Lookout®

RESEARCH REPORT

The State of Mobile Phishing

Understanding current phishing trends is essential to effectively protect your mobile and remote workers

Contents

Executive Summary

The mobile security landscape is constantly evolving. With more reliance than ever on mobile devices for both personal and business use, the entire world is looking at mobile accessibility as the vehicle to higher connectivity and better productivity. Of course, the shift to mobile reliance comes with heavy risks, but the *Verizon Mobile Security Index 2020* report shows that despite the risk, 43% of organizations are still cutting corners on security, even with 39% suffering from a security compromise.

Malicious actors have taken note of how reliant we are on mobile devices. From their perspective, mobile phishing is often the cheapest way to compromise an individual or an organization. Traditionally, people think this can only happen over email, but accordingly to Verizon, 85% of mobile phishing happens outside of email apps. Combining the fact that over 96% of mobile users have communication or social apps on their phones and organizations are sacrificing mobile security puts everyone at risk.

Mobile phishing is a global problem. Across all geographies and industries, there is a steady increase in the rate of both consumer and corporate users encountering mobile phishing attacks. Smaller screens and shortened URLs make it harder to spot a phishing attack, so as the attackers become more savvy in creating near pixel-perfect imitation pages and leveraging social engineering, and taking advantage of smaller screens to make it harder to spot a phishing attack, the risk is dramatically increasing.

The financial risk of falling victim to a phishing attack can be devastating to an organization. For a large multinational company, they could be looking at hundreds of millions of dollars in losses from a successful phishing attack. Even for smaller organizations, like a regional healthcare system, the risk still falls in the tens of millions of dollars.

Mobile phishing is a problem that can no longer be ignored, no matter what part of the world or industry an organization operates in. Considering the consistent growth in mobile-focused phishing campaigns, encounter rates, and tap rates where the target actually follows the link, organizations must understand the landscape and put proper measures in place on iOS and Android devices to protect the company and its customers from a detrimental data breach.

Introduction

Phishing is the primary way malicious actors trick people into unknowlingly giving up their login credentials or downloading malware, which ultimately can allow attackers to access their organization's network and steal sensitive corporate data. Phishing links no longer simply hide in email, but in messaging platforms, social media, and even dating apps.

How did the industry get to this point? The State of Mobile Phishing report presents how the industry arrived at the current state of phishing, highlights emerging trends, and recommends effective ways to protect your mobile and work-from-home employees.

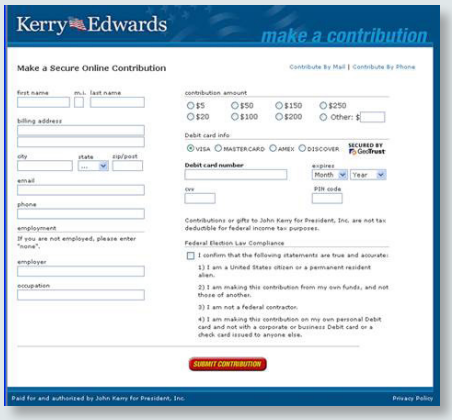
Origins of phishing

Phishing has long been one of the most effective ways for malicious actors to steal data from unsuspecting victims. In fact, 91% of enterprise cyberattacks start with a spearphishing email, in which a particular individual is targeted and tricked into granting the attacker access into corporate infrastructure.

Phishing's origins lie in email, which was one of the original ways for cyberattackers to deliver malware to victims. In 2000, the infamous ILOVEYOU virus was the first documented use of email for mass distribution of a virus. Soon after, domain spoofing emerged as an attack vector by which a malicious actor could make it look like the email was coming from a particular organization or person, and convince the victim to transfer funds, share login credentials, or give up other data as part of an online scam.

A couple years later, these scams were recognized as a viable way for cyberattackers to target a large group of individuals at low cost. In the early 2000s, phishing became an industry term when trade publications such as *PCWorld* started referring to these email scams as phishing attacks.

By 2004, phishers were experiencing massive success because victims were uneducated and under-secured. Between May 2004 and May 2005, it's estimated that U.S. businesses lost roughly $2 billion to phishing attacks. At the consumer level, it's estimated that 1.2 million computer users in the U.S. lost about $930 million to phishing. Across the pond, the Financial Services Authority's crime team reported an 8,000% growth in phishing campaigns in the UK alone. Notable early campaigns that were characterized as phishing included ones that targeted Visa credit card customers, Citibank customers, and supporters of John Kerry's presidential campaign.



A phishing email that looked like it came from John Kerry's brother asked for financial support and led to a fake donation page.

Security solutions started to address phishing and became more advanced, but so did phishing campaigns. Impersonating a particular individual or organization became common practice, and distinguishing email with real and fake identities became increasingly difficult.

Cybersecurity leaders quickly realized that it only took one employee being phished to launch them into a world of serious consequences — both internally and externally. The highest risks were in highly regulated industries with heavy compliance standards such as financial services and healthcare, with potential secondary fallout in the form of damaged brand reputation or loss of business.

The battleground for phishing shifted as more individuals and organizations became reliant on mobile devices and attackers expanded phishing well beyond email into third-party messaging platforms, personal apps, and productivity suites. The industry change makes sense. Over the last few years, more employees wanted the option to work as effectively from their mobile devices as they could from the office, with a 44% growth in remote work from 2014-2019. From the organization's perspective, enabling mobility is smart because it keeps productivity high for traveling or remote workers who might not otherwise have access to internal resources they need to get work done outside the four walls of the office. More recently, in response to the COVID-19 pandemic, working from home became a widely adopted practice for an unprecedented number of people to keep business moving during the period of social distancing. This affected many employees who had never previously worked from home in the past, which further increased risks to organizations.

