Cyber Talk

STAYING SECURE IN THE NEW NORMAL:

MANAGING THE MOBILE APP MATRIX

Mobile health apps are exceedingly popular. They can be used to track disease exposure, as diagnostic devices or to simply make healthcare more accessible. Over 100,000 health apps exist on the iOS app store and Google Play combined and this number is expected to grow.[1] By 2026, the mobile health app market is projected to reach $57.57 billion in value.[2]

Examples of mobile health apps include coronavirus proximity tracking apps, heart rate variability apps, symptom trackers, and stress reduction apps. The leading health apps are scientifically validated, federally approved, and may genuinely reduce needs for acute care.

Yet, despite the fact that mobile health apps can deliver high value, their consumption could place your organization at risk of a security breach. Health apps often fail to include basic security protocols, some have malicious doppelgangers, others may perpetuate phishing attacks and yet others can introduce backdoors into your data.[3]

Given the nature of these issues, your organization should reassess mandated mobile health apps, reevaluate your app policies, and recalibrate your mobile security. The increasing ubiquity of mobile health apps means that mobile security is more important than ever before. Read on to learn more.

---

[1] A Cross-Sectional Study of Prominent US Mobile Health Applications: Evaluating the Current Landscape, Pierre-Antoine Fougerouse, Mobin Yasini, Guillaume Marchand, Oliver O. Aalami, PubMed, 16 April 2018.

[2] Fortune Business Insights, GlobeNewswire, 16 September 2020

[3] Most Healthcare Apps Are Riddled with Bugs, InfoSecurity Magazine, Phil Muncaster, 5 October, 2020

Health App Security Flaws: Taking Precautions and Preventing Infections

Organizations are using mobile health apps to make workplaces safer amidst the coronavirus. This is a reality for executives and workers in industry sectors ranging from manufacturing to construction to hospitality.

> A recent study shows that 71% of health-focused apps have at least one serious security vulnerability.

Some organizations have developed custom apps, while others have mandated the use of apps that are mass marketed. But, regardless of which type of app an organization chooses, a recent study shows that 71% of health-focused apps have at least one serious security vulnerability.[4] Here's what you should expect and how to protect in regards to both custom built health apps and mass marketed health apps:

Custom Built Health Apps:

Perhaps your organization wanted custom features and a specific type of analytics data. For organizations that have paid for custom built virus tracking apps or that are in the process of developing one, 83% of high-level threats can be mitigated using in-app protections.

In-app security tools can be used to quickly and easily build security into mobile applications. The use of app protection tools allow app developers to focus on product features instead of becoming security experts. Ensure that your app developers have access to in-app verification tools.

[4] Most Healthcare Apps Are Riddled with Bugs, InfoSecurity Magazine, Phil Muncaster, 5 October, 2020

Mass Market Health Apps:

For organizations that depend on publicly available health tracking apps, ensure that you can offer employees a security tool that blocks infected apps from infiltrating other apps within the phone. Your business apps could be breached due to unrelated apps on a device.

For example: A coronavirus tracking app could dump spyware onto a person's phone. This spyware could then pick up corporate account login credentials from the user's clipboard.

> " The assumption has always been that...apps can't interfere with each other easily," says University of California Riverside researcher, Zhiyun Qian. "... that assumption is not correct and one app can in fact significantly impact another and result in harmful consequences..." [5]

If relevant to your organization, be sure to invest in dev team tools that can build security into apps. Alternatively, invest in security tools that can block infected devices or apps from accessing corporate data.

[5] Malicious Android Apps Can Hack Gmail, PC Magazine, Stephanie Mlot, 22 August 2014

Health App Security Flaws: Blocking Fake Health Apps

In 2020, governments across Europe, the Americas and Asia-Pacific launched a variety of contact tracing apps. Each app was built to accommodate a different sets of standards. An assessment of 17 of these apps shows that several have serious security flaws. The flaws discovered can enable hackers to create malicious clones of authentic apps.[6] Here's why this is a problem:

Recently, a group of hackers released a clone of an authentic app and sent an email to pharmacies, doctors, universities and other groups, telling them to download it. While the victims engaged with legitimate looking app content (a global map of coronavirus cases), ransomware ran in the background and mined user data. This user data was then leveraged to shut down network systems.

As visible in the example above, a clone of a contact tracing app could lead to serious consequences. This attack occurred in Italy, and yet this type of attack could occur anywhere in the world. Ensure that your organization has safeguards in place to keep your data out of hackers' hands. Get mobile security that's capable of blocking fake apps.

