Publication date:
06 Dec 2024
Author(s):
Hollie Hennessy, Principal Analyst
Aaron West, Senior Analyst, Consumer Electronics and Display Applications

Mobile Device Security Scorecard 2024

OMDIA

Table of Contents :

Table of Figures :

Summary

Google leads the smartphone industry in security feature testing for a fourth year

In the fourth annual Omdia Mobile Device Security Scorecard, leading global flagship devices from six of the largest smartphone manufacturers were compared on key security features, including anti-malware protection, network security, and secure backups. Google's Pixel 9 Pro and Samsung's Galaxy S24 both scored highly, ahead of Apple's iPhone 16 Pro and other leading Android-based devices, including the OnePlus 12, Xiaomi 14, and Honor Magic 6 Pro (see **Table 1**). The Google Pixel 9 Pro performed best in all categories except anti-phishing protection, where the Samsung Galaxy S24 performed best.

The ratings for each feature category are based on hands-on testing by Pen Test Partners and are combined with consumer importance weightings to produce a total score out of 100%. The consumer importance weighting is based on an October 2024 survey of 1,572 consumers across 13 major countries in the Americas, Asia & Oceania, and Europe. Respondents were asked to rate each category on how important it was to them.

Table 1: Smartphones rated for their security features

Security feature	Consumer importance weighting	Google Pixel 9 Pro	Samsung Galaxy S24	iPhone 16 Pro	Honor Magic 6 Pro	Xiaomi 14	OnePlus 12
Anti-phishing protection	100	50%	75%	25%	50%	25%	25%
Anti-malware protection	100	100%	75%	100%	75%	75%	75%
Files and photos protection	100	100%	100%	75%	100%	100%	100%
Identity protection	75	100%	75%	75%	50%	50%	50%
Hardware security	75	100%	100%	75%	75%	75%	75%
Lost-device protection	75	100%	75%	75%	50%	75%	50%
Network security	50	100%	75%	75%	75%	75%	75%
Security updates	50	100%	100%	75%	75%	50%	75%
Secure backups	50	100%	75%	75%	50%	50%	50%
Physical access control	25	100%	100%	100%	100%	75%	75%
Security awareness and remediation	25	100%	100%	50%	100%	100%	100%
Parental control	25	100%	100%	100%	100%	100%	100%
Total		**93%**	**85%**	**73%**	**71%**	**68%**	**67%**

Note: Consumer importance weighting is based on a survey of 1,572 consumers in October 2024. Scores

Security feature	Consumer importance weighting	Google Pixel 9 Pro	Samsung Galaxy S24	iPhone 16 Pro	Honor Magic 6 Pro	Xiaomi 14	OnePlus 12
in each category are out of 100% with the total being out of 100% based on the weight of each category.							

Source: Omdia

Key findings

The Google Pixel 9 Pro did well in all security features tested, only losing marks for anti-phishing protection. It could not detect the phishing emails used for testing—a category in which only Samsung's Galaxy S24 did better. In anti-malware protection testing, Google Pixel users could easily download sideloaded unauthorized applications, but malware was detected and blocked. In a new test this year of spyware and zero-click exploits, the Google Pixel 9 Pro was the only phone to block the application, because it did not adhere to Google Play Store's latest protections. Offering seven years of security update support, Google also leads the industry alongside Samsung for the length of commitment to security updates. A new snatch/theft protection test was also added this year, which involved simulating the phone being snatched from the user's hand and stolen. The Pixel's Google Snatch feature, Theft Detection Lock, added in a Google Play Services update serving Android 10+ phones, successfully locked the phone and set up protections after two attempts. All the other phones took longer to activate, and the Xiaomi device failed the test.

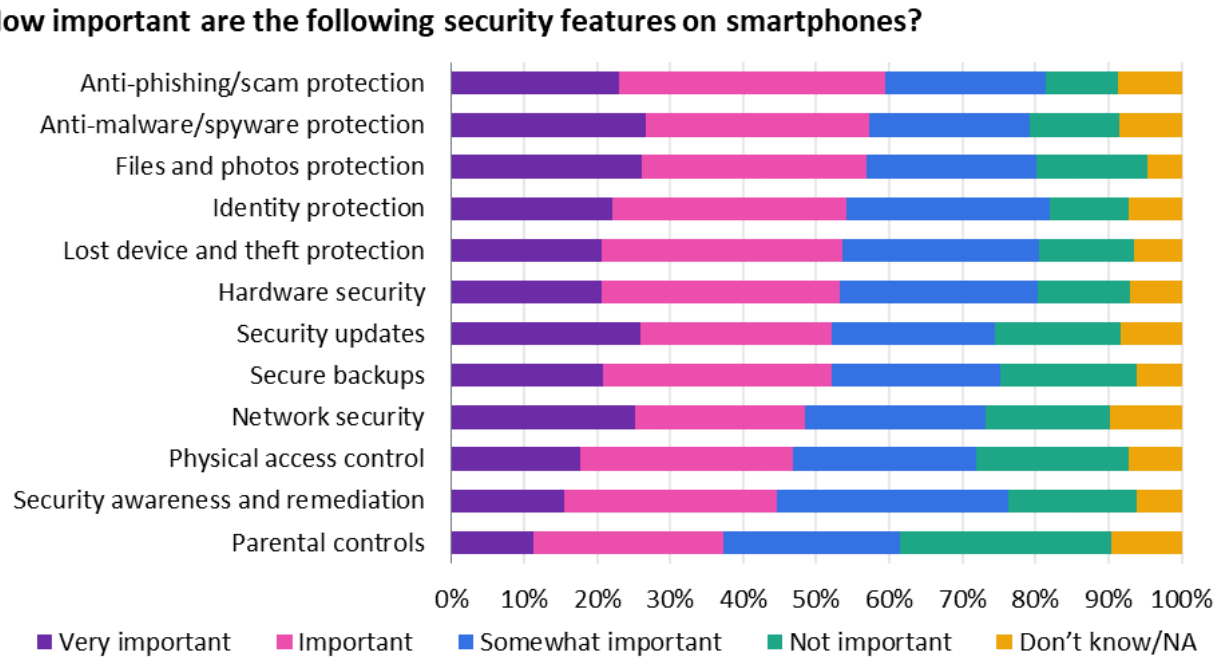
Samsung's Galaxy S24 also scored highly across all testing with the second-highest total rating. It received full marks in a number of security features, including hardware security and physical access control, and higher than 75% in all test areas. Notably, the Samsung was the only phone able to protect against the phishing emails used during testing. That said, it was held back by tests including the spyware test, where despite Samsung Knox's additional protections, it was unable to identify and block the installed spyware. Only being able to turn off 2G by selecting a 3G-only option in settings is also another area for improvement. Samsung's own password manager also does not proactively check saved passwords for compromise, which both the Google Pixel and iPhone do.