However, as the shift to a modern remote workforce takes place, many organizations put mobility enablement ahead of security. Since mobile is a relatively new vector in the threat landscape, most IT and security teams aren't part of the project plan to shift to mobile, which negatively affects the company's overall security posture. Malicious actors know this, and are taking advantage of the gap in security to feast on uneducated mobile users who don't know how to recognize a mobile attack.

In the case of phishing, distinguishing between real and fake on a mobile device is exponentially more difficult for the typical user, and is leading to an increase of mobile-focused phishing attacks around the world.

What is mobile phishing?

Early phishing protection tools focused primarily on email. This made sense, as it was the only way for bad actors to blast a phishing message to a massive population connected to the Internet. Email also provided a route to try a wide variety of campaigns, as proven by the early banking and political messages we looked at earlier. Looking at email phishing as a numbers game, a cyberattacker could assume a reasonably high return on a relatively low investment of both money and time with simple phishing campaigns.

As email security solutions became better at detecting phishing campaigns, bad actors needed to innovate to keep their campaigns successful. With the smartphone revolution occurring nearly in parallel as the escalation of the phishing war, focusing on mobile was the sensible next move for phishers. Since shifting their focus to mobile, phishing has evolved into an effective means of attack by leveraging new channels like SMS (smishing) and social engineering on social media platforms.

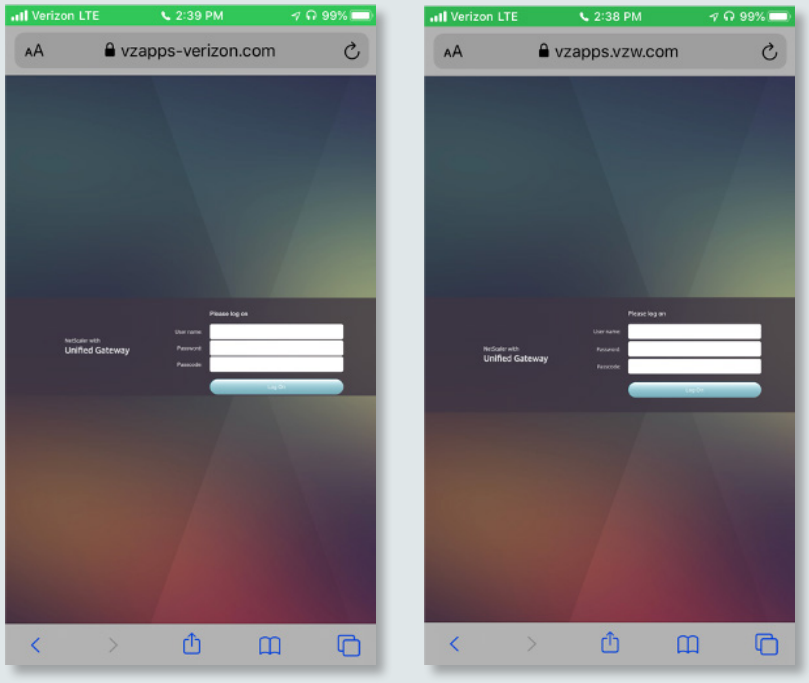
Phishing via messaging: A fake bank security text, free data offer using the target's name, and a social engineering attack in Facebook Messenger.

How is mobile phishing successful?

Phishing attacks on mobile devices have very high success rates because of how difficult it is to spot the tell-tale signs that people recognize on a laptop or desktop PC screen. Smaller screens, the speed at which we operate with mobile devices, and the fact that most users don't know how to preview a link on mobile before opening it can seriously reduce one's ability to identify a mobile phishing attack.

In addition, businesses are adopting a Bring Your Own Device (BYOD) model for their employees, which enables them to use personal devices as work devices and access all corporate data from those devices. Gartner predicts that "By 2022, 75% of smartphones used in the enterprise will be bring-your-own-device (BYOD), up from 35% in 2018." This shift means more people will use a personal device to access corporate data, which could lead to more careless data handling, extensive app permissions being granted accidentally, and greater risk to the organization if the right security measures are not in place.

Below is an example of a mobile phishing campaign targeting Verizon employees side-by-side with the legitimate mobile screen that the cyberattacker has mimicked. Targeting employees can be a highly effective way to get access to internal corporate data and infrastructure, and this attacker knows that it only takes one person to fall for their attack. The attacker could deliver this campaign in a number of ways, since it's simply a shared URL. Considering that the targets are internal employees, the attacker could have delivered it in a message impersonating a C-level executive, sent an SMS blast to phone numbers with area codes where Verizon employs a large percentage of people, or even targeted specific individuals with social engineering on personal platforms.



A fake Verizon employee login portal (left) versus the real one (right). Source: Lookout

As shown, the attacker did a very good job imitating the user interface (UI) of the web page, and likely chose a simple login page with very few elements on purpose. In addition, the attacker used a URL that looks perfectly legitimate, and likely wouldn't throw a red flag in the victim's eyes.

Considering how programmed people are to quickly enter login credentials on a mobile device, the odds are very low that the victim will take the time to observe the entire page that looks like the one they always log into.

