Lookout™

The Global State of Mobile Phishing

Protecting against mobile phishing is essential to minimizing data risk

Executive Summary

Gone are the days of brute force cyber attacks. Users, endpoints, and applications are now closely connected to each other, which means threat actors can initiate advanced attacks by simply stealing an employee's credentials. By posing as a legitimate user, attackers can bypass many security measures to gain access to as much data as possible.

One of the most effective tactics to steal login credentials is mobile phishing. In fact, according to global data from Lookout, 2022 had the highest percentage of mobile phishing encounter rates ever — with an average of more than 30% of personal and enterprise users exposed to these attacks every quarter.[1] This poses significant security, compliance, and financial risk to organizations in every industry.

A significant contributor to this trend is likely hybrid work, which has made the idea of using personal devices for work more broadly accepted as organizations relax their bring-your-own-device (BYOD) policies. While this gives employees the flexibility to work the way they prefer, it adds significant risk to the enterprise — so much that Verizon referred to BYOD as 'bring your own danger' in its 2022 Mobile Security Index (MSI) Report. This is because, as you will learn in this report, BYOD introduces additional risk to corporate users, devices, apps, and data.

The risks associated with mobile phishing go far beyond BYOD devices. Any device, regardless of whether it's iOS or Android, personal, corporate owned, managed, or unmanaged, is susceptible to phishing. Mobile apps with a messaging function could be used to socially engineer individuals and execute these campaigns, which means modern phishing techniques go far beyond leveraging email delivery, which many still may perceive as the primary source of phishing.

Whichever way you cut it, mobile phishing is a significant problem growing at an alarming rate. With mobile usage increasing globally year-over-year, up 79% from where it was just six years ago, it's critical to stay ahead of this issue.[2]

[1] Lookout Security Graph Data, January 1st - December 31st, 2022
[2] https://www.oberlo.com/statistics/how-many-people-have-smartphones

2022 Key Findings

Methodology

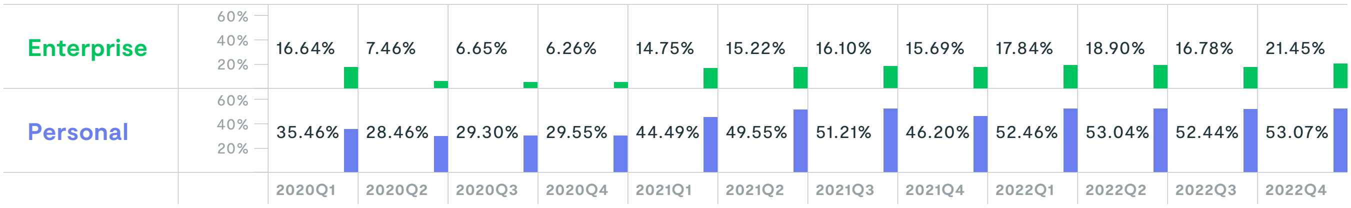
The data and trends in this report are based on findings from Lookout's ever-growing mobile dataset of security telemetry, which is built on graph-based machine intelligence that analyzes data globally from more than 210 million devices, 175 million apps, and ingests four million URLs daily.

Mobile phishing is here to stay

In the 2020 edition of The State of Mobile Phishing Report, we noted that mobile phishing attacks increased in the first quarter of 2020, as threat actors took advantage of the pandemic-accelerated digital transformation. That spike ended up coming back down for the rest of the year. At the start of 2021, we saw a similar jump across both personal and enterprise devices, but this time it wasn't an outlier.

Since the start of 2021, encounter rates have increased and the new baselines now sit at roughly 10 percentage points higher for enterprise and over 20 percentage points higher for personal than they did in 2020.

While both numbers are concerning, it's important to note that the relaxed BYOD policies resulting from hybrid work introduced a significant number of personal devices to the enterprise environment, creating a highly-targeted blind spot for IT and security teams, and they need to adjust their strategies in order to protect against it.



