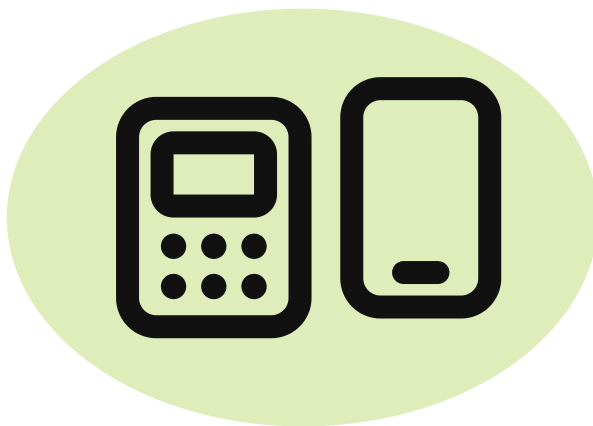


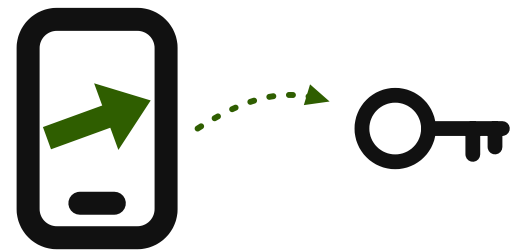
Tap, Touch and Near, Explained

What happens when you tap to pay, whether your wallet needs a shield, and how your phone finds your keys.



Tap to pay

It only works up close



Find your keys

Your phone points the way

The short answer

Your phone has two radios for things up close. One works when you tap to pay. The other helps you find your keys.

Tapping to pay is safe. Each payment uses a code that works only once. For your bank cards, you don't need a special wallet.

This guide answers three questions. What are these radios? Why do they matter to you? And what should you watch out for?

A word on the words

NFC is the radio for a tap. **Ultra Wideband**, or UWB, is the radio that measures how far away something is. The **reader** is the box at the store or gate that you tap.

What's inside

A tap has to be a tap	3	Finding your keys	10
What a tap sends	4	Four things people get wrong	13
Does your wallet need a shield?	7	Habits worth keeping	13
Where the real risk is	9	Where these facts come from	14

A tap has to be a tap

A tap card has no battery. It borrows a tiny bit of power from the reader, just long enough to answer.

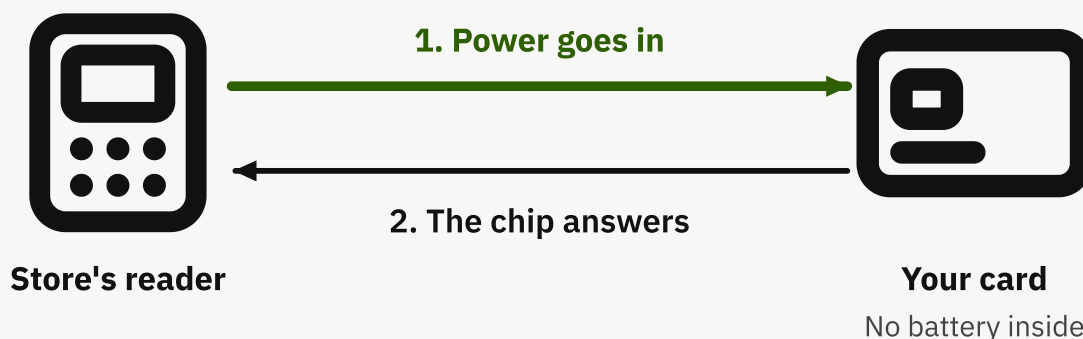


Figure 1. The card runs on the reader's power. The green arrow is the power going in. Only then can the chip answer.

That power fades fast. Move the card a hand's width away and it can't wake up at all. That's on purpose. A payment should happen only when you mean it to.

