2023 Mobile Platform Scam & Phishing

limitless innovation. no compromise.

Prepared for Google

Sept 8, 2023

Document Control

Document ID	2023 Mobile Platform Scam and Phishing Prevention Feature Competitive Analysis
Revision Version	1.00
Prepared By	Leviathan Security Group

Revision History

Version	Date	Description	Author(s)
1.0	September 8, 2023	FINAL	Leviathan Security Group

Table of Contents

Overview 4
Project Overview 4
Background 4
Scope & Purpose of Project 4
Methodology 5
Test Conditions 6
Phase 1 8
Test Matrix 8
Observations & Analysis 9
Advanced Protection Programs 9
Filtering & Flagging of Inbound Messages 10
Flagging & Blocking Malicious Sites 18
Phase II 21
Introduction 21
Test Results 21
Observations and analysis 22
Spam Call Detection 22
Spam Text Detection 22
Variables Potentially Affecting Outcome 22
Appendix – Default Phone Settings 25
Google Pixel 7 25
Samsung Galaxy S23 26
OnePlus 11 27
iPhone 14 28

Overview

Project Overview

Background

Modern attacks against mobile platforms rely almost exclusively on human actions, such as the tendency to click on a link or react to a malicious message. These actions can lead to security incidents that result in data or identity theft, and in certain cases, financial loss.

Mobile device users are increasingly concerned about the privacy and security of their personal data on these devices. High-profile data breaches and unauthorized information collection have made these issues a significant focus. They also want to know more about how their personal data is collected, used, and shared. The ability to evaluate mobile device security features helps users make informed decisions about the apps they use and the data they share.

Countermeasures against modern scalable and widespread attacks have become required functionalities for all mobile platforms. It is crucial that companies understand the human factors contributing to scam, phishing, and spam in order to safeguard sensitive information, implement protections against security breaches, and ensure privacy in our increasingly digital world.

Scope & Purpose of Project

Google engaged Leviathan Security Group to assess the Android and iOS phones to test security and privacy features and functions for safeguarding phone users against scams and phishing attacks. Feature-based testing was performed from March 17, 2023 through April 17, 2023, on four different devices. The quantitative testing phase concluded on July 13, 2023.

In June of 2022, we completed a similar competitive analysis for Google on Pixel 6, Samsung Galaxy S21, and iPhone 13 on both T-Mobile and Verizon networks. This current project revisits and expands on the previous assessment by testing the Samsung Galaxy S23, OnePlus 11, Google Pixel 7, and iPhone 14, all on the T-Mobile network.

The current project was divided into two phases. Phase 1 was a qualitative analysis comparing the features of the phones. Phase 2 was a quantitative analysis of phone performance with all provisioned on the same carrier and with the same number. This number was previously identified as very active (“hot”) target for scam calls and texts.

The assessment did not include penetration testing. Individual apps as well as Google Play and the Apple App Store were not in scope. We did not subscribe to paid features (e.g., iCloud+,

Samsung Account), nor did we opt in to T-Mobile's Scam ID & Scam Block feature.[1] No phones or the associated accounts were enrolled in Google's Advanced Protection Program.

The objective was to evaluate the effectiveness of each device's built-in security and privacy features and default settings-based protections. We tested their resilience to spammers and scammers, as well as their effectiveness in safeguarding user data and preventing unauthorized access. The assessment focus was to identify potential vulnerabilities and evaluate the effectiveness of existing security features. A specific objective was to evaluate features that help prevent or mitigate phishing and spam-based attacks. All devices were provisioned on the T-Mobile network to expedite testing.

Methodology

We leveraged our prior work, which included the 2022 analysis. Many security features noted in this document are similar to those discussed in the 2022 report. The testing is consistent with our previous methodology; our testing approach focused on utilizing security features firsthand and documenting observations about the protections offered by the various features.

We first tested and evaluated the privacy and security features of each device. This involved reviewing and documenting factory default settings and permissions, as well as security and privacy settings. Testing also included privacy policies and security features promoted with each phone. Each phone (with its respective number and email address) was signed up for spam mailing lists and phone call and text lists, and was used to navigate to websites known for phishing landing or the spread of malware.

Our testing focused on three key areas:

1. **Out-of-the-box protection programs**: Evaluate and compare the multiple account default protection security features and review advanced protection programs offered on the operating systems.

2. **Filtering and flagging of inbound messages**: Evaluate the effectiveness of each phone's available flagging and filtering features. All devices accept inbound messaging through email, voice calls, or text messages. Google and iCloud have spam email filtering via email. On all devices, texts have separate spam filtering options, whereas spam calls are marked as spam but still ring through the phone. Each phone in our test had STIR/SHAKEN functionality (all major US carriers have adopted STIR/SHAKEN as of 2023),[2] which we also tested.

[1] Help with scams, spam, and fraud | T-Mobile Support

[2] STIR/SHAKEN framework of standards: https://www.fcc.gov/call-authentication

3. **Flagging and blocking of malicious sites and mobile applications**: Navigate to known phishing and malware websites and observe the behavior of each device.

After initial testing of phone features was completed, the smartphones were consecutively tested for 30 days each in the following order: OnePlus 11, Google Pixel 7, iPhone 14, and Samsung Galaxy S23. The "hot" number was tested on each phone by swapping the eSIM between devices. Each phone was provisioned with the "hot" number eSIM, after which a test call and test text were sent. The phone was then observed for a 30-day period. All calls, texts, and their flagging were recorded. This approach allowed us to objectively evaluate and compare the effectiveness of anti-spam protections offered by each smartphone.

Test Conditions

We used accounts under our control to understand how an average user would experience the security features related to spam and phishing. When we were unable to replicate or witness a specific action firsthand, we relied on available documentation from the device manufacturer to better understand the feature itself. We analyzed these characteristics from the perspective of a casual user to determine whether conclusions can be drawn about efficacy via ease of operation.

The following phones were engaged in this project:

Phone	**Operating System**	**User Email Account**	**Default Dialer**	**Default Messaging app**
Google Pixel 7	Android 13	Gmail account	Phone by Google app	Messages by Google app
OnePlus 11	Android 13	Gmail account	Phone by Google app	Messages by Google app
Samsung Galaxy S23	Android 13	Gmail account	Samsung Phone app	Messages by Google app
iPhone 14	iOS 16.2	iCloud account	iOS Phone app	iOS Messages app

Prior to testing, we ensured all mobile devices were up to date with the latest public release versions of their respective operating systems and any relevant app and security updates.

Additional test conditions and factors included the following:

- All phones had eSIM capability, and eSIMs were used on all phones. For the Samsung Galaxy, iPhone, and Google Pixel, we needed the serial number, IMEI, and EID to set up the eSIM. This information was on or in the phone's packaging and/or in the phone settings "About" screens.
- The OnePlus 11 arrived with a sticker attached to the back of the phone that contained its model number, FCC-ID, IMEI 1 and 2, and a serial code.