Apple's iPhone performs differently from all the other phones tested because it is not based on Android and has its own App Store. Most notably, it uses the Apple App Store rather than Google Play Store and does not allow native sideloading of apps (outside the EU), thus protecting users from untested application and potential malware or spyware to some extent. Overall, the iPhone 16 Pro did well in security feature testing and most areas. It lost marks for not detecting phishing emails, texts, or calls; not offering a clear audit trail of account activity; not having a centralized security center in settings, instead scattering security options through many different settings areas; and for not offering a way to set up file or app protections on device.

Many Android features and capabilities are repeated across the Xiaomi 14, OnePlus 12, and Honor Magic 6 Pro. Key differences in testing of these arose when the brand's proprietary security features were default instead of Google's. In many cases, these did not have the same level of protection or range of features. For example, the Oppo and Honor lost-device support did not allow tracking of offline devices, and none of the three had dedicated password managers or passkey support.

When surveying 1,572 consumers in October 2024, we asked how important were the security features we tested. The most important security features include anti-phishing protection, anti-malware/spyware protection, and file and photo protection (see **Figure 1**, based on the percentage of responses that responded "very important" or "important"). These findings are consistent with those of previous years: anti-phishing has been rising in importance over many years.

Figure 1: Most important security features



Notes: N=1,572 © 2024 Omdia

Source: Omdia Mobile Device Security Consumer Survey 2024

This largely correlates with consumers' belief in the effectiveness of their smartphones. Fifty-eight percent of consumers believe their smartphone is effective or very effective at anti-malware protection. Anti-phishing was one security feature consumers felt the least confident in: just 47% rated their phone as "effective" or "very effective" at this. This lack of confidence could be what has caused consumers to rate anti-phishing protections as more important in recent years.

We also asked consumers which security issues they have experienced with their smartphone. The most common responses were phishing scams/attacks (24%), malware/viruses (20%), and physical theft (16%). Though files and photos protection was rated among the most important features, it was the least common security issue, reported by 10% of respondents.

Following any security issue, consumers reported that their trust in their smartphone brand or mobile operating system was reduced, 32% reporting significantly reduced trust and 41% slightly reduced trust. Only 8% responded that their trust increased (thanks to the way the issue was handled).

Table 2: Security features covered in Omdia's consumer survey

Feature	Description
Anti-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.
Files and photos 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 to help you generate and store passwords in a secure fashion for all of your apps and websites. Also, the ability to notify you proactively if any of your previously used passwords have been leaked or stolen so that you can immediately change them. In addition, 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. Additionally, the ability to detect and protect against physical snatching attempts.
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 will not 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 is being transmitted from your device to a cloud service. 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 trying to repeatedly 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.

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.

Source: Omdia

Test results

Anti-phishing protection

The Google Pixel 9 Pro and Xiaomi 14 come with Gmail, Google Messages, Google Phone, and Chrome all preinstalled and set as default. The Samsung Galaxy S24 includes the Google apps but also comes with Samsung's own proprietary apps preinstalled and set as the default. It additionally has Microsoft Outlook preinstalled. Honor and OnePlus each use their own proprietary Android-based email applications, and Apple's iPhone uses the default iOS Mail, Messages, and Phone apps, Safari being the default browser.

For phishing emails, no device identified the two test case emails that were sent to users across all applications assessed when campaigns were launched from Gmail. However, emails were eventually blocked by Google's Mail Delivery subsystem and identified as spam when Google's SMTP was used to launch campaigns.

For phishing texts and calls, attempts sent from an unknown number and sender ID, using short links, were not identified as malicious. The Android devices from Google, Xiaomi, OnePlus, Honor, and Samsung all had voice call protection, flagging suspected spam calls. The Apple iPhone 16 Pro did not have as many features in these areas. When texts are received from an unknown contact on WhatsApp, links are automatically made unclickable until the message is replied to or the contact added. This is a WhatsApp feature and is consistent across all devices and operating systems.

Though phishing texts and emails were not flagged in message and email apps, once malicious links were opened, the devices that used Google Safe Browsing protection successfully blocked the link. A warning screen was raised, forcing the user to bypass another protection if they wanted to proceed. Once again, the native solutions on the devices were not as successful in this area. The Samsung Internet browser blocked most malicious links except the more sophisticated custom URLs. The Xiaomi Mii and OnePlus Internet browser did not warn the user when browsing to known malicious links.

For the first time, we also tested screen-sharing protections on devices. The Google Pixel 9 Pro, Honor Magic 6 Pro, and Samsung Galaxy S24 all had the ability to prevent one-time passwords (OTPs) from being recorded. The Pixel 9 Pro also offers "Partial Sharing" with Android 15, which allows the device to only share specific apps and not the whole screen. Android 15 introduced features that prevent OTPs being read by malicious applications.

Anti-malware protection

Each device's documentation and settings were reviewed to understand whether sideloading of applications was possible and, if so, what protections exist to reduce malware and spyware risks. An attempt was made to install a test malicious app on the devices. This year, for the first time, an attempt was made to install malware exhibiting spyware behavior, and an assessment was made of malicious USB "juice jacking" protections.

Because iOS does not allow any sideloading of applications, although this is allowed in the EU, the iPhone was found to not allow easy introduction of any malware, so it passed the test.

Because it is easier to sideload applications on Android devices, they all had protections against malware, although at varying levels. The Google Pixel 9 Pro and OnePlus 12 relied on Google Play Protect only. The Samsung device introduced several layers of protection, implementing both Google Play Protect and Device Care. The Xiaomi device also used Google Play Protect and the Xiaomi Security app, while the Honor device used its System Manager app for similar functionality.

If an attempt is made to install a known malicious application, Google Play Protect will detect this and warn the user. However, the user can proceed with installation by clicking “more information” and selecting “install anyway,” allowing the app to be installed despite the warning. This was considered enough warning and protection for it to pass the test. Google Play Protect blocks or warns users depending on the malware type and severity.

In the spyware test, the Google Pixel 9 Pro blocked the application because the application did not include the latest privacy protections. All other Android devices allowed the spyware application to be run. The Samsung Galaxy S24, Xiaomi 14, and OnePlus 12 all gave warnings about the excessive permissions the app required, and the Honor Magic 6 Pro gave no warnings. However, Samsung’s Device Care antivirus scan did not identify the spyware.

The iPhone has “Lockdown Mode,” which provides an extra layer of anti-spyware protection onto top of what Android devices provide, although this is a niche use-case scenario.