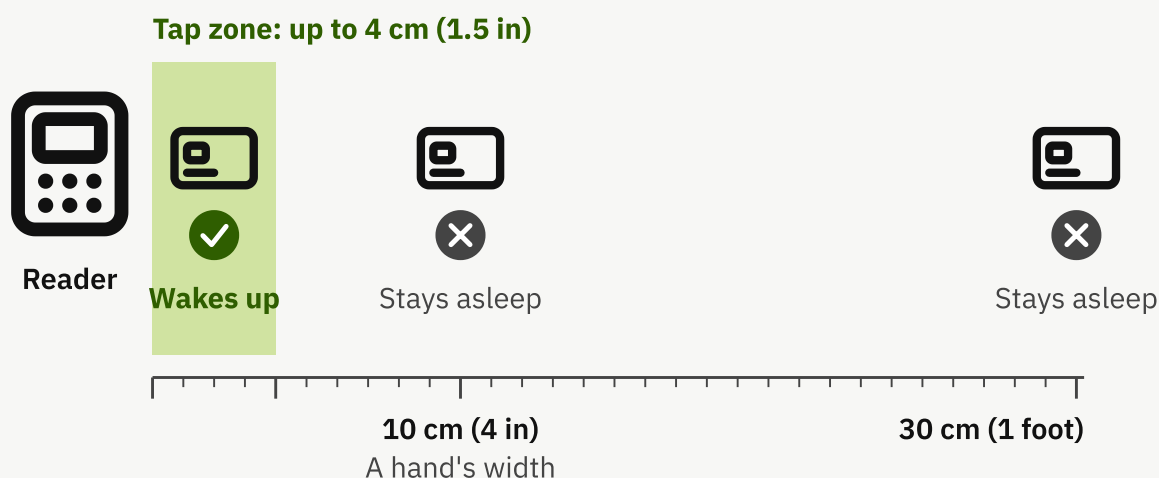
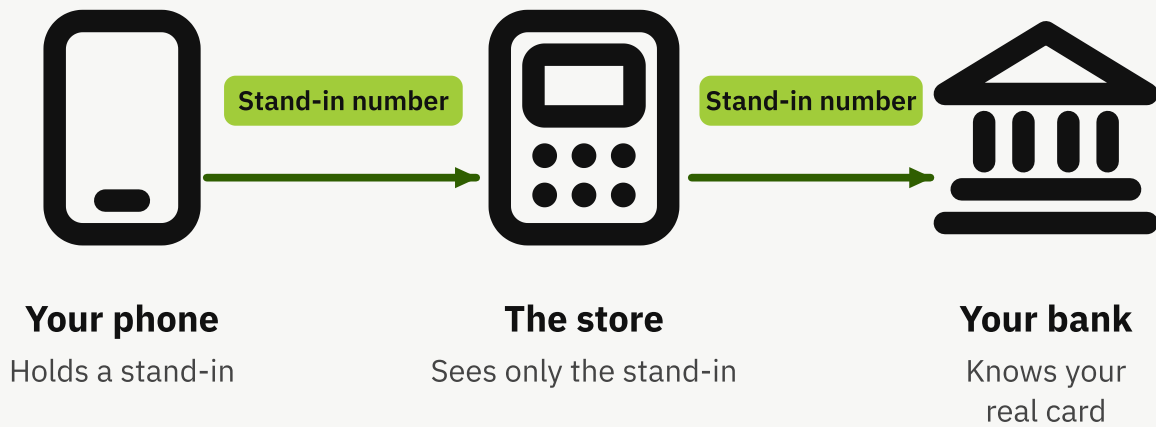


Figure 2. How close is close. Only a card inside the green tap zone wakes up. Roughly to scale.

You use this every day: paying at a store, getting through a transit gate, opening a hotel door, or tapping a badge at work.

What a tap sends

When you pay with your phone or watch, the store never gets your card number. Your phone sends a stand-in number instead.