Mobile phishing encounter rates 2020-2022. Source: Lookout

Mobile phishing attacks are getting harder to identify

In addition to increased encounter rates, we also found that more users on both enterprise and personal devices are falling for more mobile phishing links than they were even two years ago. Of the users who are tapping on phishing links, there is a steady increase in those who tap on more than six links. This could signal that threat actors are finding more convincing ways to socially engineer their targets such that users cannot tell them apart from authentic messages even after the individuals already encountered an attack before.

Mobile users tapping on 6+ phishing links annually

	2020	2021	2022
Enterprise	1.6%	6.6%	11.8%
Personal	14.3%	23.5%	27.6%

Percentage of users who tapped on at least six unique phishing links annually 2020-2022. Source: Lookout Security Graph

Regulated industries are lucrative targets

Unsurprisingly, some of the most regulated industries are also frequently targeted. This is likely due to the immense amounts of sensitive personally identifiable information (PII), intellectual property, or financial data that they own. And with a single successful mobile phishing attack, a threat actor could get access to an organization's infrastructure and sensitive data.

Increased risks equals increased costs

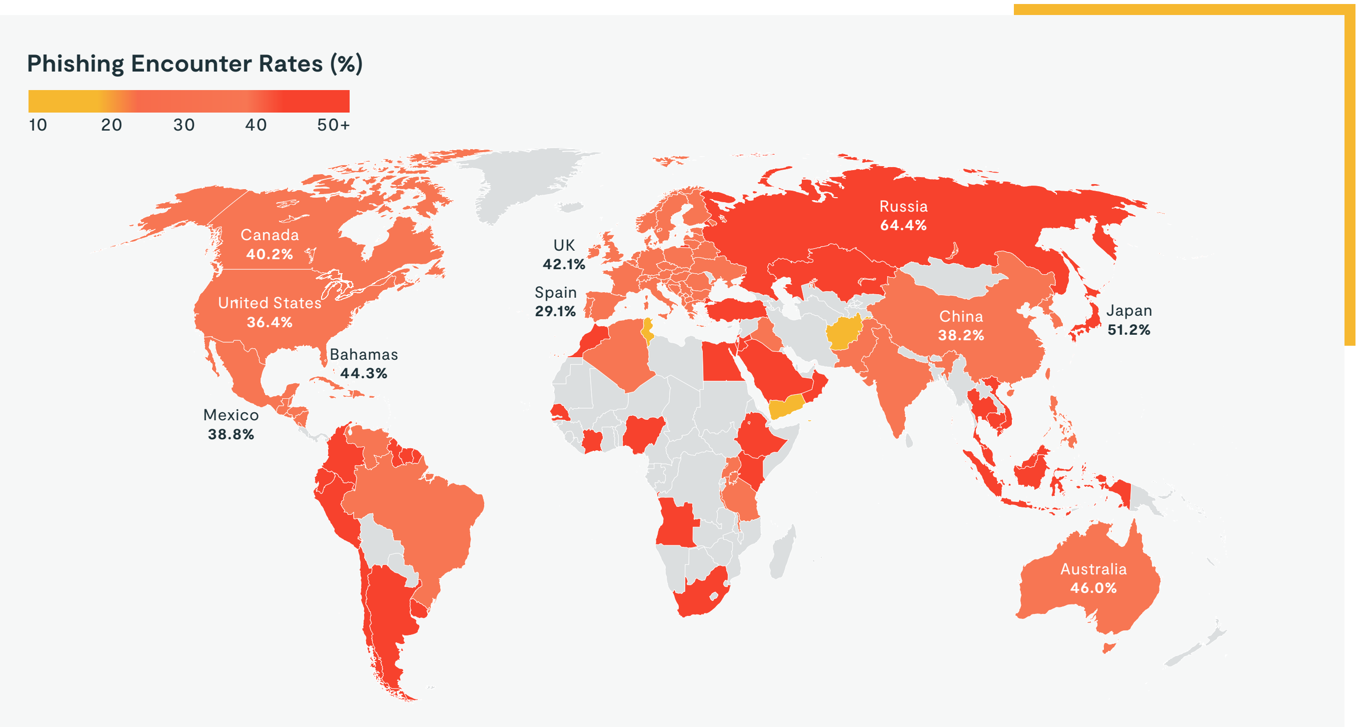
Risk can be measured in a number of ways. With how valuable data has become, cyber, compliance, and financial risk are now fully intertwined as data breaches involving sensitive user data seem to be occurring every day. Using the Factor Analysis of Information Risk (FAIR) model of risk analysis, we estimate that the maximum potential financial impact of a successful mobile phishing to an organization of 5,000 employees is **almost $4,000,000**.

