Innovation Growth Partners Specialty®

**CONTACT US**

**Dave Perkins,** RPLU
(508) 848-4263
dave.perkins@igpspecialty.com

# What is Pixnapping?

Pixnapping is a new type of side-channel attack that allows a malicious app on an Android device to steal sensitive on-screen data, such as private messages and two-factor authentication (2FA) codes. This is done by measuring microscopic timing variations in how the phone's graphics processing unit (GPU) handles pixels. The attack was recently discovered by a team of cybersecurity researchers from several U.S. universities.

## How a Pixnapping Attack Works

**MALICIOUS APP INSTALLATION:** The attack begins when a user installs a malicious app, which requires no special permissions. These apps could be disguised as something harmless to trick users into downloading them.

**TARGET APP INVOCATION:** The malicious app uses standard Android system commands (called "intents") to cause a target application—like Google Authenticator, Signal, or Venmo—to display sensitive information.

**PIXEL STEALING:** As the target app's screen content is being rendered, the malicious app performs graphical operations on individual pixels. It then exploits a known hardware side channel (referred to as "GPU.zip") by measuring the minuscule amount of time it takes to render those pixels.

**DATA RECONSTRUCTION:** By analyzing the timing differences, which vary based on pixel color, the attacker can reconstruct the victim's screen content pixel-by-pixel. This information can then be converted into text using optical character recognition (OCR).

## Affected Devices and Mitigations

**VULNERABLE DEVICES:** Researchers successfully demonstrated the attack on Google Pixel 6 through 9 phones and the Samsung Galaxy S25, running Android versions 13 through 16. Other modern Android devices may also be vulnerable.

**GOOGLE'S RESPONSE:** Google was notified of the vulnerability and released a partial patch in September 2025 (tracked as CVE-2025-48561). However, the researchers found a workaround, and Google released an additional patch in December 2025.

**ONGOING RISK:** Until a comprehensive fix is rolled out to all affected devices, users remain at risk. The exploit is difficult to carry out, but a malicious app could automate the process. Users should avoid downloading apps from untrusted sources and install security updates as soon as they become available.

## What Data Can Be Stolen?

Pixnapping vulnerability allows attackers to steal any information that is visibly displayed on the screen. This includes:

- Two-factor authentication (2FA) codes
- Private chat messages
- Emails
- Financial information
- Location data from apps like Google Maps Timeline

©2026 Innovation Growth Partners Specialty, LLC | igpspecialty.com