Publication date:
30 Dec 2025
Author(s):
Aaron West, Senior Analyst, Consumer Electronics and Display Applications
Hollie Hennessy, OT/IoT Cybersecurity Lead

Mobile Device Security Scorecard – 2025 Report

Omdia
by informa techtarget

Table of Contents:

© 2026 Omdia. All rights reserved. Unauthorized reproduction prohibited.

Executive summary: Google leads the smartphone industry in security feature testing for a fifth year

In the fifth annual Omdia Mobile Device Security Scorecard, leading global flagship devices from six of the largest smartphone manufacturers were compared on key security features, including security updates, network security, and anti-malware protection. Google's Pixel 10 Pro, Samsung's Galaxy S25, and Motorola's Moto Edge 60 Pro all scored highly, ahead of Apple's iPhone 17 Pro Max and other leading Android-based devices, including the OnePlus 13 and Xiaomi 15 (see **Table 1**). The Google Pixel 10 Pro scored the maximum marks in all categories except anti-phishing protection, where all tested devices failed to catch some of the phishing attempts used during testing.

Table 1: Smartphones rated for their security features

© 2026 Omdia. All rights reserved. Unauthorized reproduction prohibited.

Security feature	Consumer importance weighting	Google Pixel 10 Pro	Samsung Galaxy S25	Motorola Moto Edge 60 Pro	OnePlus 13	Apple iPhone 17 Pro Max	Xiaomi 15
Security updates	100	100%	100%	75%	75%	75%	75%
Network security	100	100%	100%	100%	50%	75%	50%
Anti-malware protection	100	100%	100%	75%	75%	75%	75%
Identity protection	100	100%	75%	100%	75%	75%	25%
Anti-scam and phishing protection	100	75%	50%	75%	75%	25%	25%
Hardware security	75	100%	100%	75%	75%	75%	75%
File & photo protection	75	100%	100%	100%	100%	75%	100%
Secure backups	75	100%	75%	100%	100%	75%	50%
Security awareness and remediation	50	100%	100%	75%	75%	50%	75%
Lost device protection	50	100%	100%	100%	100%	75%	75%
Physical access control	50	100%	75%	100%	75%	100%	50%
Parental controls	25	100%	100%	100%	100%	100%	100%
Total		97%	88%	88%	78%	70%	60%

Notes: Consumer importance weighting based on a survey of 1,582 consumers in October 2025. Scores in

© 2026 Omdia. All rights reserved. Unauthorized reproduction prohibited.

each category are out of 100%, with the total being out of 100% based on the weight of each category.
© 2025 Omdia

Source: Omdia

The ratings for each feature category are based on hands-on testing by Pen Test Partners and are then combined with consumer importance weightings to produce a total score out of 100%. The consumer importance weighting is based on an October 2025 survey of 1,582 consumers who use a smartphone acquired within the last three years, where we asked them to rate each security feature category on how important they were. A full list of security feature categories and their definitions can be found in **Table 2**.

Key testing findings

The Google Pixel 10 Pro is the industry leader for consumer security features on smartphones, scoring the best or joint best in all categories. Multiple additional security features have been added to all devices since last year's Mobile Device Security Scorecard, improving the protections in place for users. Google has pushed several of its own features to other Android devices, increasing their level of security, with fewer manufacturers choosing to implement their own features and instead opting to use Google's improved option.

Google only lost marks in anti-phishing and scam protection—a category where no phone tested scored full marks due to a lack of protection against more sophisticated and manual phishing attempts. This means all phones tested were susceptible to custom payloads from unknown senders across SMS and email. However, all also had some level of safe browsing checks, meaning that even if messages could be received and were not flagged as spam, users would have a second level of protection in the browser.

Offering seven years of security update support, Google and Samsung are joint leaders in the industry for the length of commitment to security updates, also offering updates monthly rather than bimonthly, as Motorola and Oppo do, or every 90 days, as Xiaomi does. For the first time, following the introduction of the EU's ecodesign legislation (Ecodesign for Sustainable Products Regulation (ESPR)) in place since June 2025, all devices offer a set end-of-life date published by the manufacturer.

Samsung's Galaxy S25 scored highly with the second-highest total score. It received full marks in most categories, including hardware security and network security. Anti-phishing and scam protection, secure backups, and physical access control were the three categories where Samsung had room for improvement. It's unclear if the Messages app uses advanced natural language checks, and it does not show a permanent recording indicator when the screen is being shared. Samsung's own backup service through Samsung Cloud doesn't have full end-to-end encryption enabled by default for larger file sizes. The biometric access lockdown mode is also not available in the power menu by default, needing to first be enabled in settings for it to appear.

Apple's iPhone is very different from other phones due to having its own iOS and App Store. These offer a good level of protection in many categories, but also have clear areas for improvement. Most notably, improvement is needed in anti-scam and phishing protection, where its own messages, phone, and mail apps lean more toward personal privacy over security protection, with no analysis of user or sender information to flag potential malicious contacts. Even the most basic phishing messages and emails that were detected and flagged by all other Android devices were left unflagged

© 2026 Omdia. All rights reserved. Unauthorized reproduction prohibited.

by the iPhone. Apple is also the only smartphone vendor not to offer any snatch protection on its devices.

The Motorola Moto Edge 60 Pro leans heavily on Google's security features and services. Motorola does not ask you to create an account with them when first using it, unlike all other devices, instead asking for your Google account. As such, it offers the same strong level of security features and protections in many categories as the Pixel. Two areas where it is weaker are security updates and hardware security. As the cheapest phone tested, it has the shortest length of software support, with four years of bimonthly security updates. It is also the only phone tested to use a MediaTek system-on-chip (SoC), with no specific information on security processing being done separately in its own physically distinct core.

Similarly, the OnePlus 13 uses many of Google's security features and services as part of its OxygenOS, which is based on Android. It offers its own OnePlus account and security, prompting this when setting up the device for the first time, but this doesn't offer the same rigorous security features as a Google account, with no security audit page or password manager, and no ability to save passkeys. However, users have the option of setting up a Google account on the device, from which they can access all omitted features.

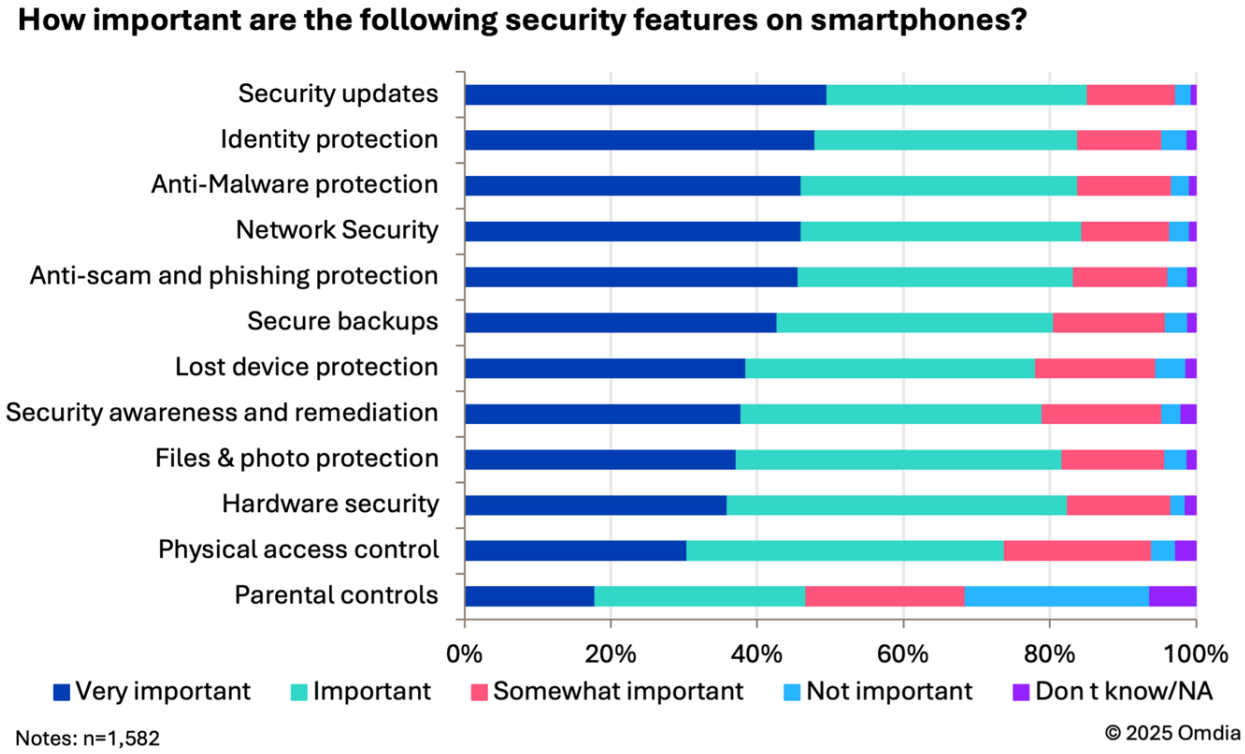
The Xiaomi 15 scored the lowest overall in testing, with the worst provisioning of security features in multiple categories. It often leaned on its own first-party Xiaomi Cloud and related Mi features and services by default, lacking the same protections as the Google services used on many other Android devices. These Xiaomi services didn't offer mandatory two-factor authentication (2FA) and only included basic features with no security checks. It is also the only device tested not to have any screen-sharing protections.