- Gmail has spam filters working to protect user inboxes and claims to block more than 99.9% of spam, phishing, and malware.[3]
- By default, iCloud also has strong spam filters in place.[4] On the tested iPhone, a "Junk" folder was not visible or accessible by default on an iCloud domain account. Only spam emails that penetrated the iCloud filters were counted as received.
- All phones retained their factory default settings.
- Phones were checked daily for software and operating system update alerts, and updates were completed when available.

STIR/SHAKEN

We tested STIR/SHAKEN functionality on each mobile device. The Federal Communications Commission (FCC) requires major voice service providers to implement the Secure Telephone Identity Revisited (STIR) and Secure Handling of Asserted information using toKENs (SHAKEN) framework to combat illegal robocalls and spoofing.

STIR/SHAKEN is designed to reduce scammers' ability to spoof phone numbers. T-Mobile's STIR/SHAKEN implementation is integrated with its network and devices, so users do not need to download additional apps or take special steps. When a call is received on a T-Mobile device, the network verifies the call's authenticity and displays a "Caller Verified" message on the device's screen if the call is deemed legitimate.

T-Mobile offers a variety of opt-in call- and messaging-blocking tools, These include Scam Shield, a tool that provides features such as Scam Block (blocks known scam and spam calls from ringing the customer's device) and Caller ID (identifies incoming calls as spam or suspected spam). **We did not opt in to these additional features** because the test focused on the spam- and scam-mitigation capabilities and settings of the phones themselves, independent of options available from the carrier on which they were provisioned.

[3] Google's Gmail spam filters; https://workspace.google.com/blog/identity-and-security/an-overview-of-gmails-spam-filters

[4] https://support.apple.com/guide/icloud/manage-junk-mail-mm6b1a2ced/icloud

Phase 1

Test Matrix

After the phones arrived, the factory default security and privacy settings were reviewed and the features for each phone were documented. Prior to activation, the phones were connected to secure Wi-Fi networks to set up accounts and download any updates. We did not set up or subscribe to any paid, advanced features available from phone manufacturers. After phone activation, the following features were tested for each phone:

Feature	Test	iPhone 14	Google Pixel 7	OnePlus 11	Samsung Galaxy S23
Account Protection Programs	The ability to enroll in a higher level of protections for the account used on the device	✓	✓	✓	✓
FIDO Multi-factor Authentication	Default account on phone can be secured with FIDO	✓	✓	✓	Not supported for Samsung account. Supported for Google account
Password Managers	Password manager that can recognize registered sites and applications	✓	✓	✓	✓
Default Mail Application Filtering	Default application detected and filtered spam without user input	✓	✓	✓	✓
Email Masking	User has option to use a temporary email address	iCloud paid feature			
STIR/SHAKEN (as per T-Mobile)	Verification exposed to user	✓	✓	✓	✓
Report/Block Unknown Senders	First inbound message from a new contact allows flagging option	✓	✓	✓	✓
Report/Block First-Time & Unknown Callers	First inbound call from a new contact reported/blocked	✓	✓	✓	✓
Spam Flagged Calls	Call from number on spam blocklist	Carriers may change caller ID banner to "suspected spam"	✓	✓	✓
Call Screening	Screen call option offered		✓		
Spam Flagged SMS	SMS with spam message from known bad sender		✓	✓	✓
SMS Branding	Inbound SMS from verified sender shows special flagging		✓	✓	✓
Email Branding	Inbound email from verified sender shows special flagging in default mail client		✓	✓	✓
Safe Browsing	Default web browser detects malicious sites	✓	✓	✓	✓

Observations & Analysis

Advanced Protection Programs

In the past year, account protections have become more sophisticated for both Google and iOS programs, offering additional ways to use features such as multi-factor authentication (MFA) and data encryption. For both operating systems, multiple account protection security features are offered by default, as are advanced protection programs.

Google provides user accounts with a variety of MFA options, such as SMS or voice call, one-time Passwords, Google Authenticator, or Fast Identity Online (FIDO) Universal 2nd factor (U2F) hardware keys. In general, FIDO keys are particularly resistant to phishing attacks as they only send authenticators to registered sites.

FIDO U2F keys have advantages over single-factor authentication methods (e.g., passwords or one-time codes). U2F keys require physical access to the device to authenticate, which makes it more difficult for attackers to gain access to a user's account. Hardware keys are also easy to use and rarely require additional software installation or setup. Finally, they are compatible with a wide range of devices and online services that support the FIDO authentication protocol.

The Google Advanced Protection Program (within the Android platform) mandates using a FIDO key as the only option for authentication on a new device or browser instance, grants additional safeguards against harmful downloads, and provides supplementary features around securing personal information. Although this program was not leveraged as a part of the test, it is relevant to note that Google provides these additional features beyond what is available by default.

iOS 16.2 has multiple account protection options. Factory-default account and phone security includes an option for two-factor authentication that allows the user to designate a trusted phone number or other Apple device for authentication. A recovery key is also available that uses either a 28-character code (user retains physically[5]) or a designated recovery contact.[6] There is an Advanced Data Protection option that secures specific user and device data types with end-to-end encryption.[7] The iPhone also has FIDO functionality with a third-party key, but there are differences in the native functionality compared to that of Android.[8]

---

[5] Apple recovery key, https://support.apple.com/en-us/HT208072
[6] Apple recovery contact, https://support.apple.com/en-us/HT212513
[7]Apple's Advanced Data Protection, https://support.apple.com/guide/security/advanced-data-protection-for-icloud-sec973254c5f/web
[8]FIDO key support on the iPhone, https://support.apple.com/en-us/HT213154

All phones tested were observed to have password manager functionality. Android phones use the Google Password Manager, while the iPhone uses the iCloud Keychain.

Apple's addition of FIDO functionality is a notable change from our previous review. However, Apple has not yet been certified by the FIDO Alliance and the feature set does not have full parity with Google/Android account protection.[9]

Filtering & Flagging of Inbound Messages

Default Mail Application Spam Filtering

Each of the 3 Android phones had a dedicated Gmail account, and the iPhone had an iCloud email account. Accounts were enrolled in numerous mailing lists, including spam mail websites and sweepstakes. In addition, we used mass spam mail services, such as mailbait.info. All phones received 6 or fewer spam emails.

Google has strong built-in security measures against spam.[10] These default measures ensured our dedicated Gmail accounts were not susceptible to spam.

Gmail displays images through proxies that makes it more difficult to track pixels. This provides users with another layer of protection when using Gmail to read messages on the Pixel. The technique can help prevent spammers from receiving confirmation that an email account has opened a message, indicating that it is a valid and active account.

The default mail application for iOS is tied to an iCloud email account. Filtered messages were not viewable unless multiple setting were changed. For additional protections, the iCloud Private Relay service obscures both the IP address and the user's internet activity on Safari. The service requires users to have an iCloud+ subscription (at additional cost).[11] The iPhone offers Mail Privacy Protection by default (without iCloud+), which hides the phone's IP address and background remote content loading (see Figure 1).