This attack is the perfect example of how an attacker can use phishing for corporate credential harvesting. As one of the main targets of an enterprise-focused phishing attack, leaked login credentials can be detrimental to the organization as a whole, especially if it's an employee with higher levels of privileged access, such as access to assets like financial records, research, or customer data.

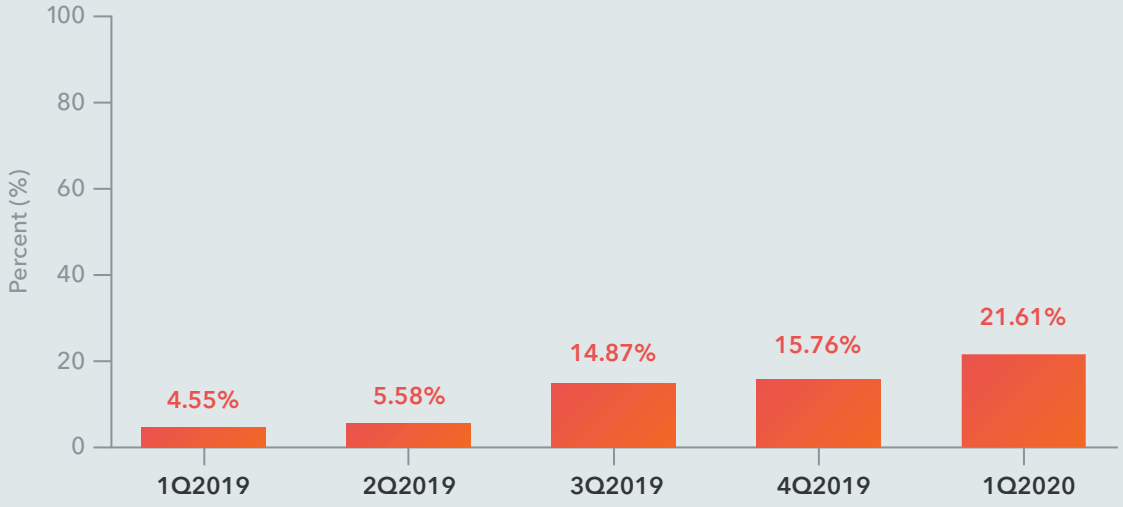
Mobile phishing is successful because employees are allowed to use their own devices in the workplace, attackers can target large groups at one time using phone numbers in a particular area code numbers, attackers can duplicate UIs to near pixel-perfect likeness, and users are not educated on how to recognize a phishing attack on their device as well as they are on their computer.

Phishing encounters are a global occurrence

Mobile phishing campaigns happen all over the world. As shown in the map below, countries in every region of the world are dealing with this problem. The data behind this map shows the 2019 encounter rates of all countries with customers using phishing protection on their mobile devices. It should come as no surprise that this problem exists across the globe.

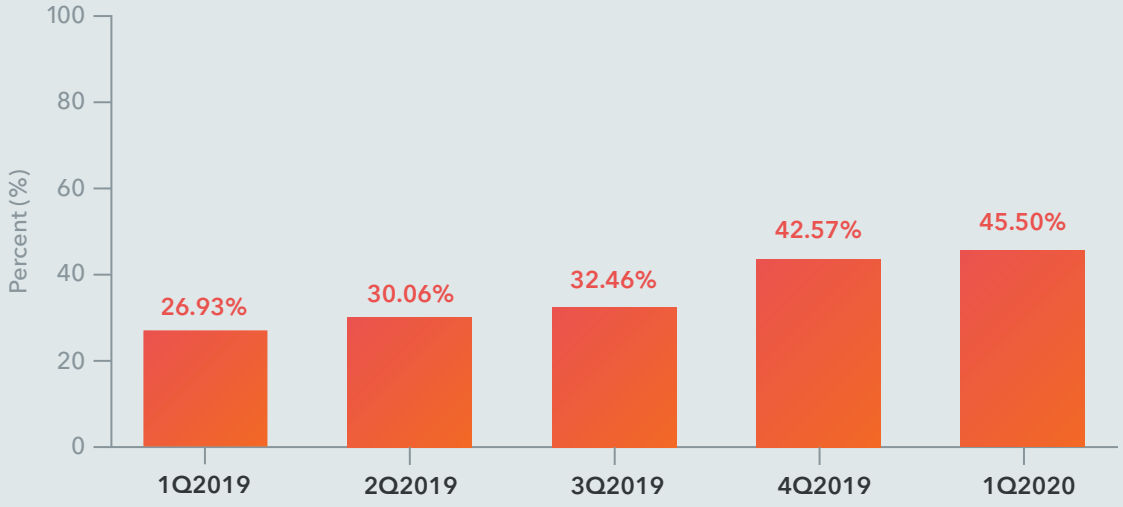
Mobile phishing encounter rates around the world in 2019. Source: Lookout

Quarter over quarter, there is an upward trend in mobile phishing over the last 15 months. Most notably, there's almost a 37% jump from 4Q2019 to 1Q2020. This is largely attributed to phishing campaigns centered around COVID-19, and shows that malicious actors take advantage of current events to phish victims.