Industry	Percentage of users targeted with at least one phishing attack each quarter in 2022
Insurance	34.5%
Banking	34.1%
Legal	31.7%
Healthcare	31.2%
Financial Services	30.3%

Why is mobile phishing so prevalent?

It's critical to understand why this has become a preferred tactic for cyber criminals to gain initial access to corporate data. The mobile device has become another appendage for most of us — not just to connect with friends and families or to shop, but also to message colleagues and connect to enterprise resources.

Attackers have shifted their focus towards attacking people rather than specific devices. They do this by casting a wide net across both personal and work platforms in order to increase the likelihood of stealing credentials and being able to impersonate an individual as a way to gain access to sensitive data.



Mobile phishing encounter rates around the world in 2022. Source: Lookout

Evolving tactics

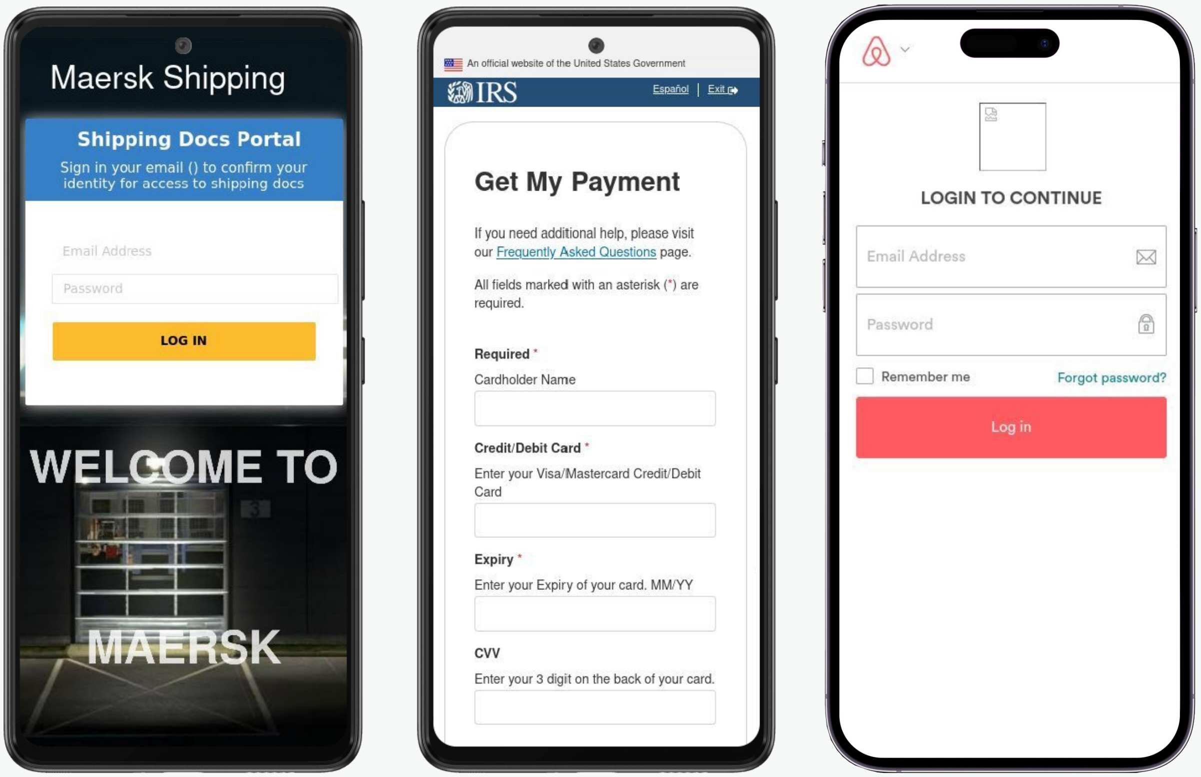
Phishing attacks are no longer executed through email alone. There has been a significant rise in vishing (voice phishing), smishing (SMS phishing), and quishing (QR code phishing). Attackers now combine these tactics together in order to compromise an employee's credentials directly, or to get past other security measures like multi-factor authentication (MFA) in what are known as hybrid phishing attacks. **These attacks increased by more than 7x in the second quarter of 2022.**[3]