[9] FIDO Alliance - Open Authentication Standards More Secure than Passwords

[10] Overview of Gmail spam filters, https://workspace.google.com/blog/identity-and-security/an-overview-of-gmails-spam-filters

[11] iCloud Private Relay informational page https://support.apple.com/en-us/HT212614

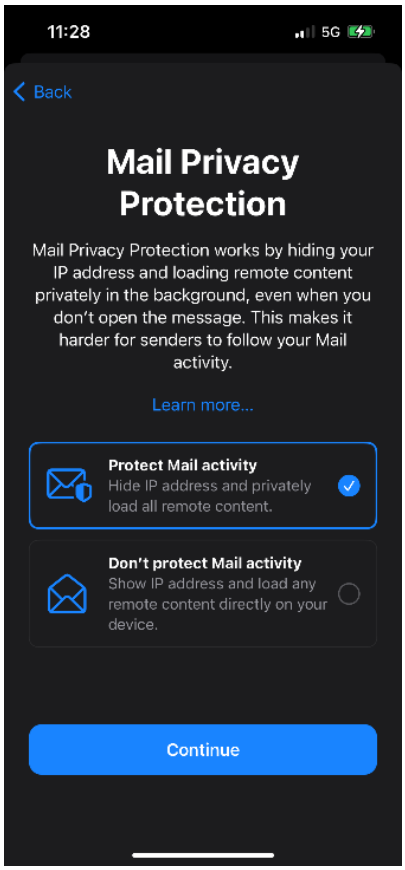


Figure 1. iPhone Mail Privacy Protection screen

Email Masking

Email masking is a technique that hides the user's email address and provides a temporary, disposable email that forwards messages appropriately. This protects the user's actual email address from being spammed or harvested by automated tools. Although there are plug-ins and apps available for the Android-based phones, email-masking functionality is not available by factory default on any of the Android phones tested. iOS offers email masking with an iCloud+ subscription (at additional cost).[12]

Inbound Calls & Texts

The detection of suspicious or untrustworthy communications in text messages or phone calls is challenging and often relies on the user's carrier and the phone's system. Because of historical reasons for open connections to phone networks, verifying the authenticity of phone calls can be difficult, and therefore call spoofing is a persistent and prevalent problem.

[12] iCloud+ Subscription features page https://support.apple.com/en-us/HT210425

On T-Mobile, call protection services are not offered by default. During the process for setting up service on the T-Mobile website, the customer must intentionally navigate to Call Protection Services to select the service (see Figure 2).

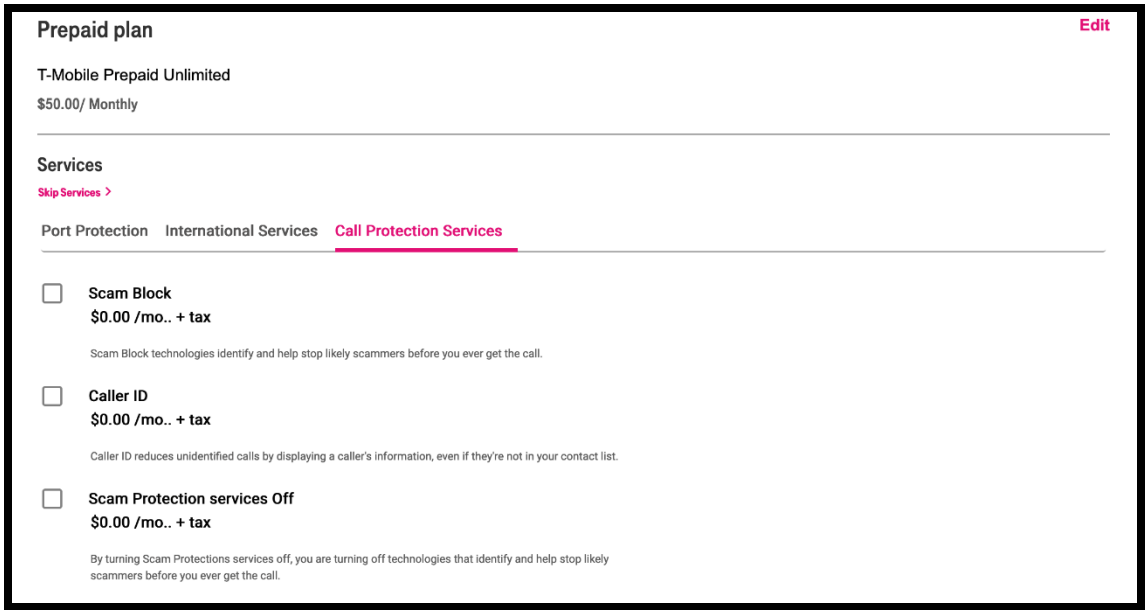
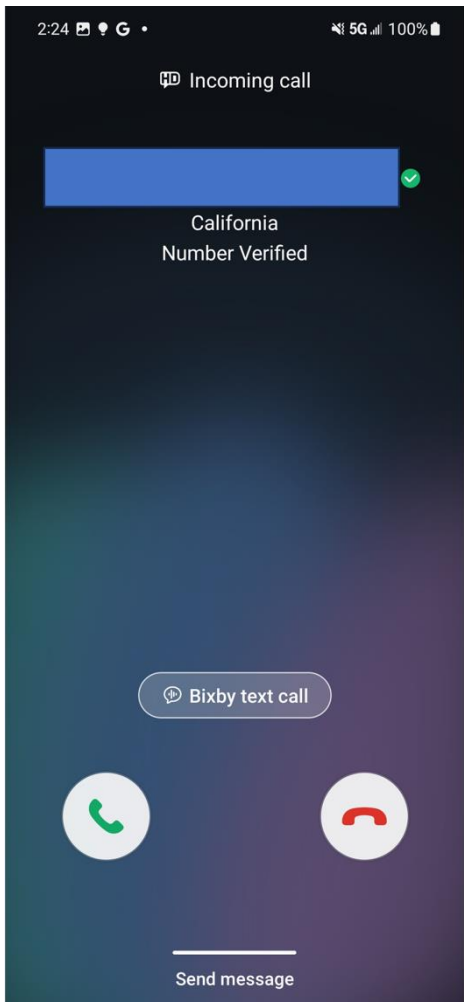
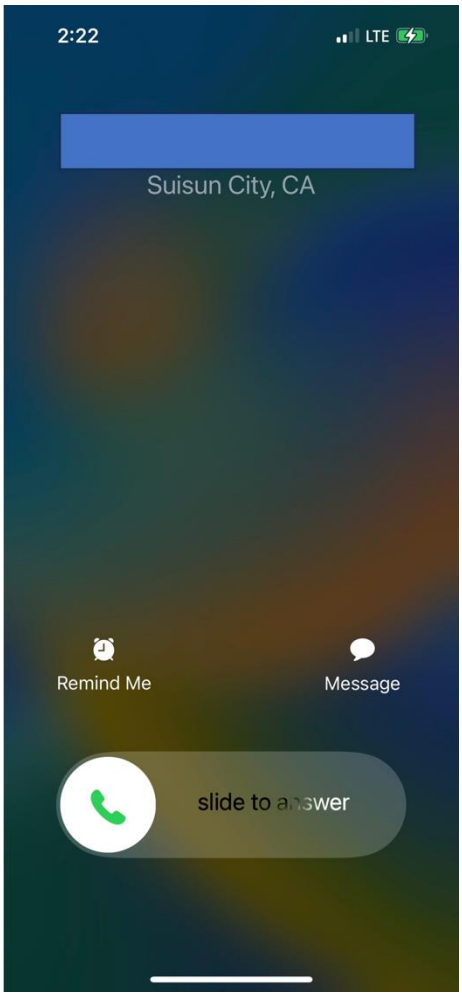