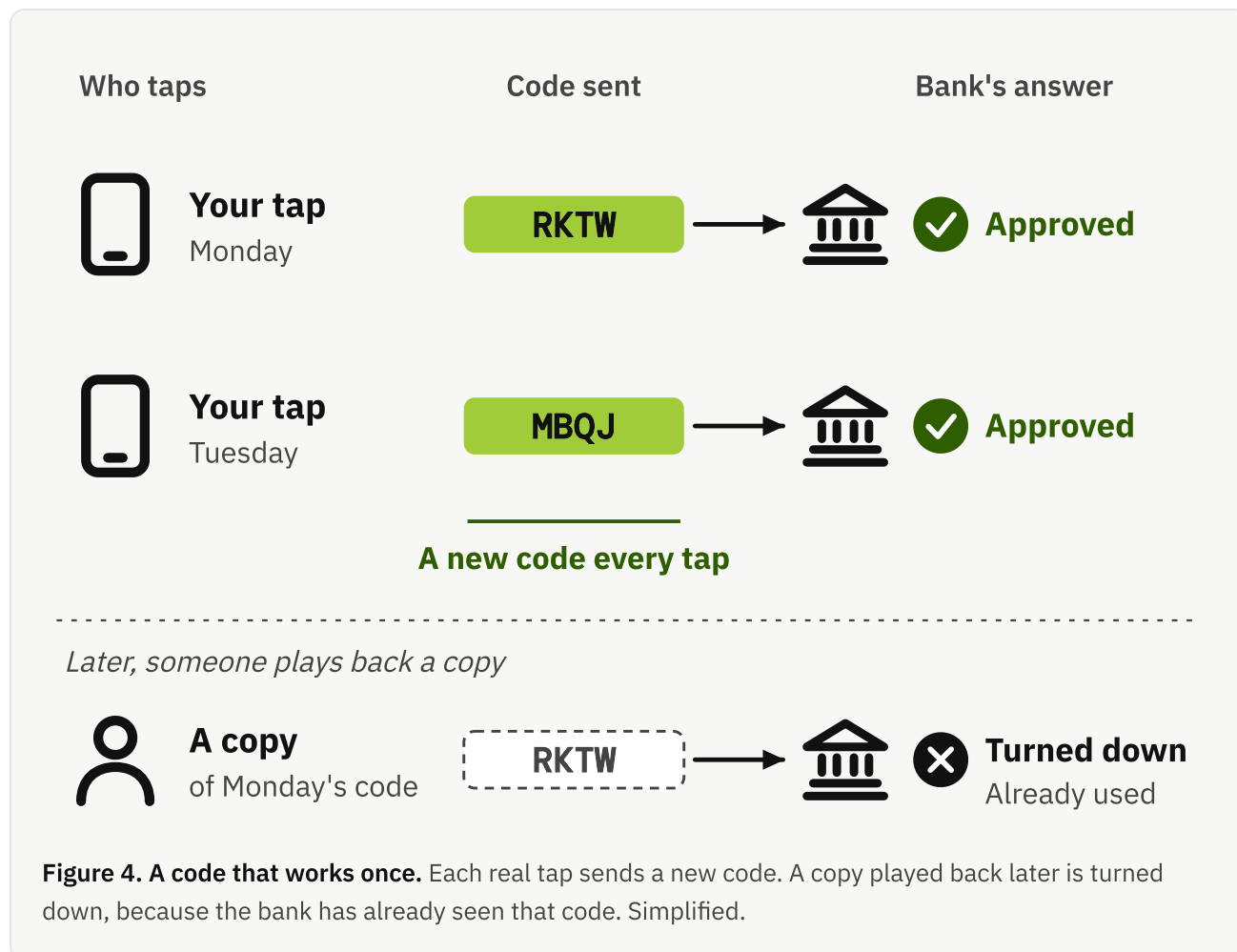


Your real card number never reaches the store

Figure 3. The store gets a stand-in, not your card number. Follow the green tags from your phone to your bank. Simplified.