Key survey findings

In October 2025, we surveyed 1,582 consumers who had bought a new phone in the past three years, asking how important the tested security features are to them. The most important security features include security updates, identity protection, anti-malware protection, network security, and anti-scam and phishing protection (see **Figure 1**, based on the percentage of responses that stated "very important" or "important"). These findings are consistent with previous years, where anti-phishing and anti-malware are ranked highly, although security updates and network security have risen in importance compared to previous years, possibly due to greater awareness of security update support periods as mandated by governments, including the EU Ecodesign regulation from June 2025 and the UK PSTI Act in April 2024.

© 2026 Omdia. All rights reserved. Unauthorized reproduction prohibited.

Figure 1: Most important security features



Source: Omdia Mobile Device Security Consumer Survey 2025

These importance ratings also mirror the most common security issues reported in our survey, with phishing scams and malware or viruses being reported by 27% and 26% of respondents, respectively. Unfixed security bugs and vulnerabilities and stolen personal data and leaked passwords were also common issues faced, with between 17% and 18% experiencing this.

Fortunately, consumers generally had high confidence in their phone's level of security, with ratings of how effective their phone is in each category corresponding to the most important categories; 33% believe their smartphone is "very effective" at providing security updates, the highest of any in our survey, followed by secure backups (31%) and network security (30%).

Table 2: Security feature categories covered in Omdia's consumer survey and testing

© 2026 Omdia. All rights reserved. Unauthorized reproduction prohibited.

Feature	Description
Anti-scam and phishing protection	A set of tools that help stop bad actors from using fraudulent emails, texts, or phone calls to scam individuals into revealing personal information such as passwords and credit card numbers.
Anti-malware protection	A set of tools to detect and prevent software that is specifically designed to disrupt, damage, or gain unauthorized access to your smartphone and the data that resides on it. Spyware is a form of malware that aims to gather information without the user's knowledge.
File and photo protection	The ability to provide an additional layer of protection for various files or photos that may be stored on your device.
Identity protection	A set of tools that helps you generate and store passwords securely for all of your apps and websites, and proactively notifies you if any of your previously used passwords have been leaked or stolen so that you can immediately change them. It also includes the ability to leverage multiple factors (something you know and something you have) to protect your identity.
Hardware security	Using the smartphone hardware to offer higher levels of protection for sensitive data that resides on your device.
Lost device protection	The ability to locate, track, lock, or even remotely wipe a lost or stolen device using a website or another device, such as a family member's or friend's smartphone, computer, or tablet.
Network security	The ability to protect the communications from your smartphone to various cloud services and your connection to the internet overall. Network security ensures your transfer of data over the internet won't be intercepted or spied on.
Security updates	A security update fixes issues that your smartphone's software has that could be used by bad actors to corrupt your device or steal information from it.
Secure backups	The data backed up from your device is protected (using encryption) while it's being transmitted off your device to various cloud services. This data is also protected while residing in the cloud service.
Physical access control	The ability to prevent bad actors from gaining unauthorized access to your device by either presenting an artificial copy of your fingerprint or by repeatedly trying to guess your passcode.
Security awareness and remediation	A central location on your device that warns you about potential security-related issues and provides steps to remedy those issues.

© 2026 Omdia. All rights reserved. Unauthorized reproduction prohibited.

Parental control	A set of controls that allow you to configure and set various restrictions on your children's smartphones and the services/apps that run on them.
	© 2025 Omdia

Source: Omdia

Full security testing results by category

Security updates

For this category, manufacturer commitments to the length and frequency of security updates were checked. Devices were also tested to check how updates are pushed to users, including the ability to schedule updates later and prompts to update and reboot.

Google and Samsung have the longest security update commitments of any smartphone vendors, supporting the Pixel 10 Pro and Galaxy S25 for seven years from launch.

For the Pixel, this includes updates in regular feature updates called Pixel Drops, meaning the Pixel will be supported up to Android 23. Security updates are released monthly to Pixel devices, and although they apply to all Android devices, Google's own Pixel devices regularly get them faster than third-party manufacturers. Some aspects of device security on the Pixel are also handled by different systems outside of the operating system updates, such as Google Play Services, meaning Google can quickly push fixes without requiring full system updates.

Samsung devices get monthly updates at first before moving to quarterly and biannually as they get older. Samsung keeps a public list of these groups and makes it clear to users. As such, both Google and Samsung score 100% in this category.

Apple has specified that the iPhone 17 Pro Max will be supported for a "minimum of five years," specifically from the end of sales, to comply with the new EU Ecodesign Directive. Apple deploys security updates through Rapid Security Responses separately from core operating system updates, but not on any specific schedule. However, there is some inconsistency between Apple devices in how long they are supported and when they receive updates. Due to this and the shorter update period than Google and Samsung, the iPhone 17 Pro Max has a slightly reduced score of 75%.

The Xiaomi 15 and OnePlus 13 are both supported for six years. However, for both, this information is not readily available to consumers at the time of purchase. Xiaomi only confirms the six years of support through Google's Android Enterprise Recommended standard, also specifying that the Xiaomi 15 will get updates every 90 days. OnePlus published the information in a community post made by the OnePlus Software Team, but with no specific information on how regular the updates would be. Based on previous OnePlus models, the updates are likely pushed bimonthly. Despite having a long support period of six years, both Xiaomi and OnePlus have a slightly reduced score of 75% due to the lack of easily accessible and clear information to consumers.

The Moto Edge 60 Pro has the shortest support period of four years of bimonthly updates, although it is not clear whether this is only for security updates or if it includes features. This information was also not readily available to users, with Motorola only confirming it in their forums and not advertising it alongside the device like other manufacturers. Following the EU's Ecodesign regulation minimum of

© 2026 Omdia. All rights reserved. Unauthorized reproduction prohibited.

five years of support, Motorola will likely update this information with an extended support period. For now, though, Motorola receives the lowest score of all devices in this category with 50%.

All devices in testing prompt security updates in similar ways, proactively prompting users to install the update and reboot the device. Also, they all allow you to schedule the update and reboot to a more convenient time, with all except the Samsung giving an option to do it overnight, while the Samsung lets you choose a specific time.

Network security

For each device, a practical test was done to attempt to intercept the system and application traffic, noting any warnings shown on the device to the user. The settings for eSIM support and additional network security features were also checked, such as the ability to disable 2G, browser warnings for unencrypted connections, and warnings for insecure Wi-Fi networks.

All of the phones acted very similarly in testing, with few differences. Traffic interception was possible on all of them, though with Android devices not fully trusting user certificates by default. Unless an app explicitly trusts user certificates, its traffic cannot be decrypted. Device modification is required to install system certificates, increasing the difficulty. While the iPhone allows certificates to be installed and used without any system modification, this would have to be proactively routed by the user and, as such, poses minimal security risk.