In the juice-jacking test, it was found that the iPhone was best: Apple’s USB Restricted Mode provided robust protection against malicious USBs. The Google Pixel 9 Pro and Samsung Galaxy S24 both required the user to explicitly allow any data transfer. The Pixel also has the Titan M2 security chip for added protection during USB connections, and Samsung Knox provides some level of security monitoring to protect against unauthorized USB connections. Though they do not have a specific restricted mode like the iPhone’s, both were deemed to have strong protections in this test.

The Xiaomi, OnePlus, and Honor devices had moderate security protections against malicious USBs, each defaulting to charging-only mode unless data transfer was explicitly enabled.

Files and photos protection

All tested devices allow users to protect chosen images on the device, for example, by putting them in a hidden gallery that requires biometrics to access.

For files protections, all devices except the iPhone allow files to be protected within their built-in applications behind additional layers of security, such as Google’s Safe Folder. The iPhone does not allow files to be secured locally, instead allowing users to store sensitive files in an iCloud Drive and restrict access with the iCloud privacy settings. This was judged to be a partial pass of this test.

For the first time, we also assessed whether it was possible to password or pin protect specific applications. This was possible on all Android devices through Google’s app pinning and Private Space feature, Xiaomi’s App Lock, OnePlus’s App Locker, Honor’s Parallel Space, and Samsung’s Secure Folder.

With iOS 18, Apple introduced a feature that allows users to lock individual apps using Face ID or a passcode, by long-pressing the app icon and selecting “Require Face ID.”

Identity protection

This test covers the manufacturer-provided account management and password manager tools on the phone. We check whether this proactively checks if any of the user's previously used passwords have been leaked or stolen so that they immediately change them, whether they can access a variety of two-factor authentication options, and whether they can see a full audit trail of account activity. We also check for passkey support of both the primary account with the manufacturer and third-party accounts.

All Android devices have access to Google services, this being the default on the Pixel 9 Pro. This includes all tested security features, all of which are managed by the user's Google account.

The Xiaomi, OnePlus, Honor, and Samsung phones also have their own proprietary manufacturer account management apps. Some of these lack the same level of security features and capabilities, such as password managers. For example, the Xiaomi and OnePlus lacked security features in testing, Honor lacked both account check-up features and auditability, and Samsung did not check for compromised passwords via its password manager.

Users can opt to just use Google's offering, but this is not the default prompted service on these phones, so the Xiaomi, OnePlus, Honor, and Samsung phones have been marked down accordingly in the test scoring.

The iPhone 16 Pro is the only phone without access to Google services out of the box. Apple's own services lacked account check-up features and full auditability. However, there is a well-used and functional password manager within iCloud Keychain, only lacking third-party account passkeys.

Hardware security

It is challenging to compare security implementations across manufacturers, especially when they use the same hardware, such as Qualcomm's Secure Processing Unit (SPU) in the Samsung, Xiaomi, and OnePlus. The interfacing software and security frameworks vary greatly, and this influences the range of security features supported.

Samsung's Knox Security is a comprehensive security system that provides protection for the device and the data stored on it. It combines both hardware- and software-based security features to create several layers of protection. Samsung's Knox Security integrates with Qualcomm's Secure Boot to detect rooting attempts and disables critical services if any tampering is detected, utilizing features such as Knox Vault and RPK. Xiaomi has added MIUI, which has its own layers of protection to prevent the system from being compromised. OnePlus allows rooting but at the cost of voiding warranties and disabling services such as Google Pay.

The Google Pixel 9 Pro, Apple iPhone 16 Pro, and Honor Magic 6 Pro differ from these with their own unique hardware. Google's Tensor Security Core and Titan M2 chip provide additional layers of protection beyond Qualcomm-based devices: the Titan M2 is separated from the main system-on-chip (SoC), offering enhanced cryptographic functions and boot-loader protection. Similarly, Apple's Secure Enclave operates independently within the SoC, managing sensitive operations such as biometric data with a dedicated security infrastructure. Honor uses the Discrete Security Chip S1, which manages security operations, also introducing proprietary layers to prevent unauthorized modifications, further differentiating it from the others.

All tested phones have a strong baseline of hardware security, although the additional dedicated layers of separate security on the Google Pixel 9 Pro and Samsung Galaxy S24 mean these two phones have received the maximum score in this test area.

Lost-device protection

The devices were evaluated based on their ability to locate, lock, and wipe in case of loss or theft, with an emphasis on the functionality of web-based and mobile app tools. Additionally, their capacity to alert users about unwanted tracking devices in their vicinity was assessed. For the first time, devices' snatch/theft protection features were tested through a simulated phone-snatching incident.

The Google Pixel 9 Pro utilized Google's Find My Device with a full suite of tracking, locking, wiping, and offline locating features. Theft protection was also added, supported back to Android 10, which locked the phone after two simulated phone thefts. Additionally, the phone can scan for nearby Bluetooth tracking devices. Other theft protection features include remote locking via a verified phone number and offline device locking.

The iPhone 16 Pro comes with the Apple Find My iPhone service, which supports location tracking, locking, wiping, and emergency privacy features such as "Safety Check." The device also enabled biometric authentication, IP address privacy, and offers Lockdown Mode for heightened security during targeted attacks.

Unlike the others, the iPhone has no dedicated snatch protection, but it does have Stolen Device Protection. This allows for a number of additional requirements to be added before an individual can make critical changes to an obtained device. Security Delay is also implemented when an attempt is made to access Apple Account security actions. Therefore, the iPhone was not marked down in this test but received the full score.

The other Android devices have access to Google's Find My Device service, although they often default to their own proprietary service. Therefore, they have been tested on these.

The Xiaomi 14 uses Xiaomi's MI Cloud, offering advanced theft protection, offline tracking via SMS commands, and device locking if it is stolen. However it was not possible to activate the protection during simulated theft.

The Samsung Galaxy S24 offers robust security through Samsung's Find My Mobile, featuring Samsung Knox for additional protection. It supports offline tracking and allows users to remotely lock the device if theft is suspected by using its phone number. Google Snatch Protection was tested but only worked successfully after several attempts.

Honor provides the Google Find My Device feature, integrated into Honor's MagicOS. No alternative finding service has been provided by Honor. This gave the same protection as the Google Pixel 9 Pro, except for the lack of offline location tracking and unwanted tracker alerts. In testing, several snatch attempts were conducted on the device before the screen successfully locked.

Similarly, the Oppo OnePlus 12 relies solely on Google's Find My Device but lacks offline tracking and unwanted tracker alerts. Snatch protection took several attempts to activate.

Network security

Manual checks were performed to understand what traffic or content could be observed in transit. For each phone, other settings were verified manually, including the ability to disable 2G, support of eSIMs, and the ability to add additional network protection in the form of a virtual private network (VPN). In addition, signals for unencrypted connections were also checked via app settings, the browser, and individual app settings.