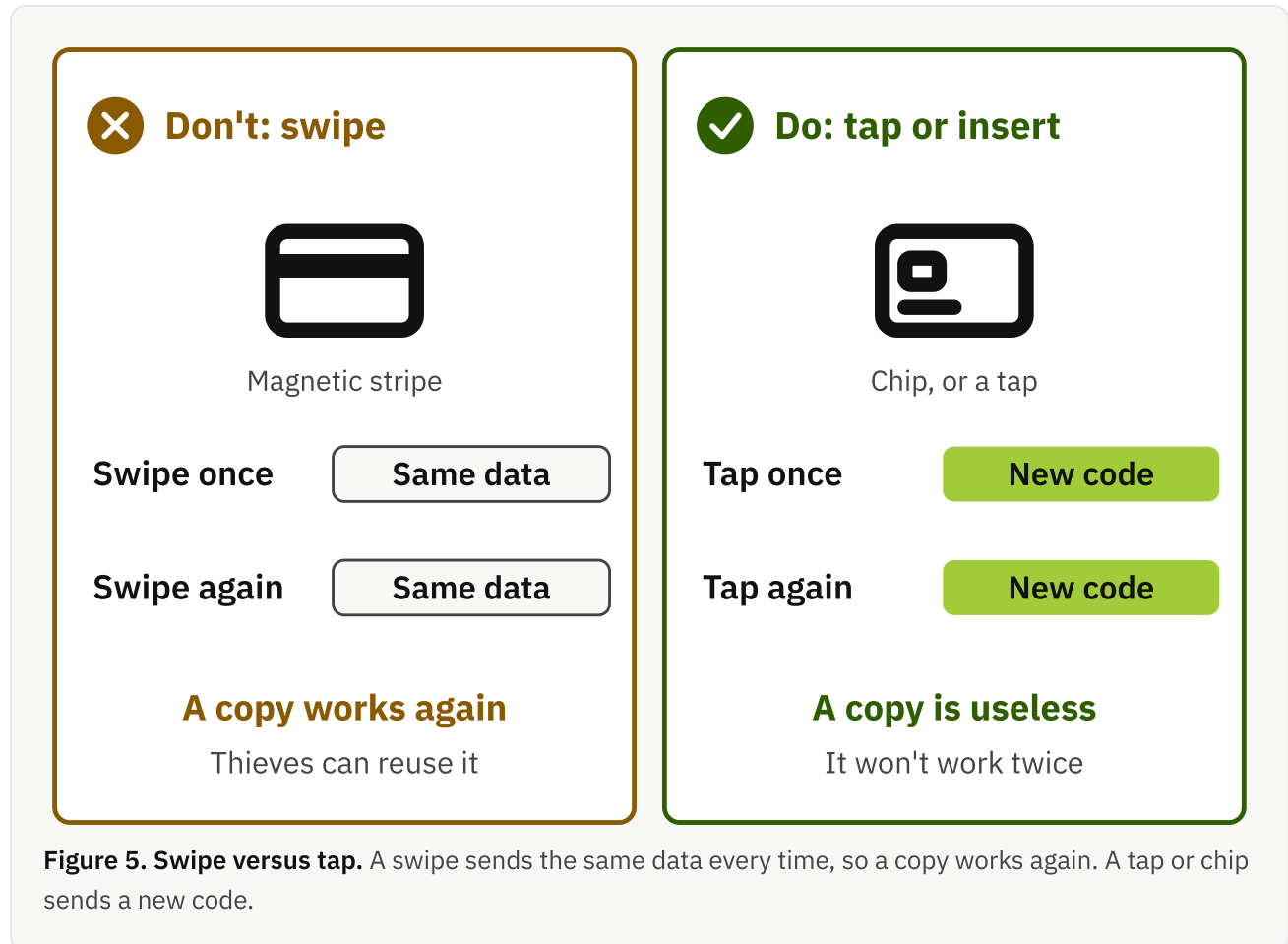
WHAT A TAP SENDS

With a phone, a card or a watch, every tap also sends a new code. The code works for that one purchase only. If someone copies it, the bank turns it down.