Enterprise phishing encounter rates by quarter in 1Q2019–1Q2020. Source: Lookout

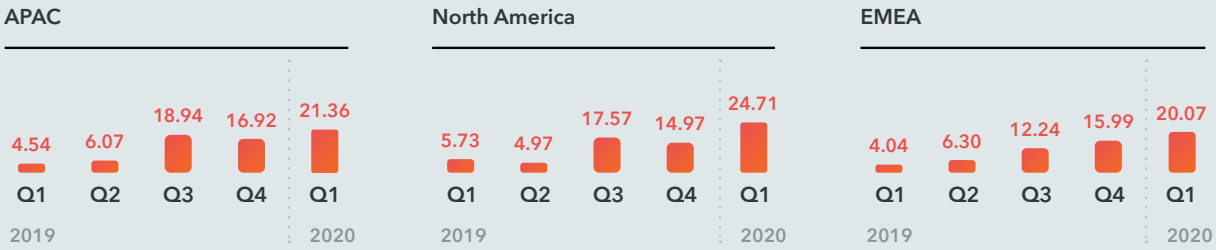
On consumer devices, there was a similar trend at greater scale. While these two percentages are very different, the increase in BYOD in the enterprise, forecasted by Gartner, will likely increase the enterprise encounter rates as the personal habits of BYOD users will likely remain unchanged, even with the added responsibility of using their personal device to access corporate data. As a result, the risk to enterprises will rise in coming years.



Personal phishing encounter rates by quarter in 1Q2019–1Q2020. Source: Lookout

Broken down by region, it becomes clear that mobile phishing is a consistent global threat. One might think that the threat would be higher in less technologically advanced regions where users have not been trained to spot the attack or don't have access to the technology to keep up with the bad actors; however, it's obvious that everyone is equally vulnerable to encountering a mobile phishing attack, as demonstrated below.

2019 Enterprise Mobile Phishing Encounter Rates by Region (Percent %)



Enterprise mobile phishing encounter rates by region. Source: Lookout

For enterprises, every industry is targeted by phishing attacks in one way or another. Unsurprisingly, because of the high value of their resources, organizations in highly regulated industries make up most of the top five targeted verticals affected by mobile phishing in 4Q2019.

The top targeted industries are also highly regulated. Source: Lookout

No matter which way you look at it, mobile phishing is a global issue that can no longer be ignored. Individuals and large enterprises alike must do their part to ensure mobile devices are secure. From the attacker's perspective, they can have success targeting both individual consumers and enterprises. As shown below, the success of those campaigns tends to fall off precipitously for enterprise users after initial effectiveness. By looking at the tap rates of enterprise users actually engaging with a phishing URL, it becomes clear that those users quickly learn from their mistakes after the initial engagement with a phishing link on their company-owned device or personal device they use for work.

However, consumer device users seem to not care as much. Since the device they're using isn't tied to corporate data and infrastructure, being blocked from a malicious URL is more of an inconvenience. It's interesting to observe that corporate and consumer users have almost polar opposite habits in this case:

Product Line	Platform	1	2	3-5	6+
Enterprise	Android	44.4%	18.2%	21.7%	15.7%
	iOS	46.5%	19.6%	20.4%	13.5%
	Total	45.8%	19.2%	20.8%	14.2%
Consumer	Android	22.0%	13.7%	23.2%	41.1%
	iOS	20.4%	13.1%	22.3%	44.2%
	Total	21.6%	13.6%	23.0%	41.8%

Phishing in 2019 broken out by the number of encounters per user. Source: Lookout

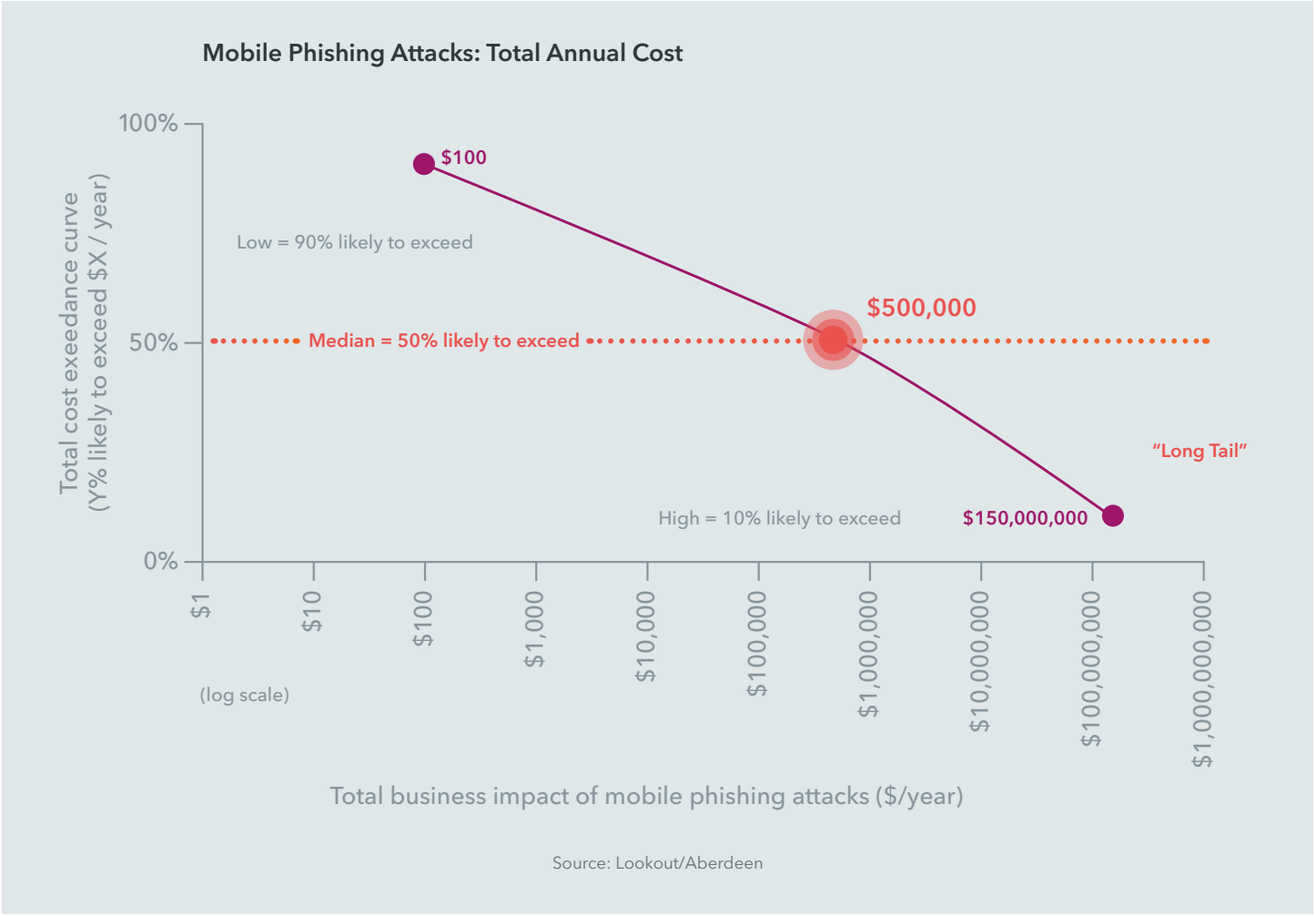
What's the potential financial risk of phishing?