All the devices had the ability to set systemwide proxies that allowed the interception of network traffic. For Android devices, this requires a user root certificate to be added to the device. This requires the Android device to be in a rooted state.

All the devices had the ability to use internal eSIMs and connect to a VPN and had additional warnings against using unencrypted connections. Pixel devices come with a free built-in VPN.

The Xiaomi 14, Oppo OnePlus 12, and Honor Magic 6 Pro could not disable access to 2G on mobile networks. The Samsung Galaxy S24 can disable 2G but only by the selection of a "3G only" option in settings. The iPhone is similar with Lockdown mode. Because this is not a dedicated solution and is therefore unlikely to be used by consumers, Apple and Samsung have been marked down accordingly in this test. The Google device allows users to specifically disable 2G in the settings.

Security updates

This test area is intended to assess how well the OEMs deliver regular security updates to their devices, for how long they commit to do so, and how well documented and transparent this is for consumers to see. The device is also hands-on tested to discover what happens when an update is pushed out and what the prompts and options for installing are.

Each manufacturer has distinct commitments about the length of software updates. Google leads, promising seven years of security updates and major OS upgrades for the Pixel 9 Pro and adhering closely to Google's monthly security patch cycle. Samsung recently matched this commitment, supporting the S24 series of devices for seven years with security updates. These updates come monthly, in line with the Android monthly security patches, and there are Samsung-specific additions. They include both Android OS upgrades and security patches. Google and Samsung received full marks in this test.

Xiaomi does not clearly define the update lifecycles. In official online documentation it states that updates are provided for a minimum of two years, without guaranteed monthly releases, and it does not state which devices will get support for longer than two years. To find out how long the Xiaomi 14 will be supported, consumers must search for a press release that was issued on its release. Because of this lack of clear documentation, Xiaomi has been marked down in this test.

Honor offers five years of security updates with bimonthly patches. OnePlus states a commitment to five years of support for flagship models, which will include the OnePlus 12, even though this is not confirmed for all consumer devices.

In previous years Apple has not clearly stated the update lifecycle of its devices. This year that changed with the introduction of new transparency legislation. For the iPhone 16 Pro, Apple has committed to five years of support from the day of its release in addition to regular updates. Apple also employs rapid security responses for critical vulnerabilities, enhancing device security.

Despite clear documentation and regular update frequencies, Apple, OnePlus and Honor have been marked down slightly in this test because they only offer five years of support rather than Google and Samsung's seven years.

All devices prompted users clearly to update their device when an upgrade is available, allowing them to install and reboot overnight or by selecting a specific time.

Secure backups

In this test, each manufacturer's documentation was investigated to determine the level of encryption offered for device backups and whether the hosting provider has access to backed-up phone data.

The Google Pixel 9 Pro offers default end-to-end encryption for backups, ensuring that Google cannot access backed-up data, which is encrypted using the device passcode. However, there is no detailed breakdown of which data types are specifically encrypted.

The Apple iPhone 16 Pro allows for encrypted local backups and iCloud backups, where data is encrypted in transit and at rest. With Advanced Data Protection enabled, iCloud backups receive end-to-end encryption, preventing even Apple from accessing the data. Unless this feature is specifically enabled—it is off by default—Apple holds the encryption keys for most iCloud backup data. Fifteen categories of data are end-to-end encrypted by default, including health and passwords in iCloud keychain, but many are not, including iCloud backup, photos, notes, and more. With Advanced Data Protection enabled, 25 categories of data are end-to-end encrypted. Similarly, the Samsung Galaxy S24, benefits from an optional Advanced Data Protection option. Because this is off by default on each device, Apple and Samsung have been marked down slightly in this test.

The Xiaomi 14, OnePlus 12, and Honor Magic 6 Pro each encrypt backups to their own services and Google Drive during transfer and storage, but neither backup service is end-to-end encrypted, meaning third parties or the OEMs could access the data. Therefore, they have been marked down in this test.

Physical access control

During setup and through the user settings of the device, the method of biometric control that a user could select was recorded. To test the effectiveness, access to each device with the incorrect biometrics was attempted and observed. The settings of each device were then looked at to determine whether biometrics could be temporarily disabled.

All the Android devices offer the same biometrics options; only the Samsung device differs slightly by offering an ultrasonic sensor over an optical sensor for fingerprint detection.

The iPhone 16 Pro has robust physical access controls, offering a number of features to protect the device. Face ID uses an array of infrared and depth sensors to accurately detect a real face. The device possesses a number of attention settings, making it less likely than the other devices to be unlocked. Similarly, the Honor device uses 3D depth-sensing capabilities that provide stronger resistance to spoofing attempts such as photos or masks.

It was also possible to unlock the iPhone phone using a voice command, using a combination of custom voice commands, accessibility settings, and Siri.

The only difference between device scores in this category arises because the Xiaomi 14 and OnePlus 12 do not have a lockdown mode that temporarily disables biometrics to secure the device.

Security awareness and remediation

We checked each device for a centralized security app or page within its settings. If this was found, the contents of the page were evaluated to determine how well users can remediate issues from this security center. Device documentation was also reviewed to understand whether permissions for unused apps were automatically revoked.

All Android devices have a centralized Security and Privacy center, which automatically revokes unused app permissions via Play Protect; therefore, all received full marks in this test.

The iPhone 16 Pro differs as the only iOS-based device by instead scattering security features and checks throughout its settings app. Though it was possible to access various built-in tools and online resources for security, including the automatic permission revocation feature in iOS 18, the iPhone 16 Pro has been marked down in this test because these tools are not in a centralized place, making it more difficult for the consumer to monitor and control them.

Parental control

Each device and its documentation were reviewed to understand the parental control features available. The devices were then enrolled to evaluate the controls that can be applied. We checked whether each allowed users to restrict certain apps, features, or services and whether specific lock screen security could be applied.

The Google Pixel 9 Pro and Xiaomi 14 both use Google Family Link for policy management, allowing parents to restrict apps and services. The Apple iPhone 16 Pro uses Family Sharing and Screen Time for content restrictions and detailed usage insights. The Oppo OnePlus 12 and Honor Magic Pro 6 support Family Link, and OnePlus also features Kids Mode. The Samsung Galaxy S24 supports Google Family Link and Samsung Family Group for managing child accounts. All have a full suite of settings and features in testing, so each device received the maximum score in this test.