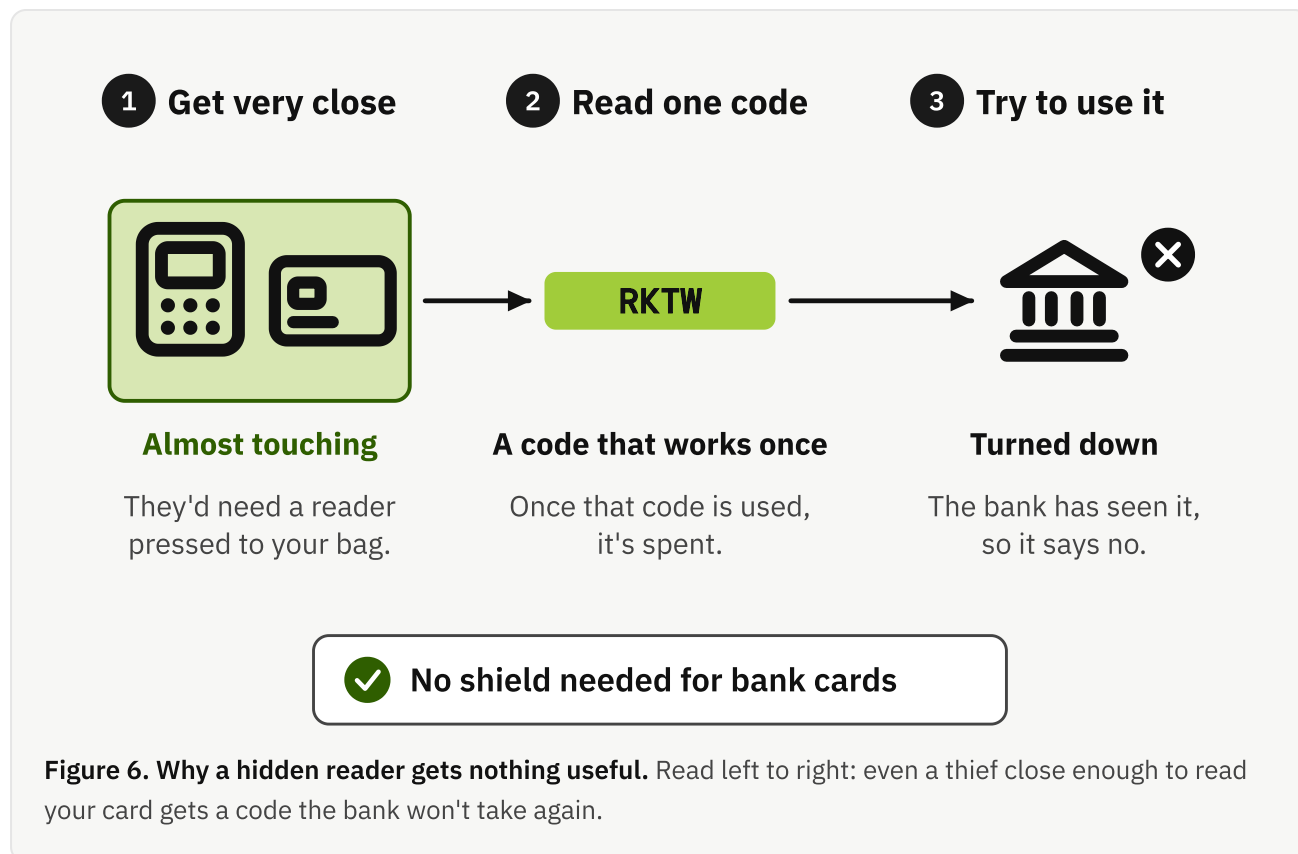
WHAT A TAP SENDS

The old magnetic stripe is different. It sends the same data every time you swipe. That's the part thieves copy. So tap or insert your card instead of swiping.



Does your wallet need a shield?

For bank cards, no. A thief would have to hold a reader right against your card. Even then, the code they get works only once.



If you like your blocking wallet, keep using it. It does no harm. You just have to take the card out to tap.