Figure 2. T-Mobile Call Protection Services sign-up

STIR/SHAKEN

To confirm STIR/SHAKEN functionality was enabled, we placed a test call to each phone and verified that the call was authenticated, and that the caller ID information matched the expected caller. On Android phones, “verified number” as well as a check mark was displayed at the time the call was received. On the iPhone, it was not (see Figure 3). We inspected the iPhone call log and found that the log displayed a checkmark designating verified numbers.





Galaxy S23	iPhone 14
A similar interface was displayed on the Pixel and OnePlus. This screenshot demonstrates "Number Verified" notice.	Note that the iPhone makes no distinction of verified number.

Figure 3. "Number Verified" screen comparison

Spam Calls

During testing, the Android and iOS devices received unsolicited spam calls. All phones provided the option to block a caller/number in the phone's call history (see Figure 4).

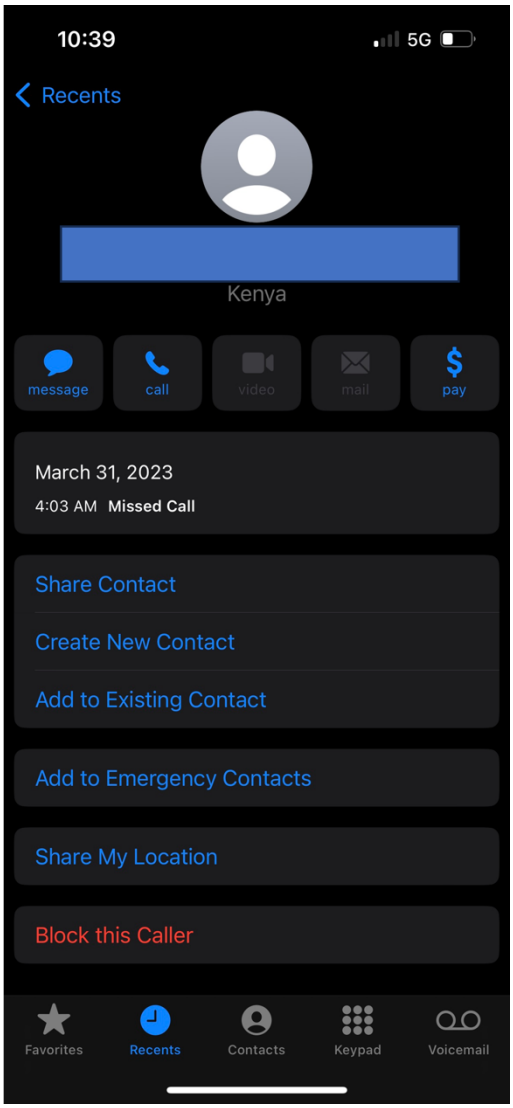


Figure 4. iPhone 14 screen, example of "Block caller" option in call history

None of the platforms flagged the spoofed caller ID as potentially scam or phishing-related, which may suggest that Caller ID spoofing is commonly used by legitimate commercial entities for business purposes. On all phones tested, spam calls from outside the U.S. appeared as "International"; in some cases, the country was identified as well (see Figure 5). This was not phone-specific; we theorize this to be country-specific based on the wireless standards adopted from the country or area within the country the call originated from.

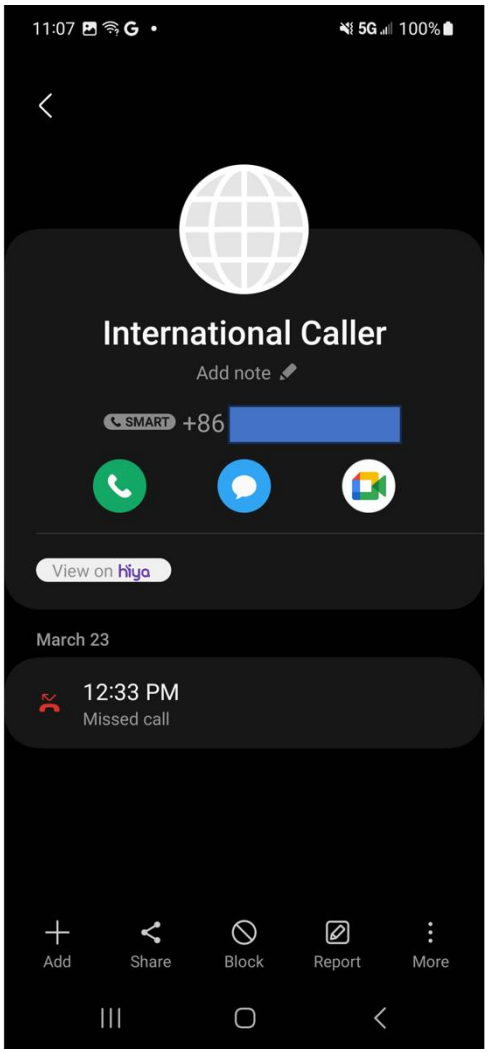


Figure 5. Screen depicting an international spam call (Galaxy S23)

Call, Email, Message, & Phishing Detection

By default, both iOS and Android offer call and message acceptance capabilities, which usually rely on the device's contact history with the phone number rather than STIR/SHAKEN verification. These features can include checking phone numbers against lists of known scam and phishing numbers, carrier-based flagging of suspicious numbers, searching through the call history associated with a phone number, and comparing the number to the user's contact list. The methods used for screening calls and messages can vary in level of sophistication and how they are displayed to users. For verified numbers, the iPhone made no distinction. The Android phones displayed a "verified number" notice below the caller's number on the call screen. Additionally, the Pixel displayed "Scam Likely" in caller ID when calls were received from potentially dubious sources (see Figure 6).