Consumer perception survey

About the survey

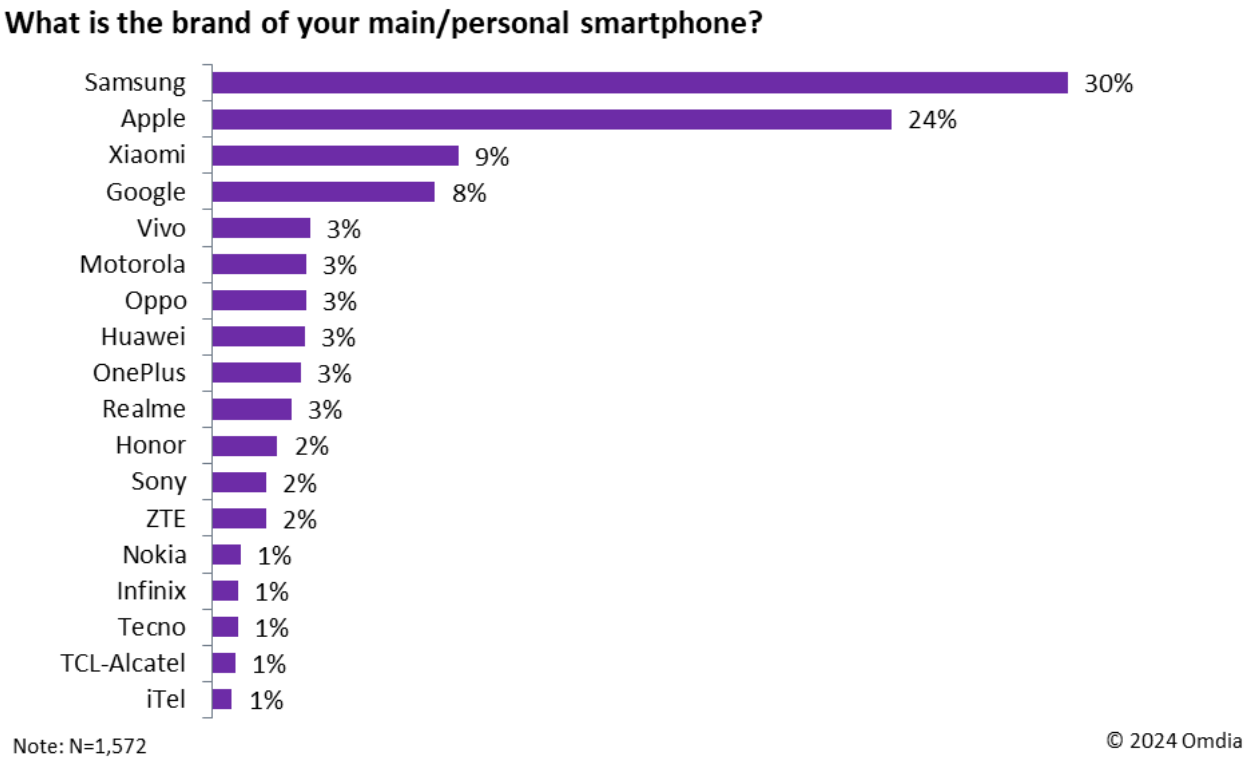
In October 2024, we surveyed 1,572 consumers who had bought a new smartphone in the past three years about their security concerns and perceptions in an online survey with computer-aided telephone interviews. Respondents participated from the following countries and territories: Australia, Canada, China, France, Germany, India, Ireland, Japan, Singapore, Spain, Taiwan, the UK, and the US.

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

Key consumer demographics

Users of 18 different smartphone brands were surveyed, most owning either a Samsung or Apple device (see **Figure 2**). Google and Xiaomi were the only other brands with ownership shares above 5%. Huawei, Motorola, and OnePlus ownership shares were down from last year.

Figure 2: Smartphone brands

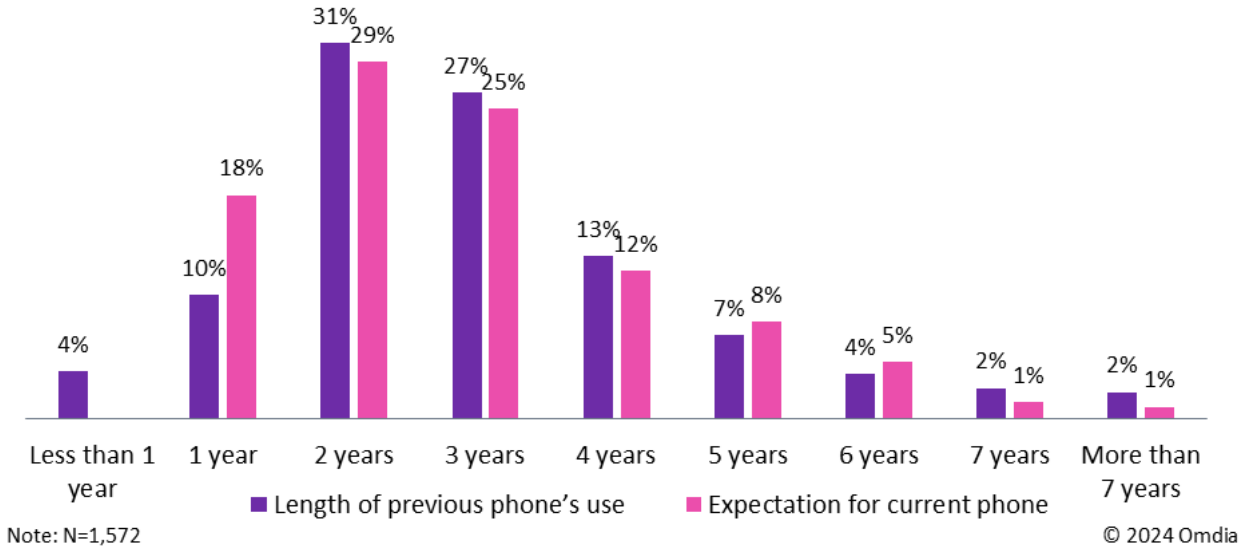


Source: Omdia Mobile Device Security Consumer Survey 2024

Security update periods continue to be a hot topic in cybersecurity, closely tied to replacement cycle rates, which continue to be a key sustainability topic. A staggering 55% of consumers reported keeping their previous phone for longer than two years, longer than security updates typically last for any given smartphone (see **Figure 3**). Further, another 8% of consumers reported keeping their previous phone longer than five years. This number is up from 5% in last year's study. Currently the only phones offering more than five years of security updates from launch are the Google Pixel 8 and 9 series; the Samsung S24 series, which offer seven years; and the Fairphone 5, which offers eight years.

Consumers tend to expect their current phone's lifespan will be longer than that of their previous phone. This suggests that the smartphone replacement rate will slow globally as consumers expect to keep their phones for longer.