THE WALLET QUESTION



Bank card

Built for a tap,
only up close



No shield needed



Passport book

Shielding is
in the cover



Just close it



Passport card

Made to be read
from farther away



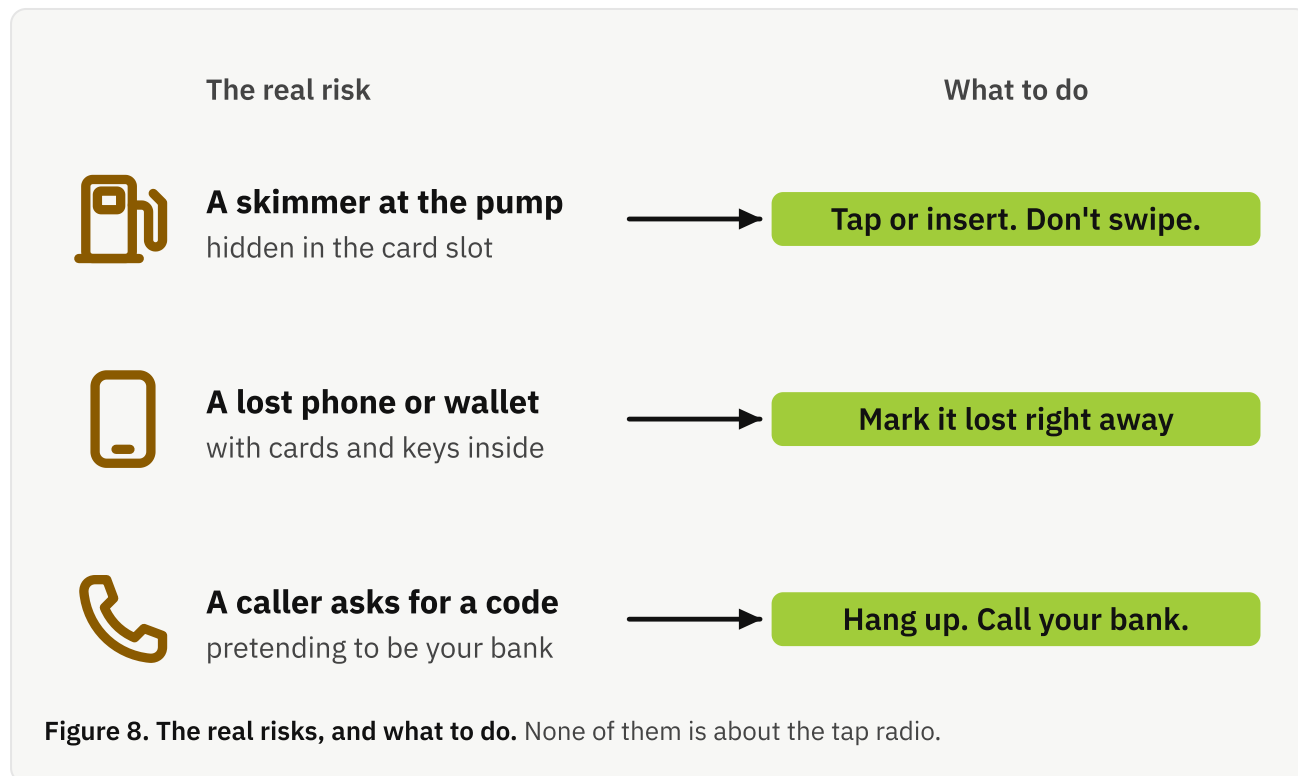
Keep it in its sleeve

Figure 7. Three cards, built three ways. A bank card is built for a tap. A passport book has shielding in its cover. A passport card is made to be read from farther away, so it comes with its own sleeve.

The one exception is a US passport card, and a few other border cards like it. They're built to be read at a distance at a border crossing. Keep yours in the sleeve it came in.

Where the real risk is

The real risks aren't about radios at all. They're older tricks.



A card skimmer. Thieves hide a fake reader in the card slot at a gas pump or a cash machine. It copies the magnetic stripe. Tap or insert your chip instead of swiping.

A lost phone or wallet. If your phone goes missing, mark it lost right away. On iPhone, use Find My. On Android, use Find Hub. That turns off the cards and keys stored in it. If a card goes missing, call your bank.