One of the few key differentiators among tested devices was the setting to disable 2G traffic. This poses a security risk to users due to its weak encryption and lack of mutual authentication. The Google Pixel 10 Pro and Motorola Moto Edge 60 Pro both have a direct on-off setting for 2G and therefore score 100%. Samsung also has a setting to disable 2G through its Advanced Protection Options and scores 100%. The iPhone only allows you to disable 2G through Apple's Lockdown Mode, therefore scoring 75%. The Xiaomi and OnePlus do not have any 2G settings and therefore score 50%.

Anti-malware protection

For this category, devices underwent a thorough review of documentation and settings, including the ability to sideload, the ability to enable or disable other protections such as anti-malware, and checks of various levels of USB protections. In testing, a known malicious app was attempted to be installed on each device, with all warnings and checks noted. If the app was able to be installed, then the device's actions after installation were also noted. While the malicious app did not attempt any zero-click exploits or advanced attacks, documentation was reviewed to check for zero-click exploit protection.

While it can be done in a restricted manner, for instance, through stolen enterprise developer certificates, Apple does not allow sideloading in much of the world. As the average consumer is unlikely to do so, this was not tested on the iPhone 17 Pro Max. Third-party app stores have now been made available in the EU following anti-competition lawsuits; however, these stores still require strict approval from Apple and must perform their own checks, and, therefore, sideloading is restricted. These checks, prior to apps being made available, essentially replace the anti-malware checks being performed on the device. For this reason, we haven't penalized the iPhone 17 Pro Max for a lack of anti-malware protection. The phone has USB protections by default, as Apple is increasingly strict and disables accessories after a set amount of time on the lockscreen, with access to data only possible when unlocked and after entering the device's passcode. The iPhone loses some marks in this category due to a lack of behavioral analysis on apps after they are installed, although it does have

© 2026 Omdia. All rights reserved. Unauthorized reproduction prohibited.

some zero-click exploit protection and has rapid security response updates in retaliation to new exploits being created.

All other phones accept sideloading applications but have effective anti-malware checks through Google Play Protect as well as their own proprietary checks, such as Motorola's ThinkShield. All devices successfully caught the malicious application that was attempted to be installed during testing, successfully warning the user at multiple stages. All allowed the installation to continue, even after the malware was detected; however, many warnings are in place. The Google Pixel 10 Pro and Samsung Galaxy S25 also have extra protections against zero-click exploits and perform regular behavioral checks on applications after installation. As such, they get a full 100% score, while Motorola, Xiaomi, and OnePlus receive 75%.

Identity protection

For this category, each device's account sign-up during setup was checked, as well as account management through the device settings. Where web access to accounts was possible, the options available were also confirmed on a desktop, as features can vary.

All Android phones support using a Google account for identity features, which provides a good level of protection. This includes comprehensive 2FA options, trusted device support, a full audit trail of account activity, a list of all signed-in devices, security check-up notifications, active password health checks, and passkey support. As this is the default and proactively promoted account manager for the Pixel 10 Pro and Moto Edge 60 Pro, both score 100%.

The other Android devices have their own account management options by default, on top of Google as a backup option. The Xiaomi account app is used for device backups and other sensitive data but lacks even fundamental security measures, such as basic 2FA options or a password manager, leaving users at risk. As such, the Xiaomi 15 scores 25%. OnePlus also had its own account app, but it actively defaults to Google services for security; as such, the OnePlus 13 scores 75%. The Samsung account manager included all features except for a proactive checker for password compromise; as such, the Galaxy S25 scores 75%.

The iPhone 17 Pro Max links with the user's Apple accounts to allow access to iCloud features for identity protection: storing backups; supporting all 2FA options except calling, with backup codes and trusted contacts; proactive password management and compromise checking; and passkey support. However, iCloud lacks any audit history or security check-up functions, so the iPhone 17 Pro Max scores 75% in this category.

Anti-phishing and scam protection

For this category, each device's documentation, as well as the settings of the default SMS and phone apps, was reviewed. Email, SMS, third-party messengers, and voice calls were all tested with both basic and more advanced phishing attempts—basic being a more generic approach with known malicious URLs or content, while advanced tests used custom content and attempts to bypass protections. Screen-sharing protections were checked with hands-on testing, while documentation was used to check for deepfake protection.

The Pixel 10 Pro, Moto Edge 60 Pro, OnePlus 13, and Xiaomi 15 all use Google Messages and its phone and email applications, with the same results across all in the phishing tests. Basic attacks using known malicious content or URLs from unknown senders that are known for sending spam were

© 2026 Omdia. All rights reserved. Unauthorized reproduction prohibited.

caught in all cases. In more advanced testing, using custom content and custom URLs without any known spam history, the phishing attempt was not detected, the links stayed clickable, and no warning was shown to the user.

Google advertises its own “Scam Detection” system for natural language checks, using local on-device AI to analyze messages and calls. This includes during phone calls, with an alert appearing during the call if it suspects it’s a scam. However, it’s not clear whether natural language checks and Scam Detection in its Messages app are available on non-Pixel devices yet.

The Samsung Galaxy S25 uses Google’s Messages and email apps but uses its own first-party phone app, differentiating it from other Android phones in testing. This Samsung phone app has its own caller ID and spam protection provided by a third-party (Hiya). Samsung also has its own internet browser, but it still utilizes Google’s Safe Browsing to flag potentially malicious links.

The iPhone 17 Pro Max is standalone in using Apple Messages and its phone and email apps, with no alternatives given. Apple’s approach favors privacy over security, not analyzing messages or sender information, and therefore not flagging even the basic SMS and email phishing attempts used during testing. For this reason, it receives a 25% score in this category.

All phones in testing, except the Xiaomi 15, had some form of screen-sharing protection, obfuscating one-time passwords from being shared, with a clear way of ending the screen sharing. Samsung did not have a clear recording indicator during screen sharing, although it did display a symbol that the microphone was in use and a silent notification to end the recording, resulting in a reduction in its score in this category from 75% to 50%. Due to the Xiaomi phone having no screen-sharing protections, it received a 25% score.

As no device detected the advanced phishing attempts during testing, and all lacked the latest protections, including deepfake detection during video calls, the highest score achieved in this category (by the Google Pixel 10 Pro, Motorola Moto Edge 60 Pro, and OnePlus 13) was 75%.

Hardware security

For this category, each device’s published documentation was reviewed, including the documents of the manufacturer of the device’s processor or SoC, reviewing rooting and jailbreak protections as well as firmware integrity checks.

The Google Pixel 10 Pro and Samsung Galaxy S25 both have two layers of protection. The Pixel has a Tensor Security Core within the main SoC and a separate Titan M2 security coprocessor, which is physically separated with increased security for keys and device encryption. The Samsung S25 has a Qualcomm SoC, which has a secure processing unit and a physically separate Knox Vault chip for handling sensitive data such as biometric authentication, PINs, and passwords. As such, both phones score 100% in this category.

The iPhone 17 Pro Max uses an Apple A19 Pro chipset, which has its own security chip, the Secure Enclave, isolated from the main processor but located on the main SoC. Apple has increased the capability of the Secure Enclave over time, adding features such as replay prevention to the subsystem. Apple has a strict Secure Boot process, which provides a hardware root of trust that cannot be altered by attackers, as it contains the signing key for the subsequent parts of the boot sequence. This effectively means that Apple has strong full firmware verification, preventing modifications by users or attackers, such as jailbreaks. While this is excellent protection, due to not

© 2026 Omdia. All rights reserved. Unauthorized reproduction prohibited.

having its own dedicated and physically separate security chip, the iPhone receives a score of 75% in this category.

The Xiaomi and OnePlus are functionally identical from a hardware security perspective, both using a Snapdragon 8 Elite chipset with the same dedicated security features, such as Qualcomm's Secure Processing Unit, TEE, and Secure Boot process. The devices, by proxy of being Androids, also include the ability to use SafetyNet for integrity checks during use in the same way as the Pixel and use Verified Boot to ensure system images are legitimate and signed. However, with no increased level of dedicated security processing, both phones get a score of 75%.

