Payment Method Red-Flag Chart

Why certain payment requests deserve extra verification. Educational only — protections vary by bank, provider and country.

If they ask you to pay by…	Why scammers like it	How hard is it to get money back?	What a scam looks like
Gift cards	Instant, anonymous, spent by whoever holds the numbers	Very hard. Contact the card company at once, but recovery is rare.	“Pay the tax / bail / fee with gift cards.”
Cryptocurrency (ATM or app)	Fast, irreversible, hard to trace to a person	Very hard. Transfers generally cannot be reversed.	“Deposit cash into this Bitcoin machine to secure your account.”
Wire transfer / international transfer	Large amounts move quickly; recipient may be abroad	Hard. Ask the bank to recall it immediately — hours matter.	Fake invoice; “safe account”; romance or investment “platform”.
Cash, courier or in-person pick-up	No paper trail; scammer may send a driver or “agent”	Very hard once handed over.	“A courier will collect the cash to keep it safe.”
Person-to-person apps and e-transfers (Interac e-Transfer, Zelle, Venmo, Cash App)	Instant and often irreversible when you send willingly	Often hard. Provider support varies — report immediately.	“Send it to me and I’ll refund the overpayment.”
Cheque / bank draft / “overpayment”	Funds can show as available before the cheque is found to be fake	Not recoverable from the bank if you spent real money.	“I paid too much — please send back the difference.”
Credit card (to a business you chose)	Not preferred by scammers — more protections	Often better. Dispute rights apply to unauthorized or defective charges.	Fake sites can still steal card details — type the address yourself.
Anything they chose, with pressure to hurry	Pressure and secrecy are the tactics, not the payment type	Varies	Urgent + secret + unusual = STOP.

Rule of thumb: If a stranger or an unexpected caller tells you *how* to pay, that is a red flag by itself.

© 2026 Cogitent Press. All rights reserved. Educational use only; not legal or financial advice.