STOP

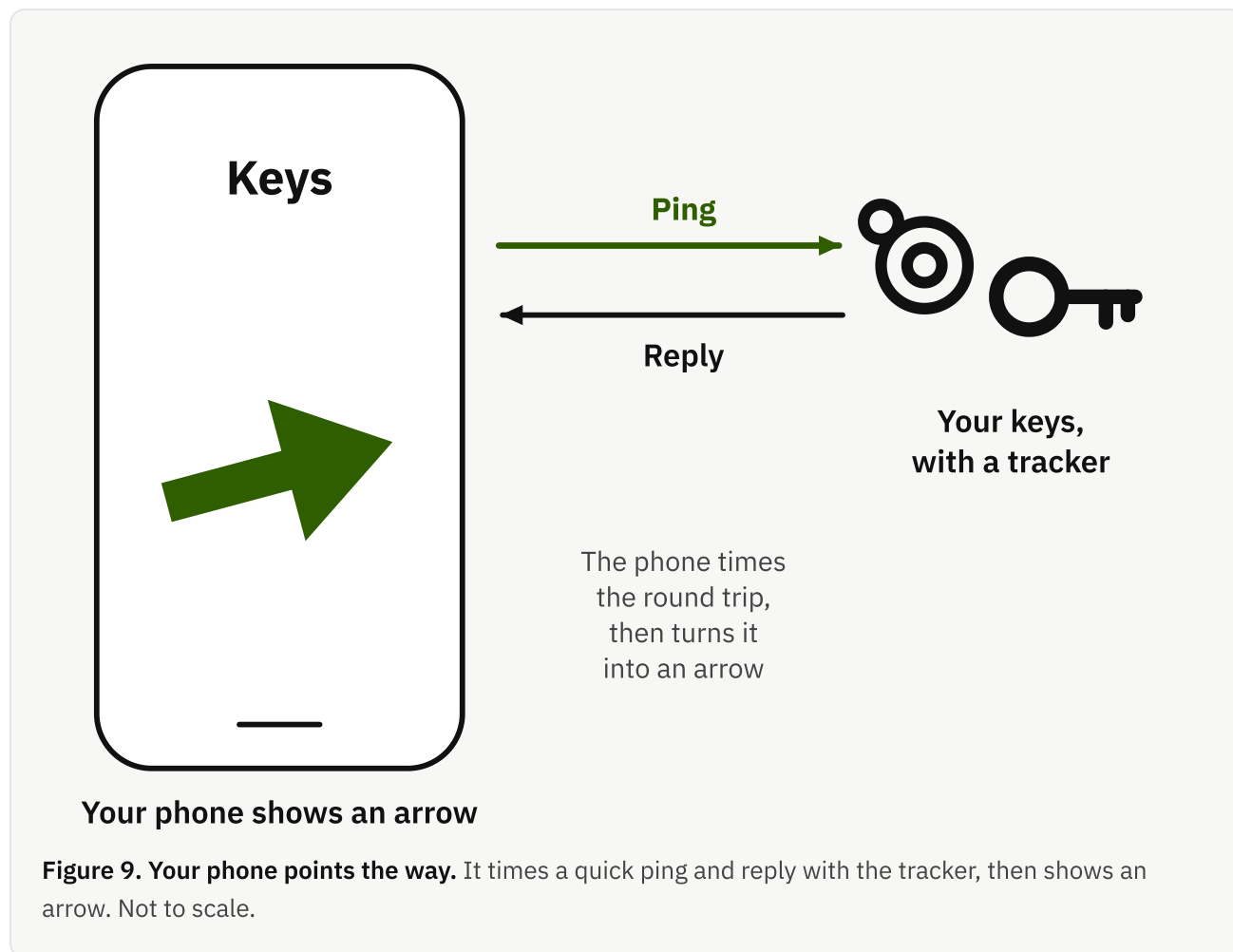
Never share a code your bank texts you

Scammers call pretending to be your bank. They ask for the code that just arrived on your phone. Your bank will never ask for it. Hang up and call your bank on a number you already know.

One more free habit: turn on purchase alerts in your bank's app. Then a charge you didn't make shows up on your phone the same day.

Finding your keys

Ultra Wideband measures distance by timing. One device sends a quick ping, the other answers, and the phone times the trip.

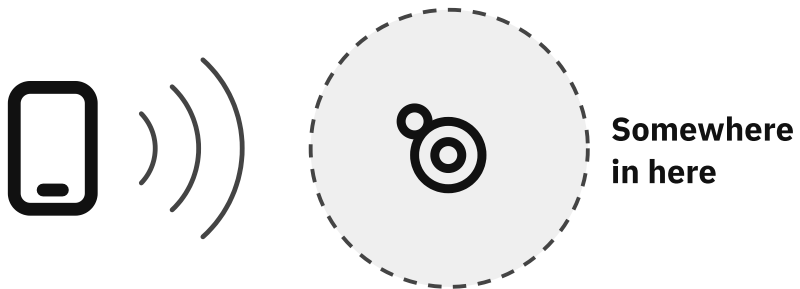


That timing is exact. It can tell where something is to within a few centimeters (about an inch).

Bluetooth

How loud is it?

A rough guess



Ultra Wideband

How long did it take?

An exact answer

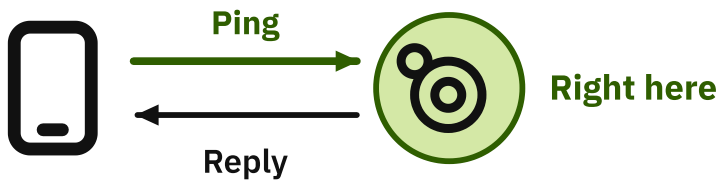


Figure 10. Two ways to judge distance. Most Bluetooth gear guesses by how loud the signal sounds. Ultra Wideband times it, which is far more exact. Not to scale.

ULTRA WIDEBAND

Some newer cars use it too. Your phone can be the car key. The car checks that the phone is close before it unlocks. That stops thieves who try to pass a key's signal along from far away.