The Moto Edge 60 Pro is unique among tested devices because it uses a MediaTek SoC. This also separates processing of sensitive information from the main processor, but still on the same SoC and not physically distinct. Motorola also implements Lenovo's ThinkShield for mobile, which includes secure boot protections linked with their hardware and a root of trust protection. This includes firmware verification and boot process integrity checks. However, there is also limited information available on the implementations Motorola has chosen. This is on top of the device being an Android device with Google's SafetyNet for integrity checks. As such, the Moto Edge 60 Pro receives a score of 75% in this category.

File and photo protection

Each device's settings were reviewed to determine whether users can add additional security layers to protect files, photos, and apps, using either passwords or PINs.

The Pixel 10 Pro offers photo protection through Google Photos, allowing users to create a locked folder and use the device's passcode to protect it. Files are protected when using the Safe Folder feature, while apps can be protected through the Private Space feature or app pinning. As such, Google gets a full 100% score in this category.

The Motorola Moto Edge 60 Pro and OnePlus 13 lean on Google services and features, having the same protections in place and also earning a full 100% score.

Samsung uses Google Photos but has its own Gallery and My Files applications, which both offer a Secure Folder feature, allowing you to lock files, photos, or apps away with a custom credential. As such, the Galaxy S25 also gets 100%.

Xiaomi uses Google Photos and Files apps and has the same features in place, but relies on its own application for apps called App Lock. This puts an extra layer of protection on apps with a basic pattern passcode, with the options for biometrics and longer passwords—also scoring 100%.

Apple has a hidden section for photos within the Photos app on iOS, but it is limited to using the device's screen lock to unlock it. The Files app doesn't have an option to lock or hide files. Apps can be protected by a long press on their icon and enabling an option such as "Require Face ID." This is also limited to the screen lock options. Technically, by locking the Files app, files by proxy can be protected, but it would simply block access to the entire app. Therefore, the iPhone 17 Pro Max receives a slightly penalized score of 75% in this category.

© 2026 Omdia. All rights reserved. Unauthorized reproduction prohibited.

Secure backups

For this category, documentation for each device was reviewed to confirm the level of encryption used in backups, as well as whether the encryption was only in transit or if it was end-to-end encryption. Further settings were also reviewed for more advanced security measures.

Each device supported thorough backup options that cover most of the content on the device, from settings and messages to app content. All devices but the Xiaomi 15 offered end-to-end encryption on their default backup option. While you can use Google's backup service on the Xiaomi 15, the default Xiaomi Cloud option must first be disabled; therefore, it receives a penalized score of 50%.

The level of end-to-end encryption varies across providers, though, with it not being enabled by default on Apple and Samsung's backup services. Apple's Advanced Data Protection for iCloud allows more secure end-to-end encryption, but this is an opt-in service. Samsung Cloud also offers a service, but some files cannot be encrypted, such as miscellaneous file sizes larger than 1GB. For these reasons, the iPhone 17 Pro Max and Samsung Galaxy S25 both score 75%.

The Pixel 10 Pro, OnePlus 13, and Moto Edge 60 Pro all use the Google services by default, which encrypt all backups in transit, with further protection on devices using the screen lock as a key. The encrypted backups include SMS and MMS messages, call history, device settings, apps and app data, and photos and videos. As such, these devices all score 100% in this category.

Security awareness and remediation

The settings app on each device was reviewed for its security information and monitoring features, often found together in a security hub page, including features such as automatic revocation of unused permissions and advanced protection options for users who prefer higher security measures.

Both the Google Pixel 10 Pro and Samsung Galaxy S25 have comprehensive security hubs that offer helpful information to users, automatically revoke permissions for unused apps, and have a heightened advanced protection option. For Samsung, its advanced protection falls under "Auto Blocker," and for Google Pixel, this is the "Advanced Protection" feature, which is available on Android from Android 16. As such, both devices score 100% for this category.

The Motorola, Xiaomi, and OnePlus devices have similar security hubs in their settings, as is standard for Android devices, but lack the more advanced security modes that the Samsung and Google devices have. Therefore, these three devices get a reduced score of 75%.

The iPhone 17 Pro Max doesn't have a centralized security page, with security settings instead scattered across many different apps and pages. Also, iOS doesn't revoke permissions automatically for unused apps. Due to this, Apple scores the lowest in this category with 50%.

Apple has an Advanced Data Protection mode and a further option called Lockdown Mode, limiting insecure network connections, USB connections, web browsing, and other areas to increase the security of the device. However, due to restrictions imposed by the UK government, Apple can no longer offer its Apple Account Advanced Data Protection to new users, limiting the available security options.

© 2026 Omdia. All rights reserved. Unauthorized reproduction prohibited.

Lost device protection

Each device was tested for its ability to be locked, located, or tracked when lost. Both the on-device settings and web settings were checked, as well as additional protections such as offline location tracking, device wiping, lockdown measures, snatch protection, and unwanted tracker alerts.

Every device tested had a full suite of lost device and tracking features, offering options to locate, lock, and show messages received by the device on both a mobile app and a web interface. All devices also include factory reset protections, with accounts being required to reset the device fully to stop the stolen device from being reused. All Android devices had access to Google's lost device service, with it being the default option on the Pixel, Motorola, and OnePlus. The Samsung Galaxy S25 also had access to Google's service, but Samsung's own Find My Mobile was the default. These all had a full suite of features, including offline tracking, snatch protection, and more, all scoring 100% in this category.

Xiaomi also offers its own service as the default, although this lacked some features compared to Google's, such as not allowing offline location of the device, and as such, scores 75%.

The iPhone 17 Pro Max uses Apple's Find My feature, which has a strong level of features for unwanted tracker alerts, offline location detection, factory reset, and more. Snatch protection is the only feature missing from the iPhone for now, and therefore, it scores 75%.

Physical access control

Each device's biometrics and unlock pins and password options were checked, including practical tests for lock screen throttling and disabling biometrics. These included options shown during the initial device setup, as well as further options given through the device's settings after setup.

The application of biometrics is similar across all devices. All support face recognition, although Apple's Face ID is the only one to use more advanced 3D face mapping. The iPhone lacks any fingerprint reader, though, while all Android devices offer a range of options for fingerprint recognition, including being able to register multiple fingers. The Google, Samsung, OnePlus, and Xiaomi devices have more advanced ultrasonic fingerprint readers, while the Motorola has an optical fingerprint reader. The pros and cons of each face and fingerprint biometric sensor were not within the scope of our testing, so the devices were not penalized for having different biometric options.

Therefore, one of the few key differences across devices was whether they offered a setting to temporarily disable biometrics. Having this option is useful for users who want to prevent their own face or fingers from being used to unlock it without their consent. The Pixel 10 Pro, iPhone 17 Pro Max, and Motorola Moto Edge 60 Pro all have quick-access lockdown modes through the power menu, which can be activated from the lock screen. As such, all score 100%.

The Samsung Galaxy S25 also had a biometric lockdown mode, but this is off by default and must be activated in settings before appearing in the power menu; as such, it scores 75%.

The Xiaomi and OnePlus had no such lockdown mode options, scoring 50%.

© 2026 Omdia. All rights reserved. Unauthorized reproduction prohibited.

Parental controls

Each device's parental control options were reviewed and then enrolled with a "parent" and "child" account to test whether the features functioned as intended. These parental controls include the ability to restrict certain services and apps, as well as set device controls.

All devices offered in-depth parental control options, including managing app access as well as limiting other services, such as web browsing and messaging. All Android phones supported Google's thorough Family Link feature, with some also offering their own options with varying functionality. Apple's Family Sharing allows connecting families on an account level, with similar features as Family Link for device restrictions. All devices get a full score of 100% in this category.

Mobile security consumer survey

About the survey

In October 2025, we surveyed 1,582 consumers who had bought a new smartphone in the past three years about their security concerns and perceptions. Respondents participated from the following countries and territories: the US, China, Germany, India, the UK, Canada, France, Italy, Spain, Australia, Ireland, Japan, Singapore, and Taiwan.

The aim of the survey was to better understand the demographic makeup of smartphone users and understand their security concerns and attitudes, the most common security threats, and key smartphone purchasing drivers.