Security risks are always going to be an issue for organizations of all sizes across the globe. For that reason, the biggest concern for an organization is the financial risk to the organization's bottom line.

Below are three examples that show the potential financial impact of a phishing attack against organizations of various sizes and industries taken from the Phishing Risk Assessment tool designed by Aberdeen. To assess the risk of mobile phishing to an organization, there are a number of data points factored into these assessments including number of mobile devices, the mix between Android and iOS, whether the organization uses a Mobile Device Manager (MDM), and most importantly how many data records that organization possesses.

Example A: Nationwide healthcare system

In this example, we look at a large enterprise organization that's managing 50,000 devices with an MDM. The company possesses roughly 100 million data records and has a 50/50 split between Android and iOS devices. This scenario would be characteristic of a nationwide healthcare organization that operates hospitals and care centers.



Source: Lookout/Aberdeen

Based on: 50,000 mobile devices | 50% iOS 50% Android | 100,000,000 Records

Encounters: Minimum: 4,400 devices | Max: 23,760 | Median: 13,570

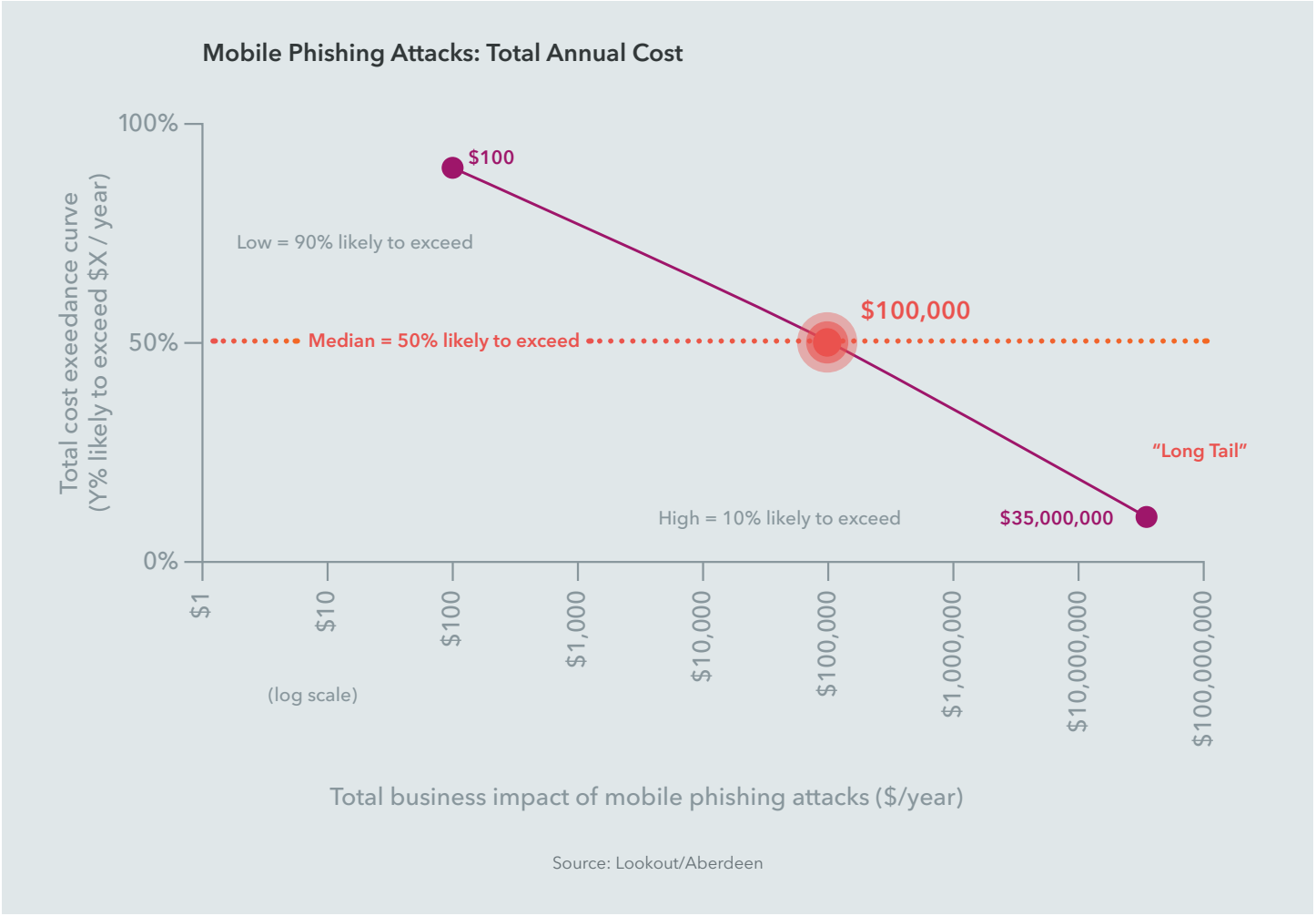
Clicks: Minimum: 1,760 | Max: 12,760 | Median: 6,640