Your phone at the car



Thieves pass the signal along

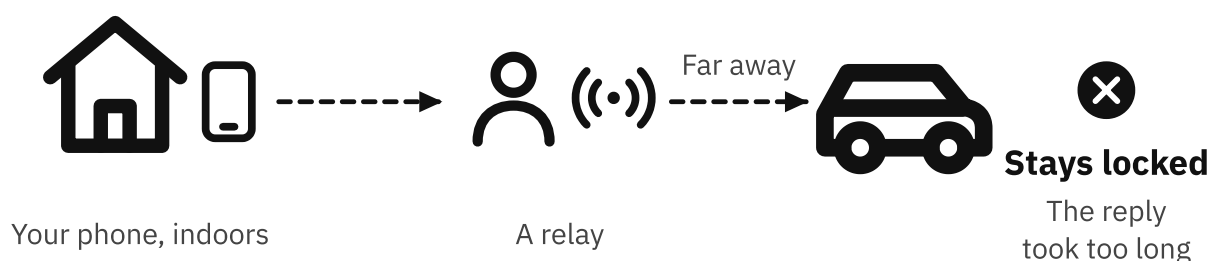


Figure 11. The car checks the timing. A signal passed along from far away takes too long, so the car stays locked. Not to scale.

Looking for your tracker?

Find My, Explained covers the arrow that leads you to a lost item. *Bluetooth, Explained* covers earbuds, speakers and your car stereo.

STRAIGHT FACTS

Four things people get wrong

MYTH Someone can read my card from across the room.

FACT A bank card only answers a reader held right up to it. And the store has to start the payment.

MYTH My bank cards need a blocking wallet.

FACT They don't. Each tap uses a code that works only once. A sleeve does matter for a US passport card.

MYTH Tapping a card is less safe than swiping it.

FACT A phone or watch sends a stand-in number. A card does send its number, but with a one-time code, so a copied tap can't be used again.

MYTH Ultra Wideband is just Bluetooth.

FACT They're different radios. Ultra Wideband times its signal to find exactly where something is.

Habits worth keeping

- 1 Tap or insert, don't swipe.** Especially at a gas pump.
- 2 Pay with your phone or watch when you can.** The store never gets your card number.
- 3 On transit, tap in and out with the same card or phone.** Keep your other tap cards away from the gate.
- 4 Never give anyone a code your bank texts you.** Hang up and call your bank yourself.
- 5 If your phone goes missing, mark it lost.** That switches off its cards and keys.

SOURCES

Where these facts come from

Checked on 28 September 2026.

- NFC Forum, nfc-forum.org home page ("just a few centimeters apart", 13.56 MHz) and NFC Technology page (card, reader and peer-to-peer roles)
- Visa, Contactless Payments FAQ, usa.visa.com (1 to 2 inches, what a card sends, one-time code, merchant must start the payment, "very unlikely and limited in scope")
- EMVCo, The What, Why and How of EMV Payment Tokenisation (a token replaces the card number)
- Apple 101554, Apple Pay security and privacy (27 April 2026); Apple 105123, Express Mode (18 November 2025); Apple 118271, car keys (18 September 2025)
- Google Wallet Help 7643925 (virtual card, screen lock) and 12060041 (digital car key); Google Pixel Phone Help 3470787 (NFC switch)
- FTC consumer alerts: "Watch out for card skimming at the gas pump" (7 August 2018); "What's a verification code and why would someone ask me for it?" (7 March 2024)
- Federal Register, 25 October 2005, Electronic Passport final rule (anti-skimming cover, about ten centimeters); Federal Register, 31 December 2007, Card Format Passport final rule (one number only, protective sleeve)
- Transport for London, Card clash, tfl.gov.uk
- FiRa Consortium: How UWB Works (500 MHz, 2 ns pulses); Technical FAQ (few centimeters, 30 cm, 100 m, signal strength); UWB Terminology (25 September 2023); Why Automakers Are Embracing UWB (4 April 2025)
- Car Connectivity Consortium, Cars That Use Digital Keys in 2026 (NFC, Bluetooth and UWB; relay attacks)

About this guide

Written for people who aren't technical and want to know what their phone does when they tap, and whether their wallet needs a shield. Apple, iPhone, Google, Android, Visa and Bluetooth are trademarks of their owners. This guide is independent and isn't affiliated with or endorsed by any of them.

About the author

Keith Parsons, CWNE #3, has designed, installed and troubleshoot Wi-Fi for over 25 years. He runs Wireless LAN Professionals and the WLPC conferences.