate network, **making gateway-only security protection ineffective.**

The implication is that Enterprises must enhance overall security architecture with tools for both next-generation threat detection and associated post-delivery insight, as well as different personnel-based approaches to security, such as more training.

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

- **Next-generation Threat Detection:** advanced malware detection that can use cloud-based dynamic malware analysis and sandboxing technology to detect URL and attachment threats that are targeted at enterprises and missed by signature and reputational-based security solutions.
- **Predictive Defense:** analyses that leverages known historical and behavioral patterns to weed our anomalies and predict whether a message could become a threat. This predictive defense helps to identify threats in real-time and proactively block users when they click, thus minimizing remediation need.
- **"Follow-me" Protection:** ability to provide coverage to users whether or not they are accessing content on or off the corporate network, and regardless of which device they are using.
- **End-to-End Insight:** ability to get insight into which users are targeted, who is clicking, who is protected, who needs remediation, and forensics to understand the nature of the threat.

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 proofpoint.com/threatinsight

[i] Ponemon Institute study, "The State of Advanced Persistent Threats", Dec 2013

[ii] 2013 Verizon Data Breach Investigations Report

[iii] "65% of all email gets opened first on a mobile device — and that's great news for marketers" - Venturebeat.com, January 2014

[iv] http://blog.proofpoint.com/2013/04/longline-phishing-infographic-how-industrial-scale-phishing-attacks-work.html