



**iGms**  
*Cyber Solution*



**iGms**  
*Cyber Solution*

## How PWA Technology Can Steal Banking Login Credentials from iOS and Android Phones



Author – Andrew Smith

August 2024

---

## ***Introduction to Progressive Web Applications (PWAs)***

Progressive Web Applications (PWAs) represent a significant advancement in web technology, seamlessly blending the accessibility of web pages with the functionality of native mobile applications. At their core, PWAs leverage standard web technologies such as HTML, CSS, and JavaScript to deliver user experiences that are fast, reliable, and engaging.

One of the standout features of PWAs is their offline capabilities. Utilizing service workers, which act as proxy servers between the network and the device, PWAs can cache resources and ensure continuous functionality even when offline. This makes them particularly appealing to users in regions with inconsistent internet connectivity.

PWA technology also promotes responsive design, ensuring that applications work well on any device, from desktop computers to mobile phones. This adaptability is pivotal in an era where users access content across a wide range of screen sizes and resolutions.

Another major advantage is the ease of installation. Unlike traditional native apps, which require downloading from app stores, PWAs can be added directly from a web browser. Users can save PWAs to their home screen with just a few taps, reducing friction and increasing adoption rates. Additionally, PWAs support push notifications, allowing businesses to re-engage users with timely updates and personalized content.

The popularity of PWAs is on the rise, driven by these compelling features and the potential for cost savings. Developing a single PWA instead of multiple platform-specific apps (iOS and Android) can significantly reduce development and maintenance costs for businesses. Furthermore, PWAs often offer improved performance and user satisfaction, leading to increased engagement and customer retention.

In simpler terms, PWAs work by employing service workers, which manage the caching of resources and handle network requests. This ensures that content is delivered swiftly and reliably. The combination of these elements forms the foundation of PWAs, transforming them into a formidable alternative to traditional mobile applications.

### ***Security Concerns Associated with PWAs***

Progressive Web Applications (PWAs) bring forward a blend of web and mobile application features, promising accessibility and functionality. However, as their adoption increases, so do the associated security concerns. While PWAs are designed to offer a secure environment, certain vulnerabilities can still be exploited by malicious entities to steal sensitive information, including banking login credentials from iOS and Android devices.

One prominent risk is the creation of fake PWAs. Cybercriminals can develop PWAs that mimic the appearance of legitimate banking applications, misleading users into entering their credentials on these fraudulent platforms. Once the information is entered, it is siphoned off to remote servers controlled by the attackers, compromising users' financial data.

A familiar security threat often encountered in the realm of PWAs is cross-site scripting (XSS). In an XSS attack, an adversary injects malicious scripts into a legitimate PWA, which then executes on the user's device. These scripts can capture keystrokes, steal cookies, or redirect users to phishing websites, making them particularly dangerous.

---

Man-in-the-middle (MitM) attacks also pose a significant hazard. Since PWAs often rely on web technologies and internet connectivity, they are exposed to interception and tampering of data exchanges. An attacker can intercept the communication between the PWA and the server, gaining unauthorized access to sensitive information such as login credentials, personal data, and financial details.

Insecure data storage is another critical issue. PWAs may store data locally on the device to enhance user experience and performance. However, if this data is not properly encrypted or secured, it becomes an easy target for attackers. Accessing unprotected data storage can lead to unauthorized retrieval of sensitive information, compromising user privacy and security.

In light of these threats, it is imperative for developers to implement robust security measures, and for users to remain vigilant when engaging with PWAs, particularly those related to financial transactions. Understanding these risks and taking appropriate precautions can significantly mitigate the potential for cybercriminal activities targeting PWA technology.

### ***How PWAs Steal Banking Login Credentials***

Progressive Web Applications (PWAs) have revolutionized how users interact with web content, but they also pose significant security risks, especially regarding banking login credentials. A malicious PWA can be designed and distributed through various deceptive means, making unsuspecting users easy targets. The process typically begins through phishing attacks, where users receive seemingly legitimate communications—often through email or text—encouraging them to install a PWA for better banking experience or improved security features.

Once users are convinced to install the malicious PWA, several mechanisms come into play to capture sensitive information. A common method involves creating fake login screens that closely resemble the legitimate banking app or website. These screens prompt users to input their credentials, which are then intercepted and transmitted to the attackers. The sophistication of these fake screens makes them nearly indistinguishable from authentic ones, leading to a high success rate in credential theft.

Another method malicious PWAs employ is keylogging. Integrated keylogging capabilities can record every keystroke made by the user within the PWA. This data includes usernames, passwords, account numbers, and even security questions and answers. The captured keystrokes are then sent to the attackers in real-time or at set intervals, providing them with continual access to fresh login information.

The ease with which users can be tricked into installing these malicious PWAs is alarming. Often, these apps are distributed through unofficial app stores or third-party websites, and sometimes even infiltrate official app stores due to their initial harmless appearance and functionality. Once installed, the PWA can request permissions that seem appropriate for a banking application, such as access to network connectivity, which further aids in the transmission of stolen data.

The risk is evident in real-life examples where malicious PWAs have duped users. In one notable scenario, a fake banking PWA disguised as a reputable financial institution's app was downloaded thousands of times before being detected. While specific outcomes vary, the underlying threat remains clear: users must exercise extreme caution when installing any PWA, particularly those related to sensitive functions like banking.

---

### ***Protecting Yourself Against PWA Security Threats***

As Progressive Web Apps (PWAs) become increasingly popular, understanding how to protect yourself from potential security threats is crucial. One practical approach is to scrutinize the source of any PWA before installation. This can be done by downloading apps exclusively from trusted repositories such as the Google Play Store or Apple App Store, where rigorous security checks minimize the risk of encountering malicious applications.

Reading user reviews and ratings can also help identify fake or suspicious PWAs. Authentic reviews often highlight the app's legitimacy or raise flags about potential issues. Equally important is verifying the permissions requested by the app. While some permissions are necessary for functionality, excessive or unrelated requests should be treated with caution. For instance, an app claiming to be a simple calculator should not require access to your contacts or messages.

Keeping your devices updated with the latest software patches is another essential measure. Manufacturers often release security updates to address vulnerabilities, and staying current reduces the risk of exploitation by malicious PWAs. Coupled with this is the importance of using reputable antivirus software, which can provide an additional layer of protection by scanning for and alerting you to potential threats.

Moreover, be mindful of the information you share on mobile apps. Sensitive data such as banking credentials, personal identification numbers, and other critical information should be handled with the utmost care. Limiting the amount of personal information shared reduces the potential impact should a security breach occur.

Organizations and developers also play a critical role in safeguarding their PWAs. Adhering to best practices for security, such as employing robust encryption, conducting regular security audits, and keeping abreast of the latest threats, can dramatically reduce vulnerabilities. Educating customers on how to use PWAs safely, through clear communication and user guides, helps foster a more secure environment for all.

By taking these precautionary steps and maintaining vigilance, both users and developers can significantly mitigate the security risks associated with PWAs, ensuring a safer digital experience.