Key consumer demographics

Users of 22 different smartphone brands were surveyed, with most owning either an Apple iPhone (38%) or a Samsung (31%), followed by Xiaomi (8%), Google (5%), Motorola (4%), and Oppo (3%)—covering all brands tested. We also asked users which brands they were familiar with to gauge brand awareness. Apple had the highest brand awareness, with 75% of respondents saying they were familiar with the brand, followed by Samsung at 66% and Google at 45%.

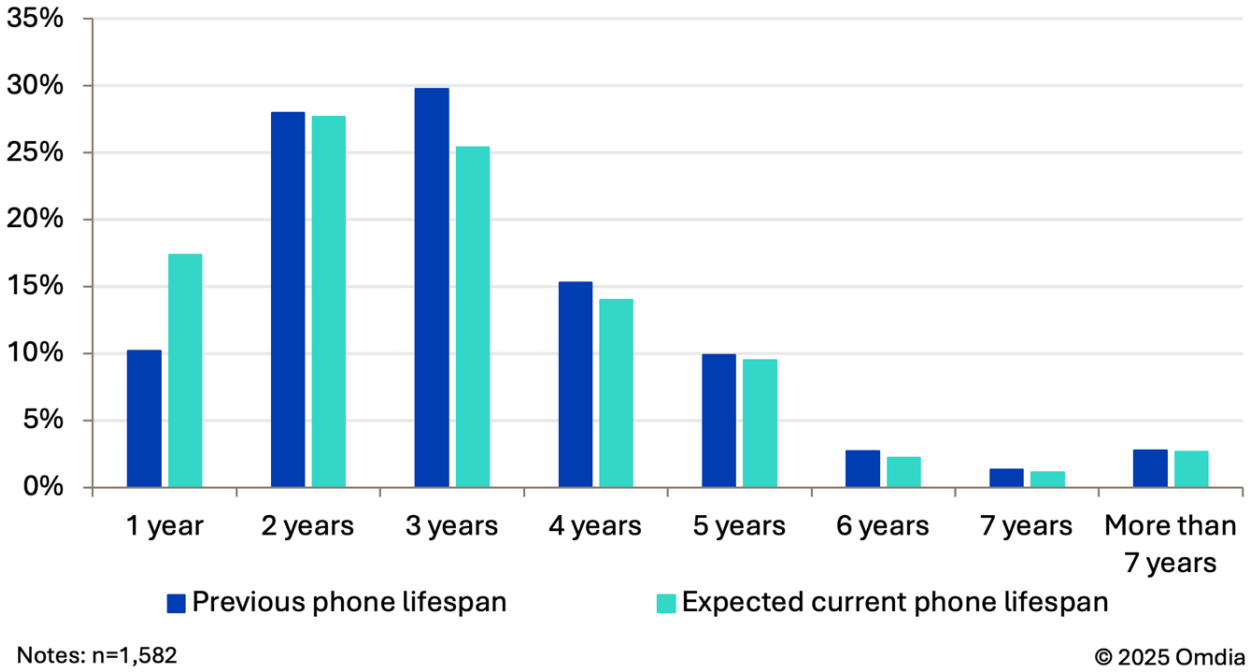
We asked how long consumers kept their previous phone and how long in total they expected to keep their current phone (see **Figure 2**). Most kept their previous phone for either two years (28%) or three years (30%), but many kept it for longer, with 17% keeping their previous phone for five years or longer. This continues to increase year-on-year, from 8% in our 2024 survey and 5% in our 2023 survey. This comes as more phones have longer support update periods, with the Samsung Galaxy S24 and S25 series and the Google Pixel 8, 9, and 10 devices all getting seven years of updates from the launch date. However, many low-end devices still only get two or three years of support from launch, which could put some phone users at risk without security update support on their phones. In June 2025, the EU introduced the Ecodesign Directive, which mandates that all smartphones must be supported with five years of updates from the end of sell-in of that model, meaning that most phones will need at least six years of security updates to be sold in the region.

The reported expected lifespan of current phones largely mirrors that of previous devices, but more people expect to replace their current phone after one year than keep their last phone for one year (17% versus 10%). This suggests that, while more people are keeping their phones for longer than five years, others are expecting to upgrade sooner. This could also be impacting the importance ratings of

© 2026 Omdia. All rights reserved. Unauthorized reproduction prohibited.

security features in the survey, with more rating security updates as of critical importance than in previous years—possibly, as updates are being supported for longer, people keep their phones for longer and view update support as very important.

Figure 2: Consumer smartphone replacement cycle

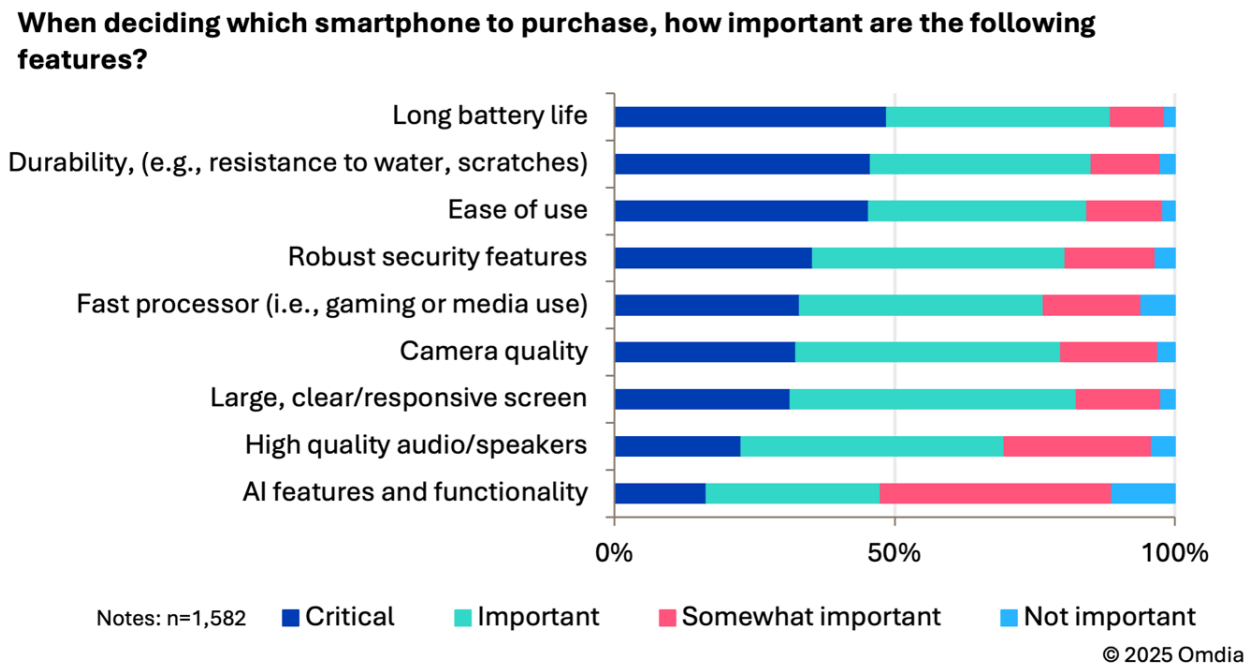


Source: Omdia Mobile Device Security Consumer Survey 2025

When asked to rate smartphone features by their importance when purchasing, a long battery life, durability, and ease of use were the most important features, with more than 40% of respondents saying they were critical (see **Figure 3**). Robust security features were also rated highly, with 35% saying they were critical and 45% saying they were important. The least important feature to consumers is AI features and functionality, with the lowest number rating it critical or important (16% and 31%, respectively), and most rating it as not important to their purchase at all (11%).

© 2026 Omdia. All rights reserved. Unauthorized reproduction prohibited.