Median Impact: $500,000/year

Maximum Risk: $150,000,000/year

Example B: Large manufacturer with field workers

In this example, we look at an organization that's managing 10,000 devices with an MDM. The company possesses roughly 10 million data records and has 80% Android users and 20% iOS users. This scenario could be a manufacturer that operates several factories and has a large field service team. Workers at the plants, corporate offices, and in the field need access to sensitive data and intellectual property to design, manufacture, and service the company's products.



Source: Lookout/Aberdeen

Based on: 10,000 mobile devices | 20% iOS 80% Android | 10,000,000 Records

Encounters: Minimum: 810 devices | Max: 5,220 | Median: 2,670

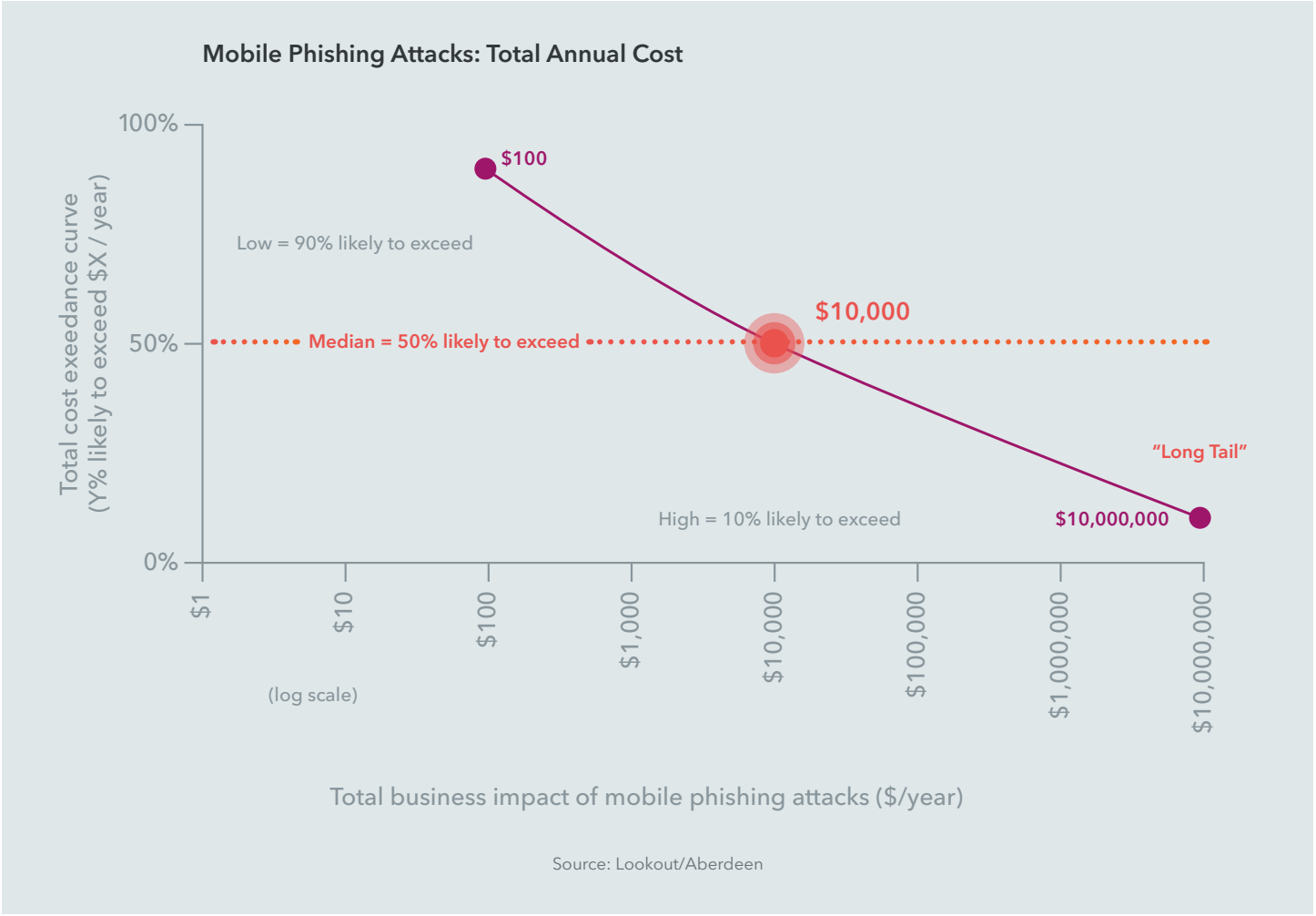
Clicks: Minimum: 270 | Max: 3,150 | Median: 1,420

Median Impact: $100,000/year

Maximum Risk: $35,000,000/year

Example C: Mid-size regional law firm

In this example, we look at an organization that's managing 1,000 devices without an MDM. The company possesses roughly a million data records and has 100% iOS users. An example of this type of scenario would be in a medium-size business such as a law firm. Employees are mostly located in a few cities, but they need access to sensitive data whether they are in the office, in court or at client meetings.