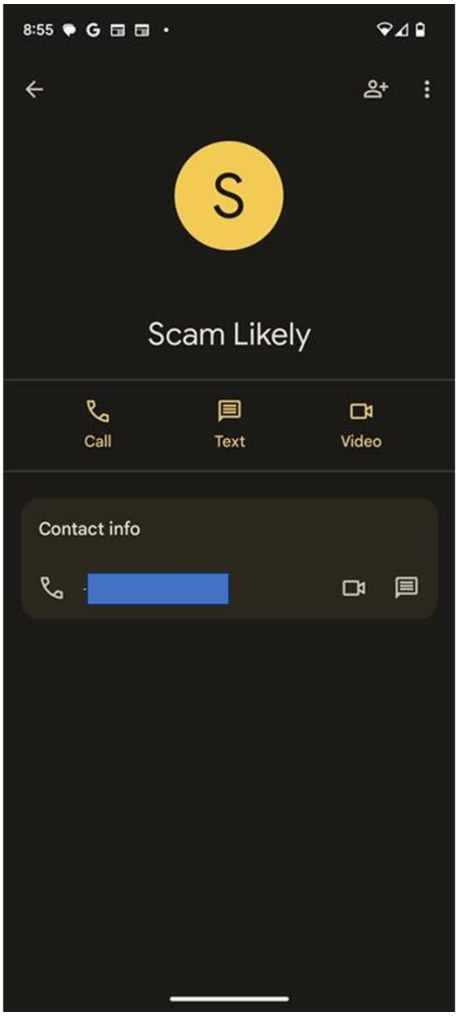


Figure 6. Pixel "Scam Likely" screen in caller ID

The Android phones have a separate folder for spam/junk messages. The iPhone does not. If the iPhone receives a message from an unknown number, the user is presented with a link to "report junk" and a message stating "This sender is not in your contact list."

Call Screening

The Pixel offers call screening, as do some Android phones using the Google Phone app in the US.[13] Call Screening is available in other countries, but not all features available in the US are accessible in other locations. Call screening is accessed via the phone app and can be set up as an automatic or manual operation. The user can either choose their preferred behavior or have the Google Assistant request additional information about the caller, and present the user with a

[13] Call screening in Android https://support.google.com/phoneapp/answer/9118387?hl=en

list of response options. The "Unknown Caller" settings can be configured to automatically screen calls; options are "Silently Decline" or "Automatically Screen. Deny Robocalls." Another key feature, when activated, will save the transcription of the screened call for later review.

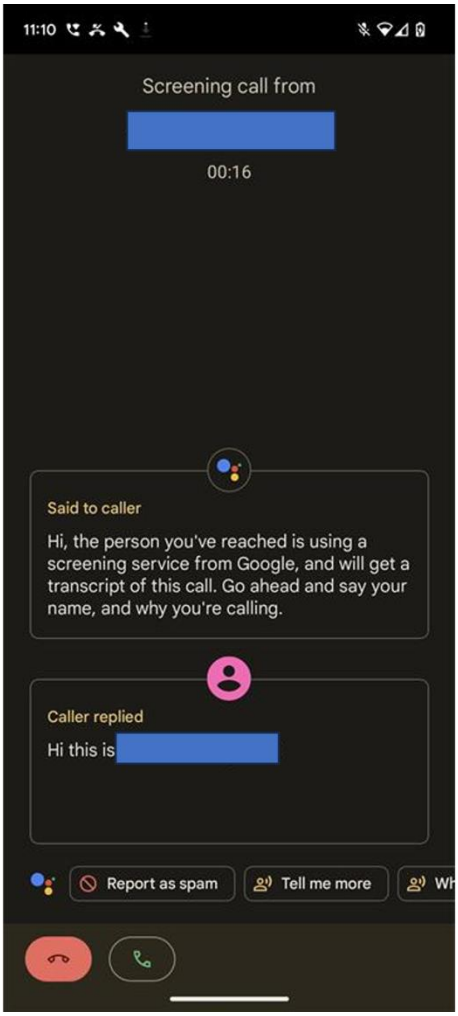


Figure 7. Call screening in use on the Pixel (Android)

iPhone also has a "Silence Unknown Callers" settings option, which was not enabled by factory default on the phone received. Therefore, we did not leverage it during testing. However, screening apps available on the Apple App Store provide additional functionality.[14]

This feature on Android is consistent with our observations from the previous report.

[14] iPhone call screening options https://support.apple.com/en-us/HT207099

Flagging & Blocking Malicious Sites

Malicious Websites/Safe Browsing

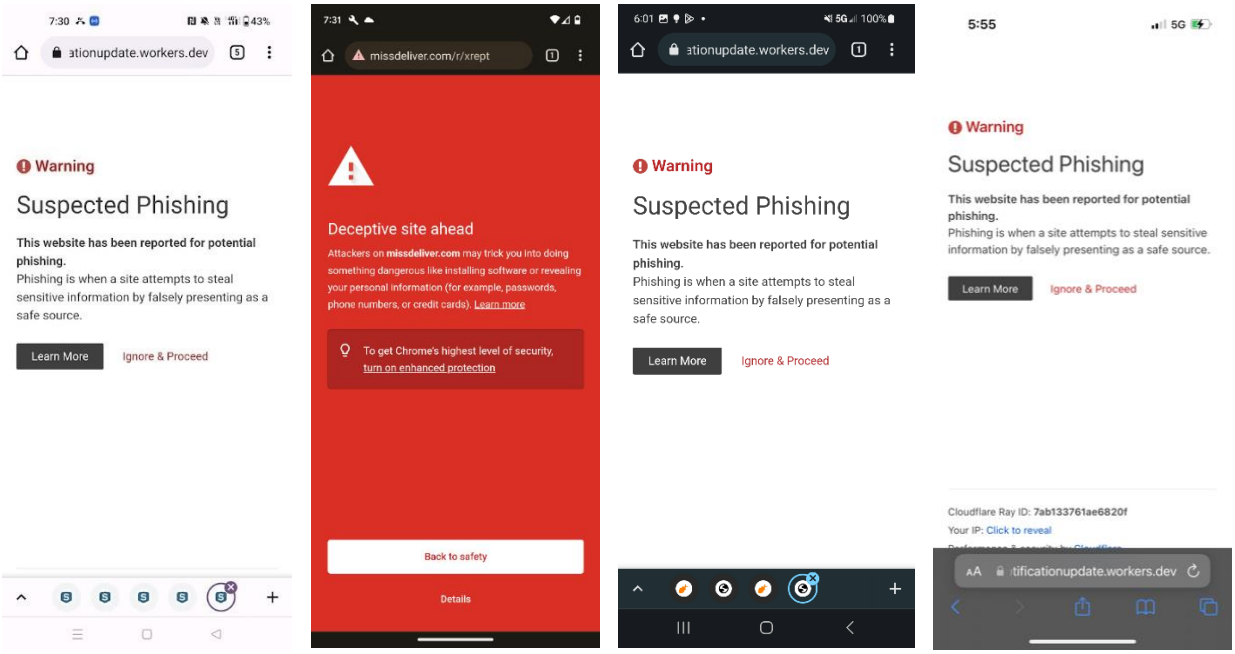
Both platforms have features intended to prevent users from accessing malicious websites. When a user visits a phishing website after clicking on a link from a text message or email, there are safeguards in place that alerts them to the risks of divulging confidential information or trusting the site's content.