Figure 3: Consumer smartphone purchase driver importance ratings



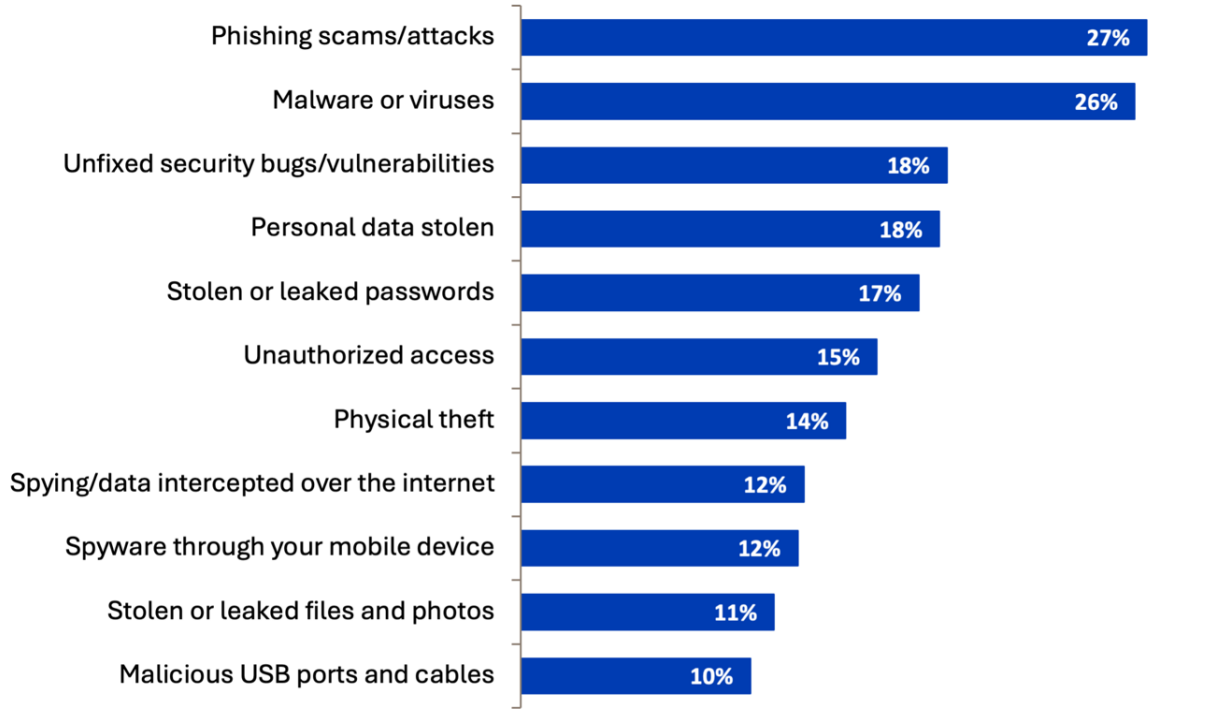
Source: Omdia Mobile Device Security Consumer Survey 2025

Consumer security behavior

The two most common security issues reported in our survey were phishing scams and malware or viruses, with 27% and 26%, respectively, experiencing these security threats (see **Figure 4**). Unfixed security bugs and vulnerabilities, stolen personal data, and leaked passwords were also common issues faced, with between 17% and 18% experiencing this.

© 2026 Omdia. All rights reserved. Unauthorized reproduction prohibited.

Figure 4: Incidence rate of consumer security issues



Notes: n=1,582

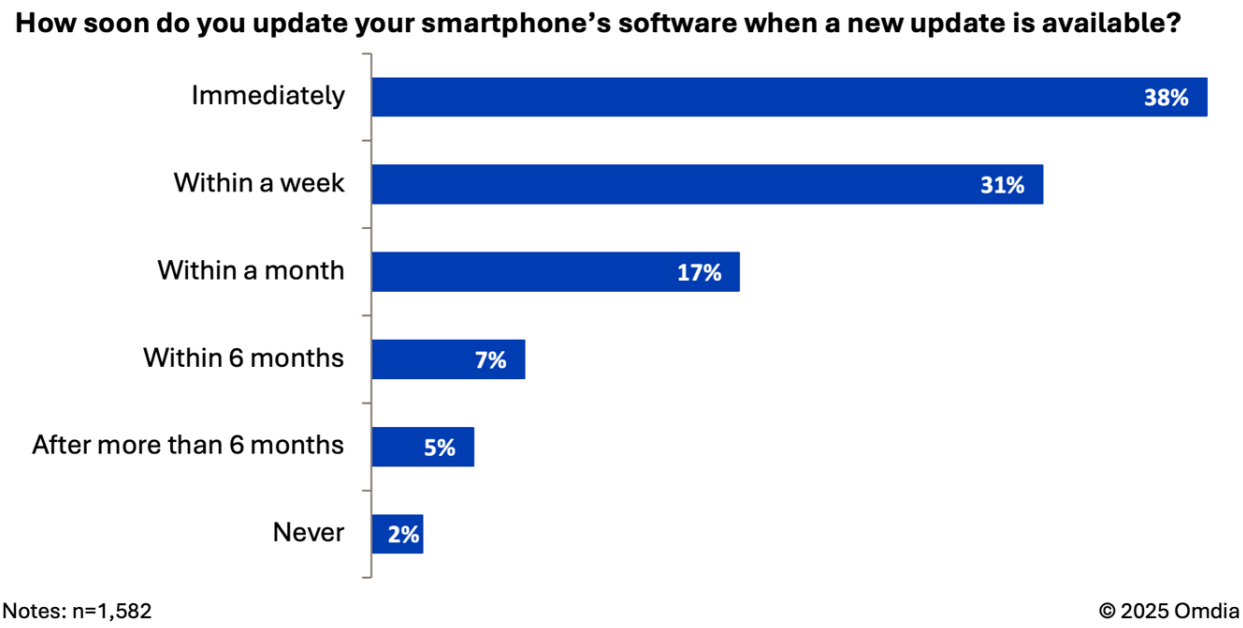
© 2025 Omdia

Source: Omdia Mobile Device Security Consumer Survey 2025

We also asked consumers how soon they update their smartphone software when a new update is available (see **Figure 5**). Prompt updating is key for smartphone security to keep up to date with the latest threats; 38% responded that they update immediately, 31% said that they update within a week (9% less than last year), meaning fewer are updating promptly; 14% take longer than one month to update; 6% update after six months; and 2% never update their devices. Device makers put in place ways of automatically updating devices or scheduling when an update takes place, although users may be intentionally avoiding updates to avoid the perceived risk of performance decline following an update. This could also be because "ease of use" ranked higher than robust security features in the ranking of purchasing drivers we asked consumers (see **Figure 3**), meaning that some may prioritize a seamless user experience and avoiding initial bugs over updating as soon as possible and staying secure.

© 2026 Omdia. All rights reserved. Unauthorized reproduction prohibited.

Figure 5: Consumer smartphone software updates behavior



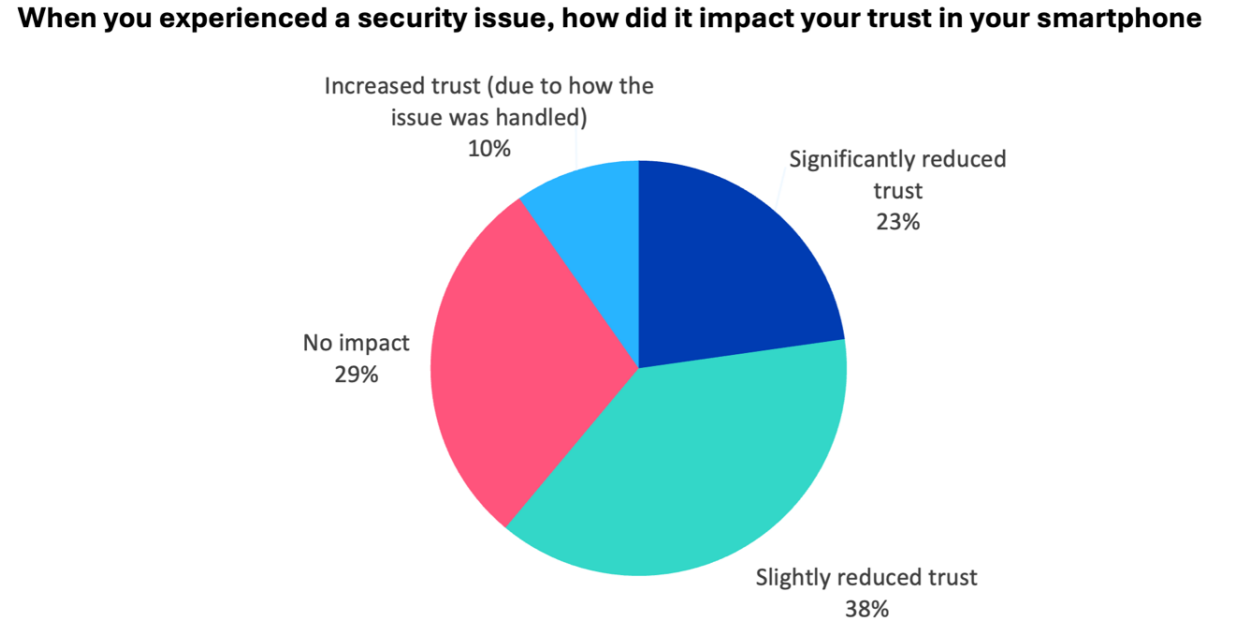
Source: Omdia Mobile Device Security Consumer Survey 2025