Health App Security Flaws: Preventing Phishing

The rapid transition to remote work has accelerated the development and deployment of mobile attack tactics. In the US, more than 65% of corporate mobile users saw an increase in mobile phishing threats when comparing Q4 2020 with Q4 2019.[7] Organizations need to protect their employees from health app-based phishing scams. Here's what can happen without mobile phishing safeguards:

An employee may accidentally download a malicious clone of an authentic app. Hackers may then send pop-up phishing notifications, posing as app service providers or other officials. An alleged app service provider's notification might read as: *"We've revised our user policies. Please sign the new agreement form and update your user information through the link below"*.

---

[6] Majority of COVID-19 Contact Tracing Apps Lack Adequate Security, HealthitSecurity.com, Jessica Davis, 19 June, 2020

[7] Mobile Phishing Attacks Increase Sharply, Dark Reading, Jai Vijayan, 2 June 2020.

> Amidst the pandemic, workers may be distracted by children, pets or more direct coronavirus-related challenges, and fail to spot phishing attacks. Small screens on mobile devices can lead people to overlook standard signs of phishing attempts.

A user may then click on the associated link and enter requested credentials, entirely unaware of the scam.

It's not just the user who may lose data here; if the 'new agreement form' requests certain work-related information, organizations can lose valuable data through these scams as well.

To reduce mobile phishing risks, organizations should ensure that mobile users are equipped with anti-phishing tools. The most sophisticated anti-phishing tools leverage threat intelligence databases and can offer zero-day threat protection.

Health App Security Flaws: Backdoors and Blocking MitM Attacks

Third-parties can have "backdoor" access to apps, including health apps. Although third-party access may be limited, you may want to reassess this aspect of any mandated workplace health app. Revisit who is authenticated to view app data and who is permitted to make changes to the app itself.

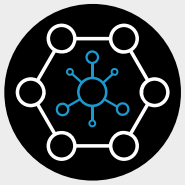
When third-parties have access to apps, hackers can gain access more easily than otherwise and can then launch man-in-the-middle attacks (MitMs).

Why worry about MitM attacks?

These types of attacks are particularly difficult to detect and MitM attacks can lead to data theft and the manipulation of data.

Most of the time, security features to block MitM attacks are not built into original version of apps due to lack of security skills among app developers or a rush to market.

But the right security features can make MitM attacks nearly impossible to execute. Advanced MitM security for employees' mobile devices is essential, especially as people download increasing numbers of health apps. Be sure that your mobile device security can protect against MitM attacks.



What C-levels should know about in-app data sharing:

- **The majority of mHealth apps do share user data for commercial purposes. Most app store downloads are not HIPAA compliant nor are they subject to HIPAA.**
- **Of 36 depression and smoking cessation apps, researchers discovered that 29 shared data with tech titans, but only 12 accurately conveyed this information to consumers.**
- **Mandating certain types of virus-tracking apps for your teams could lead to privacy problems and MitM attacks.**

Conclusion:

You can't afford to prevent employees from using mobile devices for work purposes. This could lead to a drop in productivity. You also can't afford to face a data breach. To guard against this, backstop your security with built-in app protection tools, mobile threat detection tools that can block fake apps, anti-phishing safeguards, MitM security and more. For a comprehensive mobile device security management solution, consider SandBlast Mobile.

Case Study:

The Spanish legal firm Perez-Llorca wanted to protect its fleet of 350 corporate mobile devices. To do so, they opted for a leading mobile security and threat prevention solution. Says Perez-Llorca's CTO, Aitor Lasala, *"We realized that security for our mobile devices was a must."*

The Perez-Llorca firm is built on expertise, confidentiality and trust. *"A phone contains as much information as a laptop. With SandBlast Mobile, we're taking care of our data, whether it roams within our perimeter or outside of it. It means we can analyze both the network and the apps installed on the device in an efficient way. We can manage the risk level of a device and the malicious activity that tries to reach it,"* says Lasala.

For more information on mobile device security, contact your Check Point sales representative.

Worldwide Headquarters
5 Ha'Solelim Street, Tel Aviv 67897, Israel | Tel: 972-3-753-4555 | Fax: 972-3-624-1100 | Email: info@checkpoint.com

U.S. Headquarters
959 Skyway Road, Suite 300, San Carlos, CA 94070 | Tel: 800-429-4391; 650-628-2000 | Fax: 650-654-4233

www.checkpoint.com