On the Android platform, Chrome's Safe Browsing feature is a crucial defense against malicious websites.[15] This feature leverages the vast number of websites visited across its platform to rapidly identify and flag fraudulent and phishing sites. If a user tries to access a URL from an SMS that is part of a phishing or scam attack, Chrome may recognize the website as malicious and warn the user (see Figure 8). Chrome also offers enhanced protections that are not enabled by default.

iOS has several user-controllable options to protect the user and foster safe browsing. The settings hide the device's originating IP address, prevent ad tracking, and warn against visiting fraudulent websites (see Figure 8). Cookie blocking and cross-site tracking can also be enabled.[16] By default, Safari blocks sites that have been reported for malware or phishing.

Revisiting last year's methodology, we tested the scam and phishing detection features in the browsers by finding a recent confirmed phishing attack site from phishtank.com and opening the link in each device's default browser. Each device presented a warning when the known phishing attack site was visited.

[15] Chrome's safe browsing feature https://safebrowsing.google.com
[16] Browse privately in Safari on iPhone - Apple Support



Google Pixel 7	OnePlus 11	Samsung Galaxy S23	iPhone 14

Figure 8. Phishing warning screen on each phone

We expanded upon our testing of safe browsing features this year to include testing secure browsing protections. This was accomplished by visiting a series of simulated SSL issue sites provided by BADSSL.com. All phones tested provided a user notification of “This connection is not private” or similar verbiage depending on the state of the bad SSL certificate (see Figure 9). All phones presented the user with a message when the bad certificate was encountered.

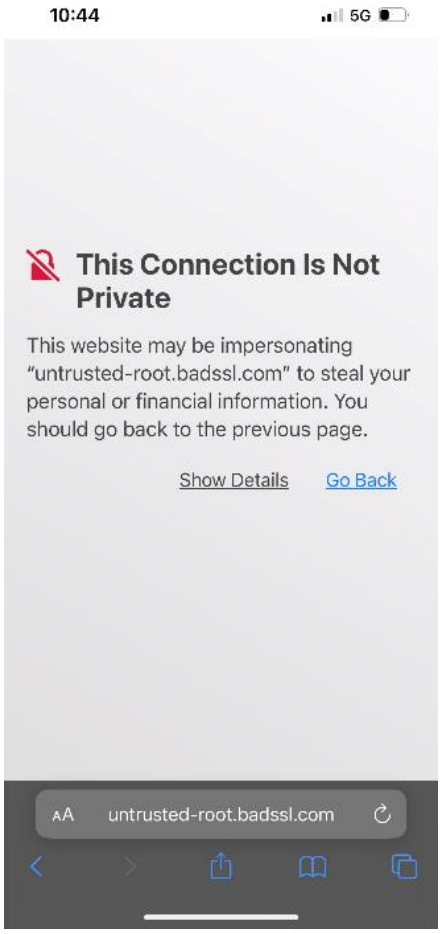


Figure 9. User notification on the iPhone. Android phones presented similar alerts

The Android phones presented the user with the options of "advanced" or "return to safety." When "advanced" was selected, details of the certificate issue were presented and the user was prompted with the option to view the certificate, continue to the site, or "return to safety."

The iPhone presented the user with the options of "Show details" or "Go Back". When "Show Details" was selected, a brief description of the certificate issue was presented, and the user was prompted with the option to view the certificate, continue to the site, or "Go Back."

On all phones, a user can only visit a site with a bad SSL certificate after selecting a detailed view and choosing to proceed after the site issue is explained. Two levels of user prompts with clear explanations should be sufficient to deter most users from visiting bad certificate (and potentially compromised) sites.

Phase II

Introduction

In Phase I, we compared each phone's security and anti-spam/scam features against the others. Phase II of this project quantitatively tested the spam detection functions of the phones. The four smartphones were consecutively tested for 30 days each in the following order: OnePlus 11, Google Pixel 7, iPhone 14, and Samsung Galaxy S23), during which the "hot" number was used by swapping the eSIM between devices. This approach allowed us to objectively evaluate and compare the effectiveness of the anti-spam protections offered by each smartphone.

Test Results

The following table summarizes the call results; phones are listed in the order of testing using the swapped eSIM:

	Total calls	Calls flagged as spam	Percentage flagged as spam	Total texts	Texts flagged as spam	Percentage flagged as spam
OnePlus 11	81	53	65.43%	11	3	27.27%
Google Pixel 7	91	59	64.84%	13	4	30.77%
iPhone 14	212	68	32.08%	37	0	0%
Samsung Galaxy S23	200	19	9%	53	15	28.3%

Total Number of Calls represents the number of calls received on each phone. This number includes calls that were not flagged as spam. Calls not marked as spam may have included personal calls to the individual previously assigned the number. Other types of calls may have been marketing calls (including those resulting from marketing materials we signed up for or calls solicited by the previous owner of the phone number).

The Total Texts column lists the total number of texts received, including personal and marketing text messages. The number of texts flagged as spam are those found in the "spam/blocked" folders on each Android phone, as well as any found flagged in the message inbox folder. Other possibilities are personal messages to the number's previous owner, including from business they may have conducted with the number, or messages they solicited. For this assessment, only the quantity of messages received and the number flagged as spam were recorded.

Observations and Analysis

We documented results related to percentage breakdown of various security and anti-spam/scam features on the OnePlus 11, Google Pixel 7, iPhone 14, and Samsung Galaxy S23 smartphones.

Spam Call Detection

The OnePlus 11 and Google Pixel 7 exhibit similar performance in detecting and flagging spam calls, with 65.43% and 64.84% respectively. This suggests both devices, utilizing Phone by Google, have robust anti-spam call algorithms, effectively identifying and notifying users about potential spam or fraudulent calls.

The iPhone 14 also performs relatively well in detecting spam calls, flagging 32.08% of calls. Although this percentage is not as high as the OnePlus 11 and Google Pixel 7, it still demonstrates an effort to protect users from unwanted calls.

The Samsung Galaxy S23 on its default dialer lagged significantly behind in spam calls detected, with only 9% of calls flagged as spam.

Spam Text Detection

Among the Android phones, spam text detection ranged from 27.27-30.77%. All Android phones used Messages by Google.

Conversely, the iPhone 14 did not flag any messages as spam. Notably, when the user opens a message, the iPhone by default sends a “This sender is not in your contact list” alert and gives the option to “report junk,” which will report the sending number to the carrier and Apple, and prevent the phone from receiving future texts from it.

These results are based on how many spam texts came in during the testing periods, as well as the devices’ abilities to detect them.

Variables Potentially Affecting Outcome

Differences in assessment results across phones may have been affected by several variables not accounted for in the testing scope. In addition, the landscape of spam and scam techniques is constantly evolving, and each device's security performance will change over time with software updates and improvements. Integrating the following variables in future testing could yield more robust results and help explain the current results:

1. Software and Algorithm Differences: Each smartphone manufacturer implements its own set of software and algorithms to detect and combat spam and scam attempts. Variations in the design and efficiency of these algorithms can lead to differences in spam/scam detection rates. The combination of Carrier and default application make a difference as they both introduce unique capabilities that help improve the detection capabilities on each device.