https://omdia.tech.informa.com/-/media/tech/omdia/assetfamily/2024/12/05/mobile-device-security-scorecard-2024/assetfamily004.pngConsumer security perceptions

Following a security issue, most consumers reported reduced trust in their smartphone brand or mobile operating system, with a total of 61% saying it either significantly or slightly reduced trust (see **Figure 6**). Just 10% reported an increase in their trust due to how well the issue was handled. This is an improvement on the previous year, when 73% reported that an issue had reduced trust and 8% reported an increase.

© 2026 Omdia. All rights reserved. Unauthorized reproduction prohibited.

Figure 6: Consumer trust following a security issue



Notes: n=1,582

© 2025 Omdia

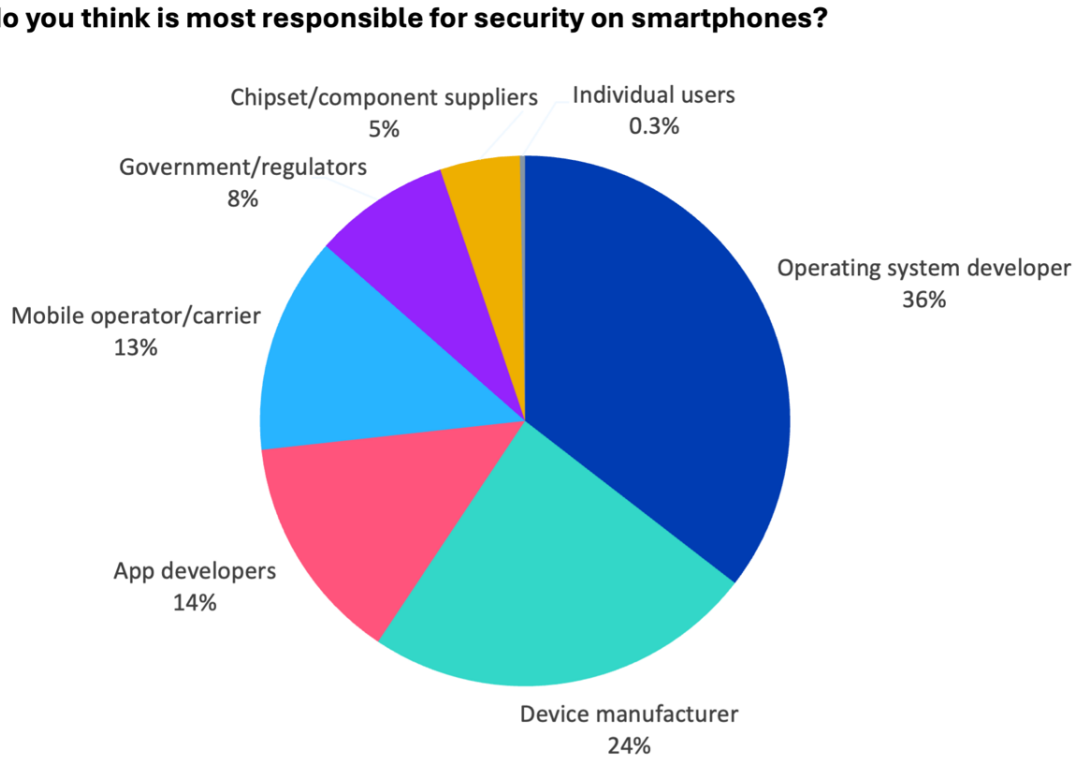
Source: Omdia Mobile Device Security Consumer Survey 2025

Security features are primarily dependent on the device maker and operating system developer (if they are different), as well as chipset/component suppliers, when negotiating support update periods. When consumers are asked who is most responsible, their attitude roughly mirrors this, with 36% thinking the OS developer is most responsible (see **Figure 7**). This is a dramatic decline from the 48% who responded this way the previous year. The second most popular answer also remains the same, with 24% saying device manufacturers have the most responsibility, falling from 27% last year.

For the first time, we also asked if the government or regulators should be most responsible, with 8% answering this way. Just five, or 0.3%, of respondents in our survey answered with "Other," specifying that they believed individual users were most responsible for the security on their smartphones.

© 2026 Omdia. All rights reserved. Unauthorized reproduction prohibited.

Figure 7: Consumer attitude to responsibility for smartphone security



Notes: n=1,582

© 2025 Omdia

Source: Omdia Mobile Device Security Consumer Survey 2025

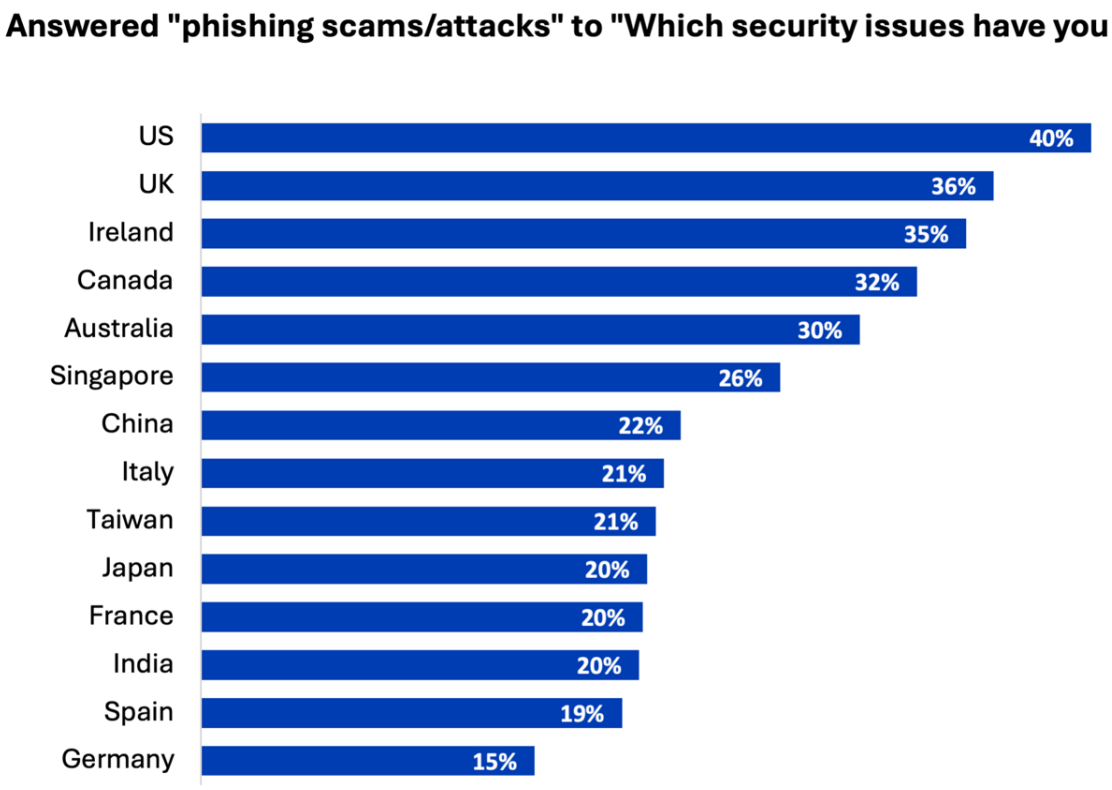
Differences by geography

Countries and territories with English as their first language have a higher reported rate of phishing scams and attacks than other countries and territories. The US had the highest reported rate of phishing attacks with 40%, followed by the UK with 36%, Ireland with 35%, Canada with 32%, and Australia with 30% (see **Figure 8**). Singapore, which has four official languages, including English, also had a high phishing attack rate of 26%.

