
Together we can
vodafone
business

Introduction

In recent years, especially with hybrid work, almost everyone uses an iOS or Android device for work. In fact, a recent survey* found that 92% of remote workers use their personal laptops or smartphones for work tasks, with 46% of them having saved files onto their devices.

But more than just at work, applications, or “apps” are part of our daily lives. Whether it is staying connected with friends and family, participating in meetings whilst working from home, paying a bill, or tracking business site assets, there is an app for everything.

Have you stopped to think about what apps do, where apps come from, what makes a good app, what makes a bad app and whether an app is safe to install?

We need to pay attention to the apps we are using, whether on mobile devices, laptops, smart devices, or cars. Are you sure that app you have just installed is only controlling your new smart lightbulb or does it contain malware that is stealing your data in the background? Does it really need permission to access your location and contacts, and where is your data being sent to? It is important to understand your apps and have a secure approach to using them.

What is an app and how do they work?

An app is a software program designed to perform a function or set of functions on a mobile device or computer. Apps can be downloaded and installed on any modern smart device, and range from productivity apps like Microsoft Office to casual gaming apps like Candy Crush.

Apps are wide and varied but have many things in common: they use the device in your hand, the data on it, the data it records or senses (e.g. date, time, location, camera view) and the data you put into it. Fundamentally apps use data. That is not bad and is often useful (e.g., performance monitoring of a service, providing relevant targeted information). Apps can have access to a lot of data, yours, and your workplace’s.

We see two categories of apps:

1. **Paid**
   You pay a one-off or regular fee, part of which goes to the entity that provides the app to fund them and the app development

2. **Free**
   You make no payment to use the application.

Most free apps are funded by advertising, whereby third parties pay the developer to display their adverts in the hope that you will buy their goods or services. The developer may also generate revenue by selling data collected by the app to third parties, who can use that data to identify and then target customers to sell their products to. So, whilst the app does not cost you any money to use, it is not “free” as you typically agree to “sell” your data to the developer and their partners. You and your data are in effect the product. Your data is clearly valuable as mobile app advertising spending is projected to reach $399.6b in 2024[1] , this will be half of the overall digital advertising spend and over a third of all spending on all advertising globally[2]. For context, the amount spent on mobile app advertising in 2024 is approximately equal to the GDP (Gross Domestic Product.) of Norway[3].

Some free applications are provided by organisations as part of their Corporate and Social Responsibility goals, such as Vodafone Foundation[4]. These are funded to support specific needs or goals by these organisations. For example, Vodafone provides Zoteria[5] , which makes it easier for people to report LGBTQ+ hate crime and access support.

1 https://www.statista.com/statistics/303817/mobile-internet-advertising-revenue-worldwide/
2 https://ebiquity.com/news-insights/blog/digital-ad-spend-set-to-grow-by-a-third-by-2024/
3 https://www.worldometers.info/gdp/gdp-by-country/
4 https://www.vodafone.com/vodafone-foundation
5 https://www.vodafone.co.uk/newscentre/press-release/zoteria-app-tackle-lgbtq-hate-crime-following-rise-in-reported-incidents-uk/

The risks of blending personal and corporate data

There are risks beyond phishing attacks, malware, risky connections, or device compromise. As employees download unvetted applications for both personal and work use, they unintentionally expand your organisation's risk surface. This is mostly due to the risky permissions that many personal apps have. Permissions like access to the address book, local files, or location might seem innocuous on a personal level, but could put corporate data accessed from that device at risk.

It is important to understand who provides the app, what use it will make of your data and that you are comfortable with this. Whilst for some applications, it is clear who makes them and their purpose, for others its much less clear.

Apps should be clear about what data they collect and how it is used. It is important to take a moment to understand that and make sure you are comfortable before you install and use the app. The service terms should make this clear to you and the privacy implications should be detailed within the platform app store.

The quantity and type of data shared with and by apps varies significantly. An Android Clock app only collects a device ID by default, which is used for app analytics. Whereas the Android version of a popular social media app will collect personal data, like your name, user IDs, email, address, phone number, and can have access to location data, contacts, messaging, audio and video including the camera) as well as your financial information. All of this is allowed if the terms and conditions of the app state that you give the app provider permission to share your data.

The more data shared, the greater the potential for that data to be used by the app provider for their business purposes and the greater the potential impact on you if it is lost by them or used and abused by others.

App providers must comply with the legal requirements of the laws governing where they are based. The laws in some countries have led to privacy and security fears about state access and misuse of user data. These fears have led to some organisations banning the use of various apps.