Source: Lookout/Aberdeen

Based on: 1,000 mobile devices | 100% iOS | 1,000,000 Records

Encounters: Minimum: 20 devices | Max: 570 | Median: 230

Clicks: Minimum: 0 | Max: 250 | Median: 80

Median Impact: $10,000/year

Maximum Risk: $10,000,000/year

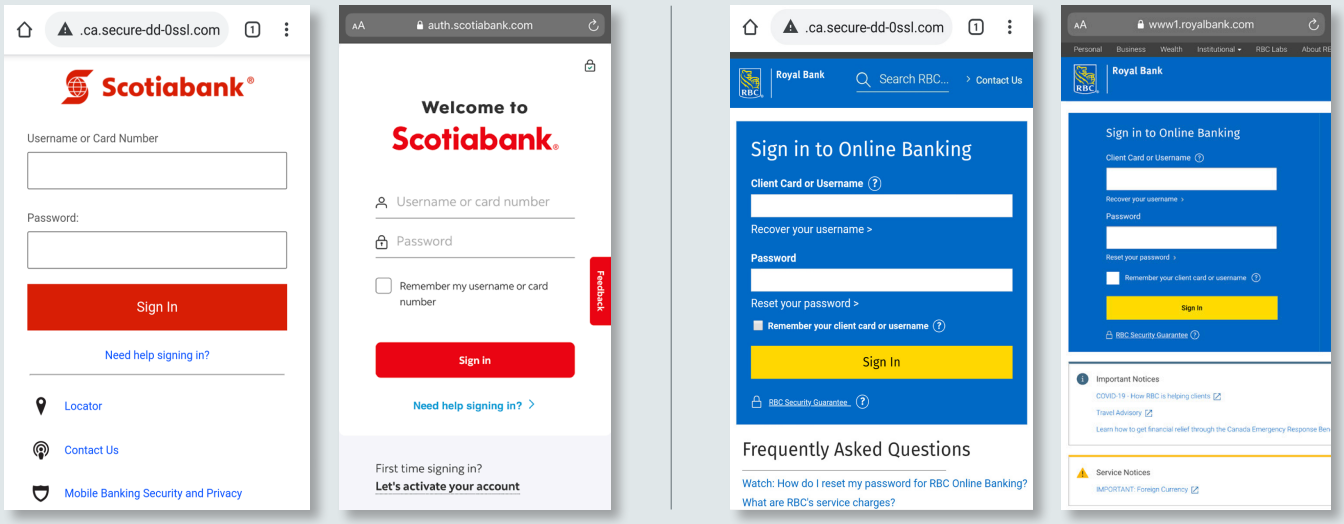
Looking at the numbers, which are based on real-world encounter rates with mobile phishing attacks, there is likelihood of significant financial damage to a company at the hands of just one employee mistakenly giving an attacker access to the infrastructure. There are countless scenarios that can be run, but no matter what the potential impact of an attack like this can be detrimental to the organization's growth and financial well-being.

Real world mobile phishing attacks on banking customers

Over the years, phishing attacks evolved in complexity to look indistinguishable from communication that the real source would have sent. Like we've discussed in this report, the evolution of phishing attacks has come a long way from the early email campaigns. With the world's heavy reliance on cloud services that enable employees to access data from anywhere, attackers' campaigns have evolved, but the end goal still remains the same for these bad actors – steal highly valuable information for financial gain, leverage against an individual or company, or to steal proprietary information.