Figure 3: Consumer smartphone replacement cycle



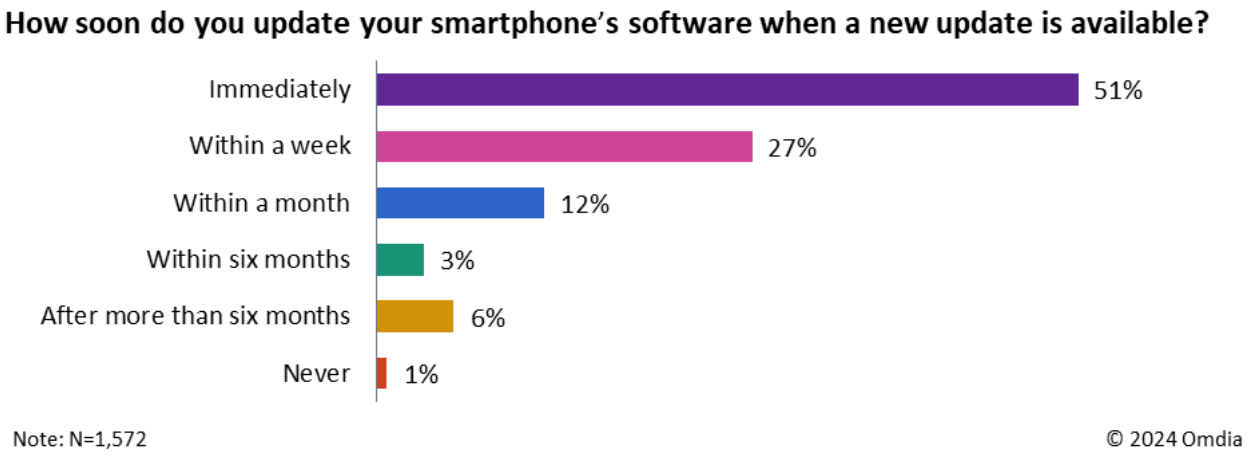
Source: Omdia Mobile Device Security Consumer Survey 2024

When we asked, "What did you do with your previous phone?" the most common responses (17% each) were that it had been kept or traded in for a discount on a new device. Sold it, recycled it, or put it in the bin each scored 14%. Waste electrical and electronic equipment (WEEE) is one of the fastest-growing waste streams globally, meaning governments, smartphone OEMs, and mobile carriers can all do more to incentivize consumers to recycle or refurbish their old device rather than put it into waste. The remaining responses were gave it to someone (13%) and donated it to charity (11%).

Consumer security behavior

We asked consumers how soon they update their smartphone software when a new update is available. Prompt updating is key for smartphone security to keep up to date with the latest threats. Fifty-one percent responded that they update immediately and 27% that they update within a week. Ten percent take longer than one month to update, 6% taking more than six months, putting themselves at greater risk. Device makers may want to put in place better incentives and systems to educate users on the risks of not updating software promptly.

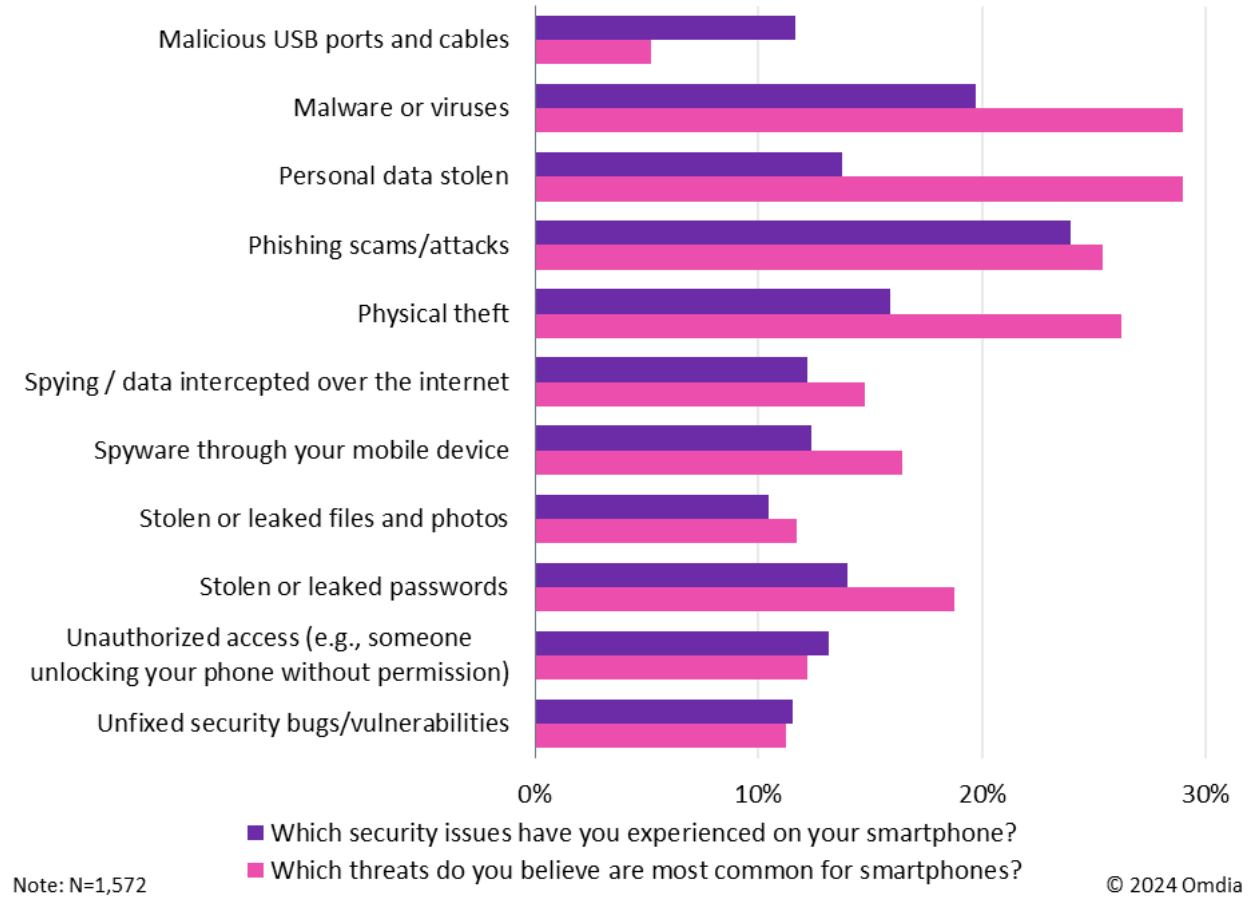
Figure 4: Consumer software update behavior



Source: Omdia Mobile Device Security Consumer Survey 2024

When consumers were asked which security risks they believe are most common, the top rated risks were malware, stolen personal data, physical theft, and phishing scams, as shown in **Figure 5**. This largely aligns with what consumers reported when they were asked which security issues they had experienced firsthand. The most common by some margin was phishing scams and attacks, reported by 24%, followed by malware, which was reported by 20%.

