Is AirDrop Still Safe?

Maria Cattini | 01/05/2025 | CYBERSECURITY

What We Know About the Privacy Flaw Exposing Your Data

AirDrop is one of Apple users' favorite features — quick, wireless sharing of photos, files, and links with nearby devices. But behind this seamless experience hides a long-standing vulnerability that still hasn't been fully addressed.

According to researchers at Technische Universität Darmstadt, AirDrop's device discovery feature remains vulnerable to an attack that can expose personal data — like your email address and phone number — simply by intercepting the connection process.

The most alarming part? This flaw is still active today.

Why It's Dangerous (and How It Works)

When you enable AirDrop, your device scans for others nearby. If your AirDrop is set to "Contacts Only," it checks if you're in someone's contact list by comparing hashed versions of phone numbers and email addresses.

These cryptographic hashes are supposed to be secure.

But here's the catch: the German researchers showed that these hashes can be cracked using brute-force attacks, especially when the attacker is on the same network — like a public Wi-Fi — and within Bluetooth range.

In short, someone nearby could sniff out your info without even being in your contacts.

□□ Has Apple Fixed the Problem?

No. The vulnerability was reported back in 2019 and, as of now, there's still no official patch. Despite concerns raised by the cybersecurity community and repeated alerts from academics, Apple has remained silent on any permanent fix.

Meanwhile, more than 1.5 billion Apple devices are potentially exposed — particularly in crowded spaces like airports, schools, events, or coworking hubs.

□□ How to Stay Safe: Simple Steps You Can Take

The good news? You can protect yourself — and it only takes a few seconds.

□ Turn Off AirDrop When Not in Use

On iOS (iPhone/iPad):

• Open Control Center
• Long-press the box with Wi-Fi and Bluetooth icons
• Tap AirDrop
• Choose Receiving Off

□□ AirDrop on macOS (Mac)

• Open Finder
• Go to AirDrop
• At the bottom, click "Allow me to be discovered by"
• Select No One

⚠ Avoid Unsecured Public Wi-Fi

The risk is much higher when using unencrypted public Wi-Fi. If you must use one, always activate a trusted VPN to stay protected.

□□ Safer Alternatives for File Sharing

Need to send files securely? Try these instead:

• iCloud Drive with private sharing links
• Encrypted services like ProtonDrive or Tresorit
• Password-protected WeTransfer links

These options don't expose your personal data during the sharing process.

□□ A Persistent Issue in a Privacy-Critical World

In today's digital age, even the most basic features can pose serious privacy threats.

Apple has built a reputation around device security — but this unresolved flaw raises tough questions about how it handles known vulnerabilities and user transparency.

AirDrop is still incredibly useful — but until stronger protections are implemented, use it with care.

What We Know About the Privacy Flaw Exposing Your Data

AirDrop is one of Apple users' favorite features — quick, wireless sharing of photos, files, and links with nearby devices. But behind this seamless experience hides a long-standing vulnerability that still hasn't been fully addressed.

According to researchers at Technische Universität Darmstadt, AirDrop's device discovery feature remains vulnerable to an attack that can expose personal data — like your email address and phone number — simply by intercepting the connection process.

The most alarming part? This flaw is still active today.

□□ Why It's Dangerous (and How It Works)

When you enable AirDrop, your device scans for others nearby. If your AirDrop is set to "Contacts Only," it checks if you're in someone's contact list by comparing hashed versions of phone numbers and email addresses.

These cryptographic hashes are supposed to be secure.

But here's the catch: the German researchers showed that these hashes can be cracked using brute-force attacks, especially when the attacker is on the same network — like a public Wi-Fi — and within Bluetooth range.

In short, someone nearby could sniff out your info without even being in your contacts.

□□ Has Apple Fixed the Problem?

No. The vulnerability was reported back in 2019 and, as of now, there's still no official patch. Despite concerns raised by the cybersecurity community and repeated alerts from academics, Apple has remained silent on any permanent fix.

Meanwhile, more than 1.5 billion Apple devices are potentially exposed — particularly in crowded spaces like airports, schools, events, or coworking hubs.

□□ How to Stay Safe: Simple Steps You Can Take

The good news? You can protect yourself — and it only takes a few seconds.

Turn Off AirDrop When Not in Use

On iOS (iPhone/iPad):

- Open Control Center
- Long-press the box with Wi-Fi and Bluetooth icons
- Tap AirDrop
- Choose Receiving Off

AirDrop on macOS (Mac)

- Open Finder
- Go to AirDrop
- At the bottom, click "Allow me to be discovered by"
- Select No One

⚠ Avoid Unsecured Public Wi-Fi

The risk is much higher when using unencrypted public Wi-Fi. If you must use one, always activate a trusted VPN to stay protected.

Safer Alternatives for File Sharing

Need to send files securely? Try these instead:

- iCloud Drive with private sharing links
- Encrypted services like ProtonDrive or Tresorit
- Password-protected WeTransfer links

These options don't expose your personal data during the sharing process.

A Persistent Issue in a Privacy-Critical World

In today's digital age, even the most basic features can pose serious privacy threats.

Apple has built a reputation around device security — but this unresolved flaw raises tough questions about how it handles known vulnerabilities and user transparency.

AirDrop is still incredibly useful — but until stronger protections are implemented, use it with care.