It could be that phishing scams are designed in English, as it is the most widely spoken language in the world, therefore first targeting people with English as their native and first spoken language.

© 2026 Omdia. All rights reserved. Unauthorized reproduction prohibited.

Figure 8: Phishing scam/attack incidence rate differences by country/territory



Notes: n=1,582

© 2025 Omdia

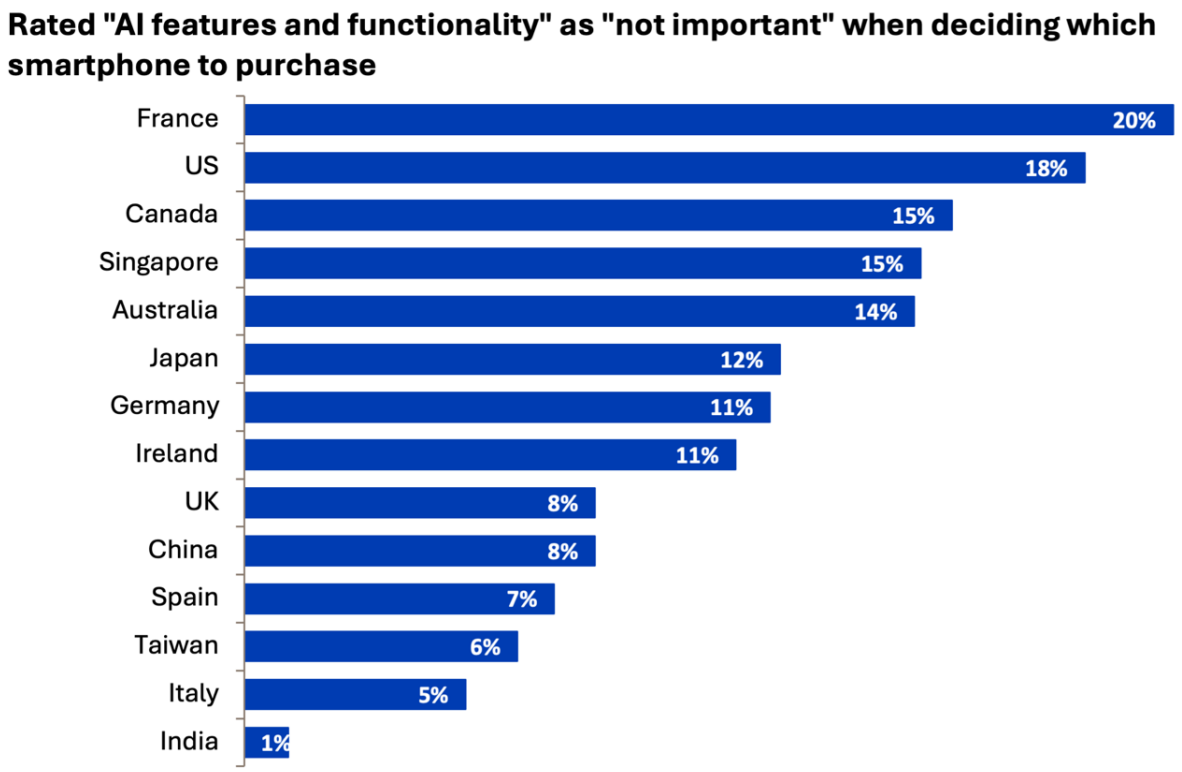
Source: Omdia Mobile Device Security Consumer Survey 2025

Attitudes toward AI features and functionality vary dramatically based on country or territory. The markets that rated AI as “not important” more than any other were France (20%) and the US (18%) (see **Figure 9**). It could be that consumers in these markets are more hesitant and skeptical of the value AI can offer them, especially compared to similar markets that rate it as more important, such as the UK (8% rated it as “not important”), Spain (7%), and Italy (5%).

To contrast this, just 1% of respondents in India rated AI features and functionality as “not important” when deciding which smartphone to purchase, with 25% actually rating AI as critical to their purchase (although this is still the lowest feature in the survey by how many rated it as critical).

© 2026 Omdia. All rights reserved. Unauthorized reproduction prohibited.

Figure 9: Consumer attitude to AI differing by geography



Notes: n=1,582

© 2025 Omdia

Source: Omdia Mobile Device Security Consumer Survey 2025

Appendix

Methodology

The Mobile Device Security Scorecard is a combination of hands-on testing by Pen Test Partners and consumer importance weightings based on an October 2025 survey of 1,582 consumers across 14 major countries or territories in North America (Canada and the US), Asia & Oceania (Australia, China, India, Japan, Singapore, and Taiwan) and Europe (France, Germany, Ireland, Italy, Spain, and the UK), who were asked to rate each security feature category we tested on how important it was to them.

Table 3: The following devices were tested:

© 2026 Omdia. All rights reserved. Unauthorized reproduction prohibited.

Figure	Model	Operating System	Firmware Version	Chipset
Google	Pixel 10 Pro	Android 16	BD1A.250702.001	Google Tensor G5
iPhone	17 Pro Max	iOS 26	N/A	Apple A19 Pro
Motorola	Moto Edge 60 Pro	Android 15	V2VV35.58-37-1	MediaTek Dimensity 8350 Extreme
Xiaomi	15	Android 15	2.0.7.0.VOCEUMXM	Qualcomm SM8750-AB Snapdragon 8 Elite
OnePlus	13	Android 15	CPH2653_15.0.0.703(EX01)	Qualcomm SM8750-AB Snapdragon 8 Elite
Samsung	Galaxy S25	Android 15	AP3A.240905.015.A2.S931BXXU3AYE7	Qualcomm SM8750-AC Snapdragon 8 Elite

Source: Omdia

Author

Aaron West, Senior Analyst, Smartphone Technology

Hollie Hennessy, OT/IoT Cybersecurity Lead

askananalyst@omdia.com

© 2026 Omdia. All rights reserved. Unauthorized reproduction prohibited.

Citation policy

Request external citation and usage of Omdia research and data via citations@omdia.com.

Omdia consulting

We hope that this analysis will help you make informed and imaginative business decisions. If you have further requirements, Omdia's consulting team may be able to help you. For more information about Omdia's consulting capabilities, please contact us directly at consulting@omdia.com.

Copyright notice and disclaimer

The Omdia research, data and information referenced herein (the "Omdia Materials") are the copyrighted property of TechTarget, Inc. and its subsidiaries or affiliates (together "Informa TechTarget") or its third party data providers and represent data, research, opinions, or viewpoints published by Informa TechTarget, and are not representations of fact.

The Omdia Materials reflect information and opinions from the original publication date and not from the date of this document. The information and opinions expressed in the Omdia Materials are subject to change without notice and Informa TechTarget does not have any duty or responsibility to update the Omdia Materials or this publication as a result.

Omdia Materials are delivered on an "as-is" and "as-available" basis. No representation or warranty, express or implied, is made as to the fairness, accuracy, completeness, or correctness of the information, opinions, and conclusions contained in Omdia Materials.

To the maximum extent permitted by law, Informa TechTarget and its affiliates, officers, directors, employees, agents, and third party data providers disclaim any liability (including, without limitation, any liability arising from fault or negligence) as to the accuracy or completeness or use of the Omdia Materials. Informa TechTarget will not, under any circumstance whatsoever, be liable for any trading, investment, commercial, or other decisions based on or made in reliance of the Omdia Materials.

CONTACT US

omdia.com

askananalyst@omdia.com

© 2026 Omdia. All rights reserved. Unauthorized reproduction prohibited.