Figure 5: Consumer security concerns and reported incidence rate



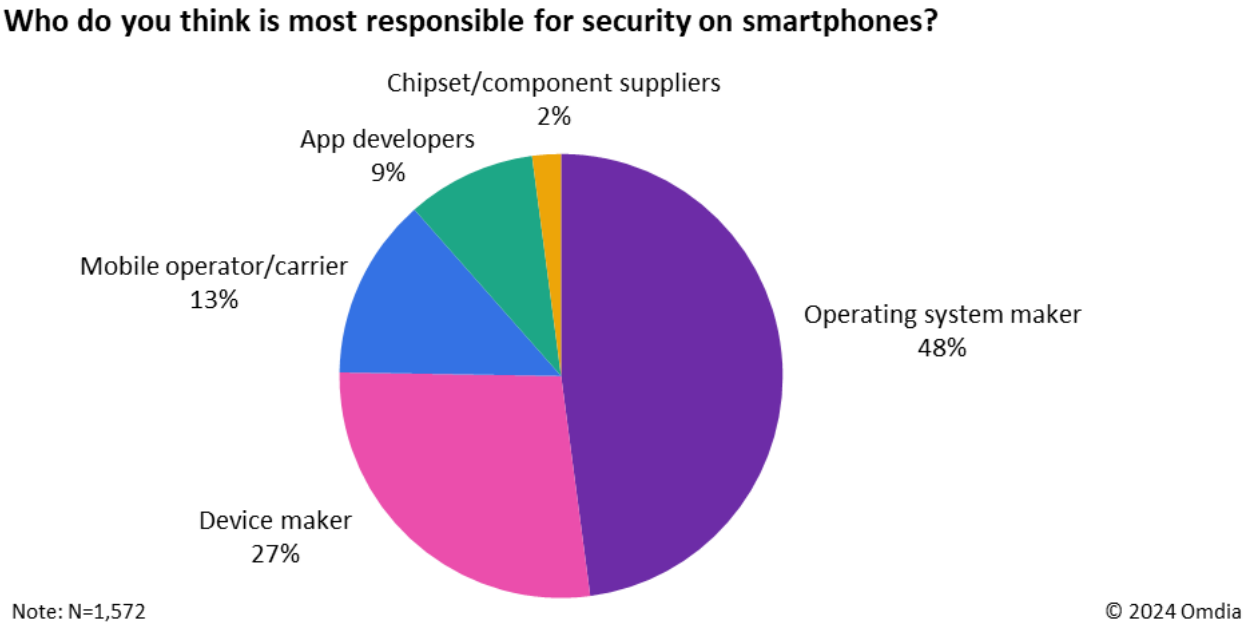
Source: Omdia Mobile Device Security Consumer Survey 2024

The biggest mismatches between what consumers believe the threats are and their actual incidence in our survey were in stolen personal data, physical theft, and malware and viruses, all of which happen less often than consumers believe, and malicious USB ports and cables, which happen more often than consumers believe.

Consumer security perceptions

Though security updates are primarily dependent on the device maker and chipset supplier, nearly half of consumers believe it should be the operating system developer (either Apple or Google) that is responsible for the security of their smartphone (see **Figure 6**), and 13% believe the mobile operator/carrier should be responsible. These results show there is an imbalance between how consumers view responsibility for security and where the key security decisions are actually made.

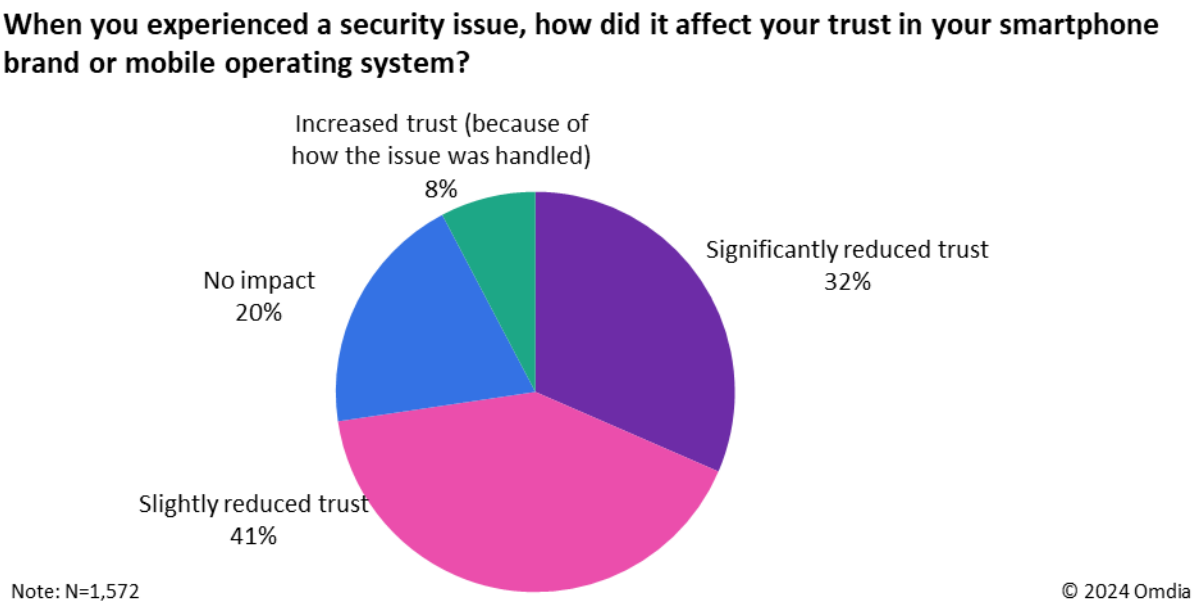
Figure 6: Consumer attitude to responsibility for smartphone security



Source: Omdia Mobile Device Security Consumer Survey 2024

Following a security issue, most consumers reported that it reduced their trust in their smartphone brand or mobile operating system. Overall, 73% had reduced trust versus just 8% who increased their trust because of how well the issue was handled.