One common combination is for an attacker to target an individual with a spear phishing attack, then pair it with a vishing attack in which they pretend to be the IT department to get that target to accept MFA validation, share their login credentials, or install malware for remote access. In fact, data from IBM's X-Force Threat Intelligence Index 2022 shows that the click effectiveness for targeted phishing campaigns adding phone calls (vishing) is about three times more effective, which nets a click from a whopping 53.2 percent of victims, compared to a click rate of 17.8 percent for the average targeted phishing.[4]

Mobile is a vulnerable blind spot

The mobile device presents a fundamentally different environment from a laptop or desktop. They can give a significant leg up to attackers who use the smaller screens, simplified interfaces, and hidden URLs to their advantage. This, coupled with our natural tendency to immediately tap on anything that comes up on our smartphone or tablet screen, gives phishing attacks a higher chance of success.

Three examples of very convincing mobile phishing pages.



Maersk Shipping

Shipping Docs Portal

Sign in your email () to confirm your identity for access to shipping docs

Email Address

Password

LOG IN

WELCOME TO

MAERSK

An official website of the United States Government

IRS Español | Exit

Get My Payment

If you need additional help, please visit our Frequently Asked Questions page.

All fields marked with an asterisk (*) are required.

Required *

Cardholder Name

Credit/Debit Card *

Enter your Visa/Mastercard Credit/Debit Card

Expiry *

Enter your Expiry of your card. MM/YY

CVV

Enter your 3 digit on the back of your card.

LOGIN TO CONTINUE

Email Address

Password

□ Remember me Forgot password?

Log in

[3] https://blog.knowbe4.com/hybrid-vishing-attacks-increase-625-in-q2
[4] https://www.ibm.com/downloads/cas/ADLMYLAZ?C1f3C

BYOD and the blurry lines between work and life

In addition to those mobile-specific technical challenges, smartphones and tablets have also fundamentally altered the way we think about work. Specifically, the way we think about what devices we use and how they relate to work and personal responsibilities. While these shifts have made productivity easier, they have also created additional security challenges for IT and security teams.

The first challenge is that there's little to no separation between work and personal device usage, and this is being amplified by BYOD. One of the biggest risks of using a device for both personal and work reasons is that mobile threats from the personal side of the device, such as using social media or connecting to an unknown Wi-Fi network while traveling, could impact the enterprise data accessible from that device. To address this problem, Google has tried to separate work and personal activities on Android devices by offering Dual Enrollment as part of its Android for Work offering. Apple takes a different approach by giving iOS users the option to build "work focus mode" and "personal mode," which affects the apps displayed on your device at certain times of the day. However, there have been challenges in the past where malicious personal apps have been able to compromise data in the work profile.[5]

There's also the challenge of visibility. IT and security teams have minimal visibility into what risk those devices pose to sensitive enterprise data. The risk could come from data permissions that apps have, risky network connections, or what websites the user visits on that device.

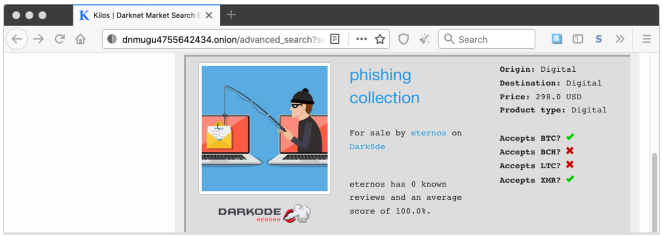
Finally, as the National Cyber Security Centre warns, a determined attacker who is very focused on finding a route into a particular company network may also target users' personal accounts.[6] This means there's also significant risk that an employee could fall victim to a socially-engineered attack that comes to them through personal channels like social media, third party messaging platforms like WhatsApp, or even dating apps.