2. Updates and Patch Management: The frequency and regularity of software updates can significantly impact a device's security performance. For this testing, updates were made when they were pushed via update notification or automatic update in order to simulate "average user" interaction. Upon initial unboxing and prior to activation, all phones were updated via Wi-Fi connection. No beta or other test versions of phone operating systems were used in this test.

3. Integration of Third-Party Services: Some smartphone manufacturers may collaborate with third-party service providers for anti-spam and anti-scam solutions. The quality of these external services can vary, leading to differences in detection rates among different devices.

4. Geographical Variations: Anti-spam and anti-scam measures may be tailored to specific regions based on the prevalent types of scams and spam in those areas. Different devices might prioritize different types of threats depending on their target markets. In the current test, one factor that may have affected the outcome is that the Google Pixel 7 and OnePlus 11 were located in Fairfield, California for the testing period, whereas the iPhone 14 and Samsung Galaxy S23 were located in Fredrick, Maryland. However, more data would be needed to confirm this.

5. Time of year: The overall increase in calls was detected in May, June, and July, which are peak months for planning and taking vacations for many people in the US. It is possible that there were additional marketing pushes for late spring and summer.

    a. Theoretically, the increase in volume should have made little to no difference in the detection % for spam calls as the numbers should increase concurrently. This was the case between the Pixel and the OnePlus where the detection difference was less than 1%. The iPhone demonstrated decent protection, although because it is a different operating system, its results were somewhat expected. The true outlier is the Samsung, which performed worse than the other Android devices.

    b. Some of the Samsung's unsolicited calls were repeats from the same number(s). This could indicate a contact of the previous user who had the number, or a call list to which the previous user had opted in. This represents only a small percentage of the total calls to the phone, however.

6. Reused number: This testing was conducted with a number recognized as very active or hot. The total number of calls and texts received represents the calls and texts received for the duration that each phone was provisioned with the "hot" number. A portion of the calls and texts may

have been meaningful or useful to the previous user of the number; however, for the purpose of the test we determined that they would be logged as any other call without further parsing because they were:

a. Unsolicited, whatever connection to individuals or entities that the previous user of the number had to the messages received and calls logged had no bearing or connection to our use case and were not actively sought.

b. Unknown contacts, in the use case for our test and for every device tested, a known contact would not be considered spam. For call logging, this report shows total number of calls received regardless of source or number of repeats from same phone number, and number of calls flagged. For message logging, this report shows the total number of messages received regardless of source or repeat messages from the same phone number.

Appendix – Default Phone Settings

All phones had privacy settings available, including requiring an opt-in for location services, camera and microphone, app permission, advertising, and password storing.

Google Pixel 7

The Pixel 7 has the following privacy features embedded into the phone (see Figures 10, 11):

- Privacy dashboard: Users can view and manage permissions for each app installed on their device.
- Location services control: Users can choose when and how their location is shared with apps, including setting location sharing to "off" by default.
- Call Screen and screening calls: Users can customize these settings to screen spam or unwanted calls.
- App permission prompts: Users are prompted to grant permissions that allow apps to access features (e.g., camera, microphone).
- Google Play Protect: This feature automatically scans apps installed on the device for malware and security issues, protecting users from harmful apps.

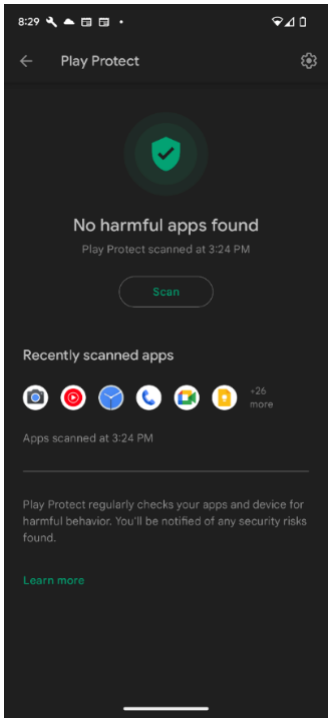


Figure 10. Google Play Protect on the Pixel

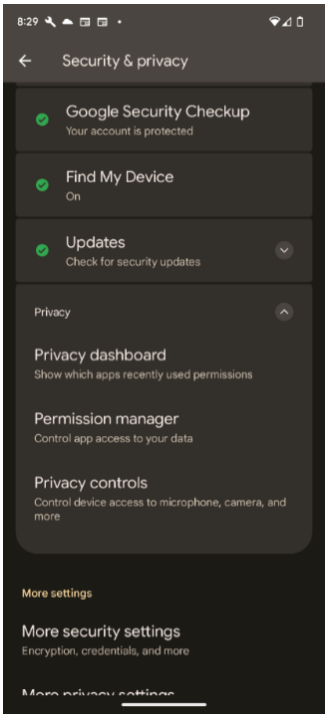
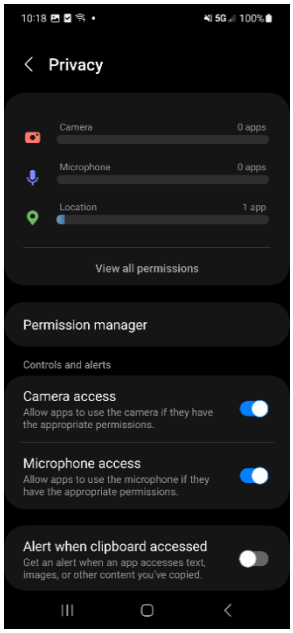


Figure 11. Security & Privacy Settings on the Pixel

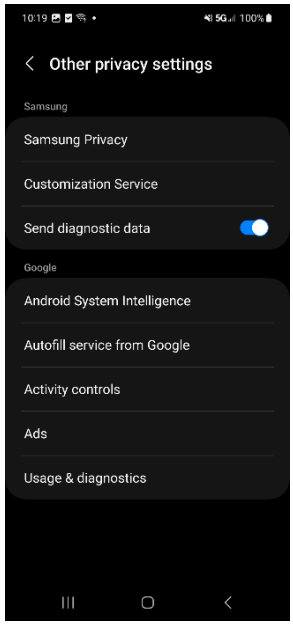
Samsung Galaxy S23

The Samsung Galaxy S23 has the following privacy features (see Figure 12):

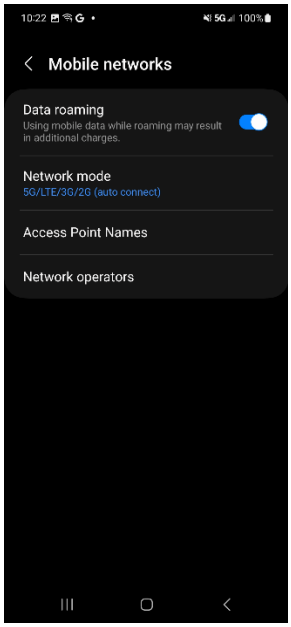
- The Samsung has Location Services active by default.
- For camera and microphone, user-based permissions prompts appear whenever a new app and site is used/visited for the first time.
- App permissions are managed via "Permission manager" in the privacy settings.
- Advertising is managed through the Google services setting through the associated Google account's advertising ID.
- Account security is by default managed by Google account security. However, there is an option to enroll in Samsung account security for additional features (e.g., find phone app synch, family sharing).[17]
- Privacy reporting is a dashboard in the privacy main screen.