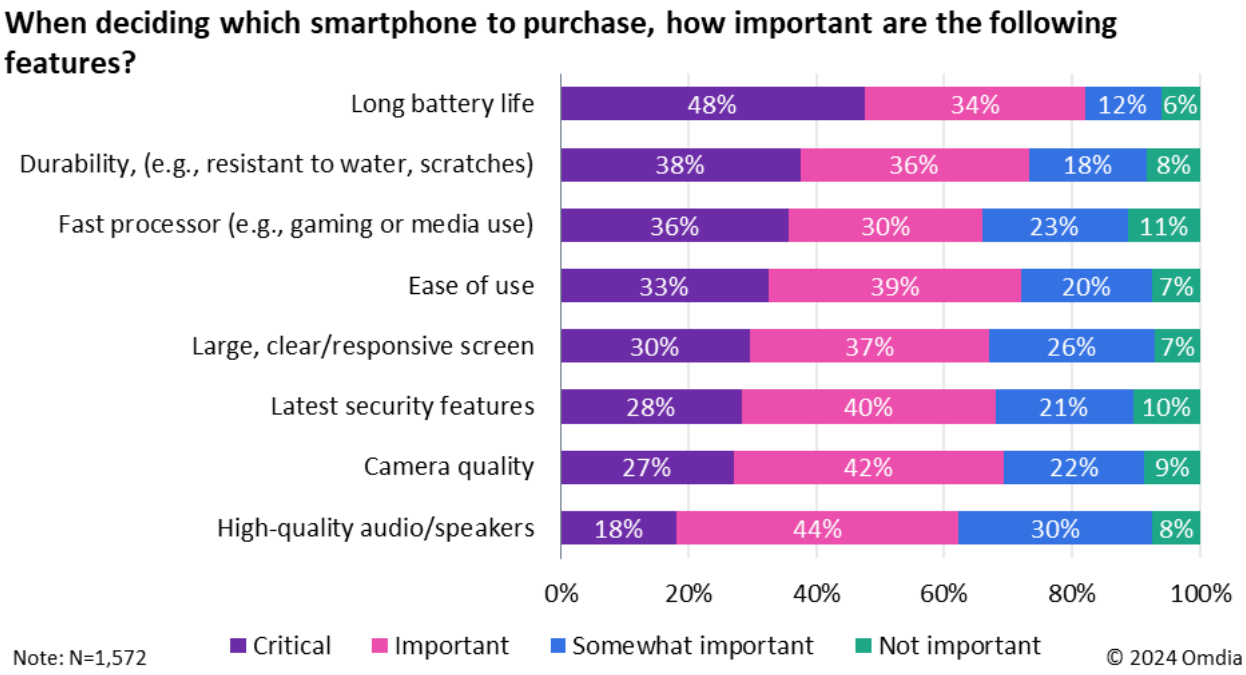
1. Figure 7: Consumer trust following a security issue



Source: Omdia Mobile Device Security Consumer Survey 2024

When they were asked whether they would be prepared to pay a premium for their next smartphone to be equipped with advanced built-in security features, 65% said they would. But if security features are compared with a variety of other key purchasing drivers, many others take precedence. Long battery life is the runaway winner: almost half said it was a critical feature. Just 28% of respondents said the latest security features were critical.

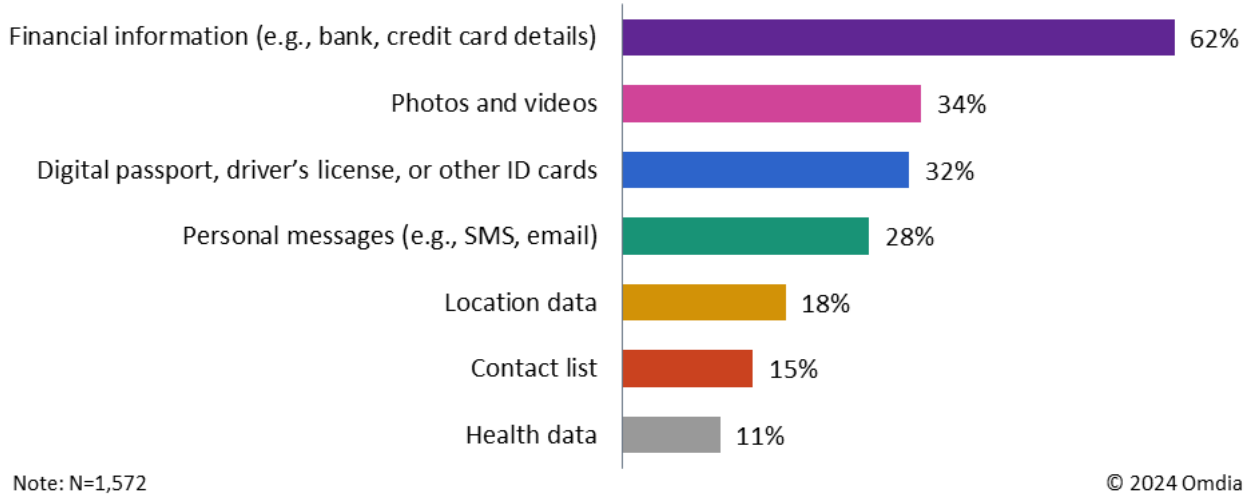
Figure 8: Key smartphone purchasing drivers ranked by importance to consumers



Source: Omdia Mobile Device Security Consumer Survey 2024

When consumers were asked to pick the top two types of data they were most concerned with protecting, financial information was ranked most important with 62% selecting it. The next data types did not even come close: photos and videos were at 34% and digital passport, driver's licenses or ID cards at 32%. Health data, despite being considered special category data within GDPR regulations and being incredibly sensitive information, is one type of data consumers are least concerned about.

Figure 9: Which types of data are consumers most concerned about protecting



Source: Omdia Mobile Device Security Consumer Survey 2024

Differences by geography

- How long did you use your previous phone before upgrading?
  - Consumers in Japan (72%), Australia (60%), and the US (58%) are most likely to use their phone for two or more years.
  - Those in France (20%), Japan (19%), and the US (18%) are most likely to use their phone for five or more years.
- What did you do with your previous phone (i.e., the handset you used before your current one)?
  - Singapore is the most sustainability-conscious: only 4% of consumers reported binning their old phone.
- Will better security features be a key purchase driver when you are buying your next phone?
  - Better security features are most often a key purchase driver for consumers in India (69% answered yes) and Japan (58%).
  - Security features are least often a key purchase driver in the UK (43% yes), Singapore (48%), and the US (49%).
- Which security issues have you experienced on your smartphone?
  - Security issues are most prevalent in India (71% experienced) and Australia (66%).
- Issues are least prevalent in the US (58% had not experienced an issue) followed by Germany, Japan, and the UK (all at 54%).
- Thinking about your next smartphone, how likely are you to pay a premium to have it equipped with advanced built-in security features (e.g., anti-malware, anti-phishing, network security, identity protection, etc.), regardless of other features and functionality?
  - Consumers in Spain and India are the most likely to pay a premium for advanced security features (80% and 79%, respectively).
  - Forty-five percent of Indian consumers are “very likely” to pay a premium, similar to last year’s findings and among the highest of any country we surveyed.

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 2024 survey of 1,572 consumers across 13 major countries in the Americas, Asia & Oceania, and Europe, who were asked to rate each security feature category we tested on how important it was to them.

Authors

Hollie Hennessy, Principal Analyst, Cybersecurity

Aaron West, Senior Analyst, Smartphones

askananalyst@omdia.com

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