In 2022, more than 50% of personal devices were exposed to a mobile phishing attack.[7]

Phishing kits are easily accessible

It's not just that mobile devices are more exploitable. Following the trend of the broader malware-as-a-service market, which has become a way for malware developers to provide their services as pre-built kits, attackers are getting access to cheap, easy-to-use phishing kits that developers put up for sale on the Dark Web. This means attackers need less technical knowledge than they used to in order to stand up a phishing campaign and can do so with less up-front cost.

For example, the below kit titled "phishing collection" was up for sale for $298. The developer claims that it can be used to target a handful of major platforms that enterprise organizations everywhere use such as iCloud, Dropbox, Amazon, Office 365, and Adobe.


Kilos | Darknet Market Search E
dnmugu4755642434.onion/advanced_search?se
Search
DARKODE
REBORN

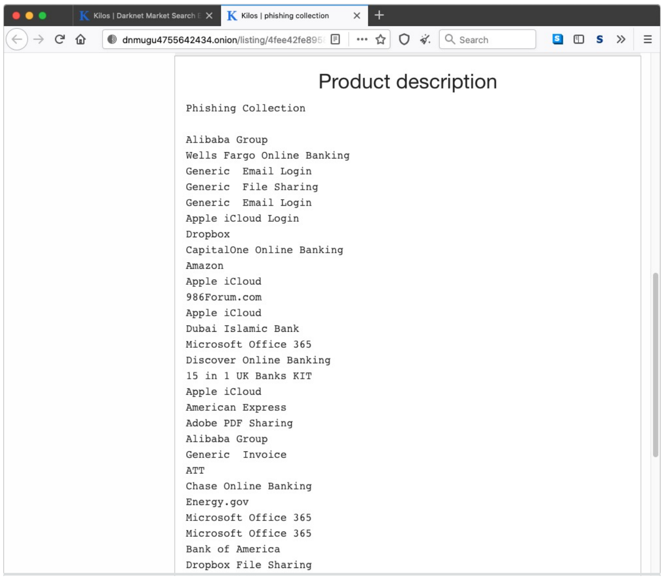
phishing collection

For sale by eternos on Dark0de

eternos has 0 known reviews and an average score of 100.0%.

Origin: Digital
Destination: Digital
Price: 298.0 USD
Product type: Digital

Accepts BTC? ✓
Accepts BCH? ✗
Accepts LTC? ✗
Accepts XMR? ✓


Kilos | Darknet Market Search E
Kilos | phishing collection
dnmugu4755642434.onion/listing/4fee42fe895
Search

Product description

```
Phishing Collection

Alibaba Group
Wells Fargo Online Banking
Generic  Email Login
Generic  File Sharing
Generic  Email Login
Apple iCloud Login
Dropbox
CapitalOne Online Banking
Amazon
Apple iCloud
986Forum.com
Apple iCloud
Dubai Islamic Bank
Microsoft Office 365
Discover Online Banking
15 in 1 UK Banks KIT
Apple iCloud
American Express
Adobe PDF Sharing
Alibaba Group
Generic  Invoice
ATT
Chase Online Banking
Energy.gov
Microsoft Office 365
Microsoft Office 365
Bank of America
Dropbox File Sharing
```

[5] https://www.darkreading.com/mobile/new-attack-threatens-android-for-work-security
[6] https://www.ncsc.gov.uk/blog-post/telling-users-to-avoid-clicking-bad-links-still-isnt-working
[7] Lookout Security Graph Data, January 1st - December 31st, 2022

Mobile phishing is the tip of the spear

Your employees expect to be able to access the data they need to be productive from any device, location, or network. With that being the case, more apps, data, devices, and networks are being introduced into complex enterprise ecosystems that make planning a security strategy more difficult every day. Attackers are using this to their advantage by targeting employees on mobile devices and apps to steal credentials and gain initial access to an organization's corporate infrastructure.