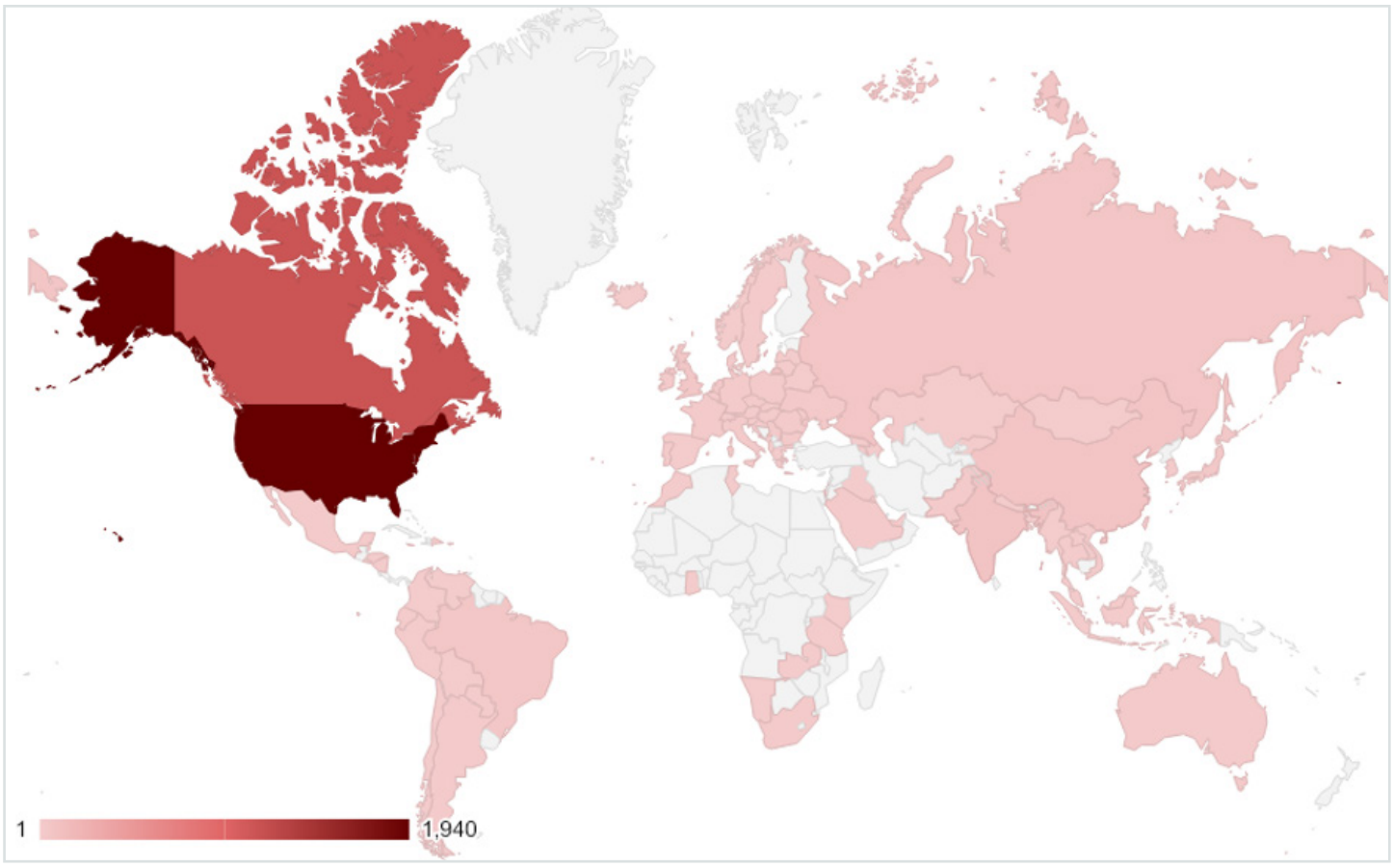
A perfect example of a well-executed and mobile-focused phishing campaign was discovered in February 2020. Targeting customers of major Canadian banks, this campaign was a simple mass-blast SMS text from a local Canadian number asking the recipient to click a link to log in to their account.

Clicking the link brought the recipient to a mobile site that, unless the recipient visited that page every day, looks like a perfectly legitimate login page for that bank's online account services.



Side-by-side comparison of the real and fake login pages for Canadian banking customers. Source: Lookout

As the screenshots above show, there is very little to tip off a Scotiabank or RBC customer that this login page might be fake or nefarious. The URLs are the only real giveaways that these are fake pages. People would likely pay no attention to the web address because they are programmed to quickly move through login screens and often view them as a nuisance.



Heat map showing the spread of IP locations of victims of this phishing campaign. Over 3,900 unique IP addresses were captured over a seven-month period. Source: Lookout

How to detect and protect against mobile phishing

Whether your organization provides company-owned mobile devices or allows BYO devices, every Android and iOS device should have phishing protection deployed. Since attacks can come from anyone and occur anywhere, there is no way to predict how they will present themselves, and everyone must be prepared.

Without anything in place to monitor devices, it's impossible to detect and respond to a phishing attack, much less protect against it. If an employee encounters a phishing link and is able to identify it as such, odds are they're just going to delete the email, text, or social media message. Instead, they should report the incident to the organization's security team to provide data on how to strengthen their anti-phishing strategy. What's worse is that if the person actually falls for the attack and gives up login credentials, monetary funds, or whatever the attacker is targeting, they wouldn't realize the consequences of their actions until the ramifications came back around to harm the company.

A successful mobile phishing attack can have a multitude of negative effects on a company beyond just financial loss. The hit to brand reputation can be highly disruptive, especially in a highly regulated industry like financial services, legal, or healthcare that loses highly sensitive customer information. The road to forgiveness by those customers that stick with the company is long and compliance officers will come knocking to levy fines against that firm. The financial loss of that alone has potential to be detrimental to the future growth of the company.

Implementing an organization-wide purpose-built mobile-first security solution is the critical to detect and protect against mobile phishing. Many solutions are bringing traditional desktop-focused email phishing solutions to mobile that, as we explored earlier in this report, do not cover all the vectors of a mobile phishing attack. It's important that the solution covers both iOS and Android equally, as most organizations have a mix of both in their fleet – especially when an organization supports BYOD.

You also don't want your users to feel like they're being watched, so the mobile security you choose needs to protect without prying. Ideally, the solution should not inspect content and should instead only alert the person when they have clicked on or loaded a malicious link and automatically block the nefarious connection. These alerts will educate users to adjust their browsing habits and ultimately lower your organization's overall risk profile.

See Lookout Phishing and Content Protection in action in this video.

To learn more, visit us at lookout.com