Mobile phishing at all time high

Users, endpoints and applications are now so closely connected that threat actors can initiate advanced attacks simply by stealing user credentials. Mobile phishing is one of the most effective tactics to steal login credentials, which means that mobile phishing itself poses significant security, compliance, and financial risk to organizations in every industry. It is likely that the rise of remote work has contributed to this, as organisations relax bring-your-own- device (BYOD) policies to accommodate employees accessing corporate networks outside the traditional security perimeter.

Mobile phishing attacks are also growing more sophisticated. The share of mobile users in enterprise environments clicking on more than six malicious links annually has jumped from 1.6% in 2020 to 11.8% in 2022, indicating that users are having a tougher time distinguishing phishing messages from legitimate communications.

Long-term research on mobile usage in the UK* highlighted that phishing attacks increased in the first quarter of 2020, as threat actors took advantage of the pandemic-accelerated digital transformation. That spike declined and normalised through the rest of the year, then at the start of 2021, there was another significant increase of 47% between Q4 of 2020 and Q1 of 2021, and this time it wasn't an outlier. In the last two years, 20-30% of mobile devices in the UK have been exposed to at least one malicious phishing attack every quarter. There was a 35% increase in the average number of mobile devices exposed to at least one malicious phishing attack per quarter between 2020 and 2022.

App security

There have been issues with malicious apps, often disguised to appear legitimate, popular, and useful, such as a PDF reader or QR Scanner. As fast as the app store provider removes malicious apps, threat actors seek new ways of remaining undetected when they upload their malicious code. Often the apps have large numbers of positive reviews and many installations, so appear convincing[6].

One such malicious app is Sova[7 8] which prompts the user to enable the 'Accessibility Service' upon launching. With this permission, it exploits the service to automatically approve requested permissions, enable device administration, and initiate keylogging activities. It then connects the device to the attacker's server and downloads malicious code for the installed banking apps to collect the user's credentials.

An app that isn't outright malicious can still pose risk to your organisation's data. What data is being collected, do you know where that data is being sent and processed, what changes in data collection scope and transmission have occurred? It's often opaque, dynamic and hard to know exactly what apps are doing with your data.

In some cases, such concerns have even prompted government bodies to restrict or forbid the use of some mobile apps that have links to certain adversarial, or even rogue states. Whether it's a national security issue, as claimed by many government bodies across North America and Europe, or it's a compliance issue of geofencing data to align with laws like GDPR or CCPA — it's critical to understand how mobile apps could potentially access and handle sensitive data.

How to stay secure

You need confidence that the app is not operating in a dangerous way, that the data you are providing is acceptable to you and that the app developer is being responsible with your data. Whether it's tackling mobile operating system-level vulnerabilities, app risks as described above, or phishing and network threats, mobile security is critical to your security posture. Here are three key things to think about to better monitor and mitigate against these threats:

- **Think beyond just management:** Mobile device management (MDM) solutions serve a strong purpose, but there's a reason they're called management tools and not security tools. For app risks, MDMs have some control over what apps users install, but they have no visibility into the risks themselves.
- **Continuous risk-based monitoring:** You need real-time visibility into the app itself to minimise risks, such as what permissions they have, how data is being handled, the networks it communicates with, and the vulnerabilities and malicious codes embedded in them.
- **Consistent policy enforcement:** Many endpoint security solutions that have mobile capabilities are limited in the protections they can provide certain device types, which can result in gaps that open up devices, users, and data to compromise. A true mobile threat defence solution should enable the capability to enforce policy and protections consistently across all devices — regardless of whether they're iOS, Android, managed, BYOD, or company-owned, personally enabled (COPE) devices.

Given the undeniably prominent role that mobile devices have in how your employees work, mobile app risks cannot be ignored. Contact Vodafone to learn:

- How adversaries are leveraging avenues outside traditional email to conduct phishing on iOS and Android devices.
- Real-world examples of phishing and app threats that have compromised organisations.
- How to protect mobile users, devices, and your organisation's data.

Lookout mobile security

Vodafone Business has partnered with Lookout to provide a mobile security solution that empowers your employees to work the way they want. It's designed to fully protect your business' sensitive information. All without invading your workers' privacy.

Lookout is a solution that protects organisations and individuals from threats on mobile devices, for example phishing and malware. It is a lightweight mobile app that is available for iOS, Android and Chrome OS and monitors the security health of mobile devices in real-time, enabling you and your employees to directly react to issues without requiring a security expert or administrator.

6 https://www.threatfabric.com/blogs/deceive-the-heavens-to-cross-the-sea.html
7 https://blog.cyble.com/2023/03/09/nexus-the-latest-android-banking-trojan-with-sova-connections/
8 https://www.livemint.com/news/india/what-is-sova-virus-all-you-need-to-know-about-the-new-mobile-banking-virus-11663474696806.html

vodafone
business