The below data shows the number of unique URLs accessed by users on both consumer and enterprise devices from 2020–2022 in an aggregate view of each year. The percentage of both consumer and enterprise users globally who are interacting with more than six malicious links is increasing each year. This is likely due to attackers getting better at creating convincing phishing campaigns that target both enterprise and personal channels as well as a blurrier line between personal and work usage on mobile devices.

Enterprise Devices

# of Unique URLs accessed	0	1	2	3–5	6+
2020	91.8%	3.4%	1.5%	1.7%	1.6%
2021	79.6%	6.4%	3.2%	4.3%	6.6%
2022	72.5%	6.8%	3.7%	5.2%	11.8%
2020–22 Percent Change	-21.00%	+100%	+146.70%	+205.90%	+637.50%

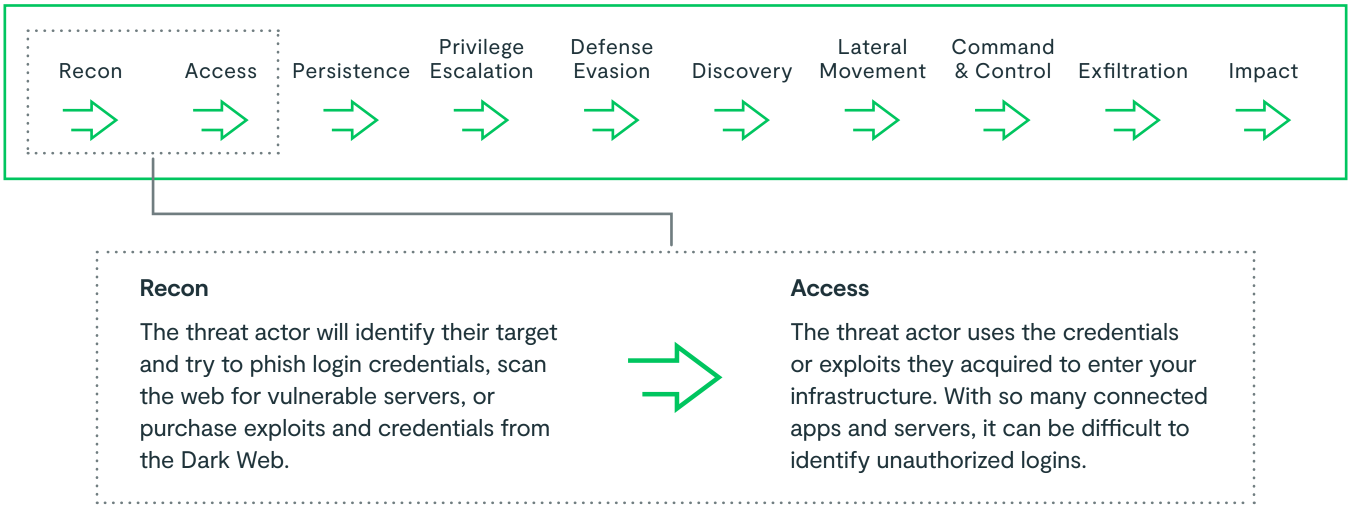
Personal Devices

# of Unique URLs accessed	0	1	2	3–5	6+
2020	62%	9.8%	5.7%	8.3%	14.3%
2021	51.8%	9.5%	5.7%	9.5%	23.5%
2022	45.8%	9.8%	6.3%	10.6%	27.6%
2020–22 Percent Change	-26.10%	-0.6%	+10.50%	+27.70%	+93.00%

There are a number of interesting trends to observe in this data that indicate how much more problematic mobile phishing has become over the years. **The first is that there is a significant decrease in users who avoid tapping phishing links altogether on both personal and enterprise devices, which means login credentials and data are being put at risk more frequently now than they were in 2020.** This means that there is an inevitable increase across the board, with the exception of users on personal devices who only tapped one link, of users interacting with more phishing links than ever before.