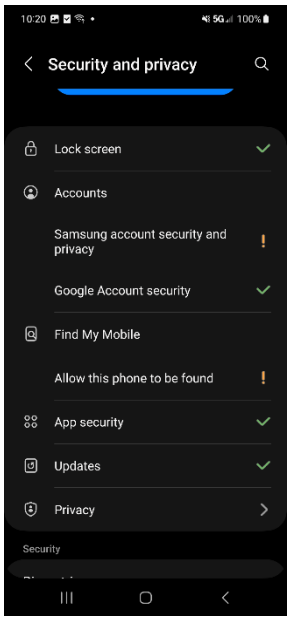
Default Privacy Settings



Default Privacy Settings (continued)



Default Call Settings



Default Security Settings ("Find my phone" disabled, Samsung account not signed up for to ensure factory "out of the box" settings in place)

[17] Samsung Account landing page with detailed overview of features. https://www.samsung.com/us/samsung-account-benefits/

Figure 12. Samsung Galaxy S23 default setting screens

OnePlus 11

The OnePlus 11 has the following privacy features:

- Privacy Dashboard: This dashboard contains information on app permissions and use of sensitive data (see Figure 13).
- App permissions: Users can control which apps have access to features such as location, camera, microphone, and contacts.
- Privacy alerts: OnePlus devices may provide alerts when an app is using a sensitive feature such as location, camera, or microphone.

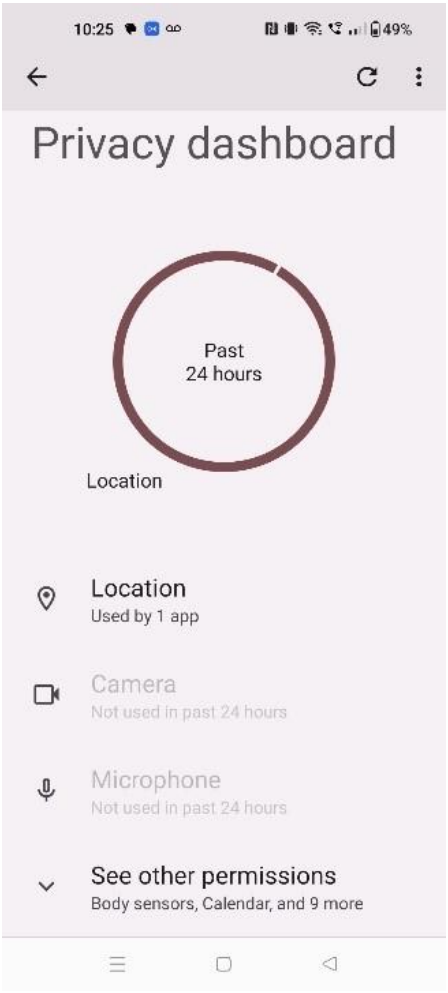
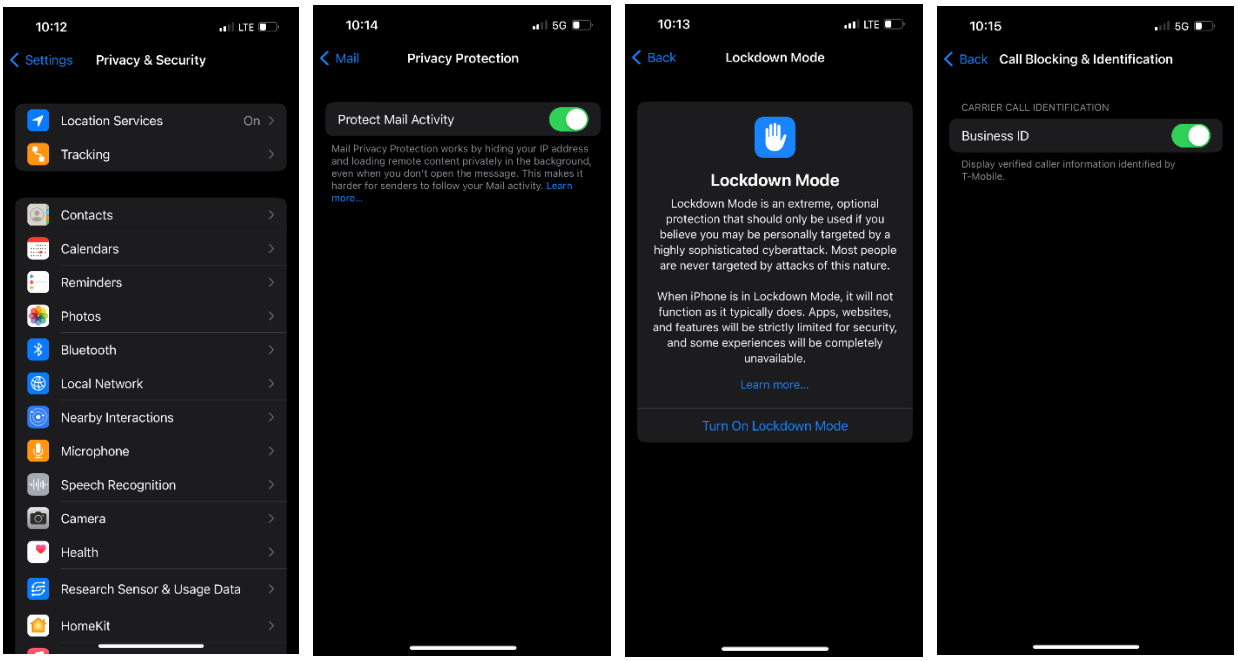


Figure 13. OnePlus 11 has a privacy dashboard that contains information about what applications are using microphone, location services, camera, and other permissions

iPhone 14

The iPhone 14 has the following privacy features (see Figure 14):

- For location services, camera, and microphone, user-based permissions prompts appear whenever a new app or site is used/visited for the first time.
- For each application, further individual setting adjustments are available through an App permission setting screen.
- "Personalized ads" are enabled by default via Apple advertising.
- Passwords are managed by the iCloud keychain, and a privacy report of all applications is available in the privacy settings. The iPhone also had a "Lockdown" mode that limits access to apps and sites.[18]



Default iPhone Security and Privacy Settings Screen 1	Email Protection enabled by default	Lockdown mode Setting screen disabled by default	Carrier call identification enabled by default

Figure 14. iPhone 14 privacy feature screens

[18] Apple's Lockdown mode explained, https://support.apple.com/en-us/HT212650