The numbers that stand out the most are the significant increases over time of users on enterprise devices tapping on malicious links. These targeted enterprise-level attacks intend to steal corporate credentials, which the attacker will then try to use across hundreds of known enterprise cloud-based platforms like AWS, Google, Salesforce, or Slack. They could also try to log in to a variety of VPN services, which would give them broad access to the organization's network resources. Once they're in, an attacker can do anything from a quick-hitting data exfil to a long-term surveillance campaign where they implement a backdoor to be able to enter and exit the victim's infrastructure as they please before executing an advanced attack like ransomware.

Ransomware Killchain



Recon → Access → Persistence → Privilege Escalation → Defense Evasion → Discovery → Lateral Movement → Command & Control → Exfiltration → Impact →

Recon

The threat actor will identify their target and try to phish login credentials, scan the web for vulnerable servers, or purchase exploits and credentials from the Dark Web.

Access

The threat actor uses the credentials or exploits they acquired to enter your infrastructure. With so many connected apps and servers, it can be difficult to identify unauthorized logins.

What is the business impact of mobile phishing?

Cybersecurity risk isn't just an issue for IT and security teams. As more breaches occur, finance and compliance teams are increasingly concerned about what cyber risk means to them.

Potential financial impact

As the risk of mobile phishing increases every year, so does the potential impact to an organization's bottom line. Below is a calculated estimation of the potential financial risk due to mobile phishing attacks on an annual basis.

To calculate this estimation, we took into account three key factors — the average number of phishing attempts per device, the likelihood of a phishing attack getting through, and the average impact per event.

The average number of attempts was extracted from the Lookout Security Graph over a two year period from December 31, 2021 to December 31, 2022.

The Threat Capability estimate, which is the likelihood of an attack reaching the target, is based on research that about 20% of people will open a phishing message, and about 67% of them will click the link and enter their credentials on the malicious webpage.[8] Multiplying these numbers together gives us a threat capability of 13.34%. This is confirmed by the National Council of Identity Theft Protection who indicates that it is possible that 13.4% of employees submitted their passwords to a phishing website.

This indicates that an organization with 5,000 devices could potentially face 2,501 phishing attacks each year. It should be noted that without proper security controls, these attacks could all have a direct impact.

Finally, the impact numbers are pulled from the Ponemon 2021 Cost of Phishing report, which surveyed 591 IT and IT security practitioners. Of those surveyed, the average organization size was 9,576 employees and the average costs incurred directly from phishing, ransomware, business email compromise or credential loss was $10,545,645. The average costs of business disruptions was extrapolated to be $4,280,572. Adding those two numbers together and dividing by 9,576 employees shows that the average cost of an incident is $1,550.

[8] https://etactics.com/blog/phishing-statistics

3.75 x	5,000 x	13.34% =	2,501
Average number of phishing attempts	Devices	Threat Capability	Potential phishing attacks annually

All of this was then calculated under the basis of the Factor Analysis of Information Risk (FAIR) model of risk analysis.

$1,550 x	2,501 =	$3,876,550
Average risk impact per event	Potential phishing attacks annually	Potential annual impact of mobile phishing

Now take the average financial risk impact per device and multiply it by the average attacks that penetrate an organization to get the resulting overall risk.

On the spectrum of risk tolerance, an organization that holds highly sensitive data in a regulated industry will have incredibly low risk tolerance because their chances of reaching this $3,876,550 number is high. However, even if that number represents 100% of the potential impact, even just 10% of that risk could cost an organization over $387,655 annually.

Highly targeted industries can take guidance from government initiatives

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 are some of the most affected by mobile phishing in 2022.

In addition to industries with well-known compliance regulations, such as banking and healthcare, it's also interesting to note that industries like energy and utilities, transportation, and manufacturing make this list. This could be due to the significant impact that supply chain disruption can have, as well as the immense amount of logistical data and intellectual property these organizations possess.

When teams see information about how their industry or organization is targeted by attackers, it can be difficult to know what first steps to take in order to mitigate the risk posed by that particular threat. In the case of mobile phishing, there has been significant development of government-backed initiatives and communications that can be looked at for guidance. In some cases, such as with the creation of GDPR, those initiatives have been turned into law.

Industry	Percentage of users targeted with at least one phishing attack each quarter in 2022
Insurance	34.5%
Banking	34.1%
Legal	31.7%
Healthcare	31.2%
Financial Services	30.3%
Government	27.9%
Energy & Utilities	25.5%
Transportation	20.9%
Manufacturing	20.5%
Retail & Wholesale	18.2%

Governments of various countries have taken initiatives to drive stronger mobile security throughout their agencies. If an issue is big enough that the government is focusing on it, then private organizations should follow suit and use these initiatives as guidance to prioritize their own security strategy.

For example, the Office of Management and Budget (OMB), which oversees the implementation of Presidential initiatives in the United States, issued two critical memorandums in 2022 pertaining to mobile security.

OMB M-22-01

Notes that Executive Order 14028 directs agencies to adopt an Endpoint Detection and Response (EDR) solution; specifically noting that the EDR of choice should enable "continuous monitoring and collection of endpoint data (for example…mobile phones) with rules-based automated response and analysis capabilities.[9]"

OMB M-22-09

Sets forth a federal zero-trust architecture (ZTA) strategy, requiring agencies to meet specific cybersecurity standards and objectives by the end of Fiscal Year (FY) 2024. The directive breaks cybersecurity strategy into three pillars — devices (mobile), applications/workloads, and data.[10]

Mobile threat defense (MTD) fills in the gaps around mobile device security and ensures a robust approach to zero trust security for mobile. A critical piece of this strategy is ensuring protection against mobile phishing campaigns that could lead to eventual data compromise. With phishing attacks frequently being the first step in data compromise, understanding where risk lies across all of your devices including mobile is critically important.

Data privacy and protection laws are now dictated by governments around the world as well as industries as a whole. Even if an organization isn't obligated to comply with specific regulations, government initiatives can drive the private sector to evaluate its own cybersecurity standards.

Protect against mobile phishing and secure your data

Regardless of whether employees use company-issued or personal devices, every iOS, iPadOS, and Android device needs to be protected against mobile phishing. Now more than ever, empowering employees to use mobile devices is a critical piece of boosting productivity. But with one in five enterprise devices and over half of personal devices being exposed to at least one mobile phishing attack every quarter, you need to be aware of the risks they pose to your users and data. It's critical to take adequate steps to treat the mobile device like other endpoints worth protecting in your environment.

The significant increase in phishing attacks on both corporate and personal mobile devices through 2022 as well as the hefty potential financial risk show that continuously modernizing security is critical to both the technical and business side of any organization. IT and security teams need to think about how they can adapt their own strategies to be able to dynamically visualize, detect, and minimize data risk posed by these devices. We anticipate that many private organizations will take the lead from government initiatives to ensure that mobile device security and detection and response capabilities that are extend to include mobile devices.

Credential compromise is frequently the first step in an attack as it grants the malicious actor direct access to the target's infrastructure. We have even observed attackers taking advantage of MFA fatigue explicitly on mobile devices — which allows the attacker to not only compromise an employees credentials, but allows them to compromise systems which are protected with a password and MFA. Supplementing that with the ability to detect anomalous activity across all of your platforms, apps, and networks rounds out a holistic endpoint-to-cloud strategy necessary to protecting enterprise data against today's evolving threat landscape.

To learn more about the Lookout Cloud Security Platform, visit us at www.lookout.com

[9] https://www.whitehouse.gov/wp-content/uploads/2021/10/M-22-01.pdf
[10] https://www.whitehouse.gov/wp-content/uploads/2022/01/M-22-09.pdf

About Lookout

Lookout, Inc. is the endpoint to cloud security company purpose-built for the intersection of enterprise and personal data. We safeguard data across devices, apps, networks and clouds through our unified, cloud-native security platform — a solution that's as fluid and flexible as the modern digital world. By giving organizations and individuals greater control over their data, we enable them to unleash its value and thrive. Lookout is trusted by enterprises of all sizes, government agencies and millions of consumers to protect sensitive data, enabling them to live, work and connect — freely and safely. To learn more about the Lookout Cloud Security Platform, visit www.lookout.com and follow Lookout on our blog, LinkedIn, and Twitter.

For more information visit
lookout.com

Request a demo at
lookout.com/request-a-demo