# Forwards or Backwards

https://forwardorbackwards.com




# Scams and Social Engineering: Tricks and Manipulation

**Watch on YouTube:** https://www.youtube.com/watch?v=lVfSyPzOZUc

A scam is not a technical trick against a computer. It is a very old confidence trick, aimed at a person, now sent to millions of targets at once because sending it costs almost nothing - so even a response rate near zero still pays.

This video explains what a scam and a fraud actually are, and what social engineering means: hacking the person in front of the screen using trust, urgency and fear, rather than hacking the machine behind it. It traces the trick back to the 1840s American 'confidence man', then forward to America Online in the 1990s, where a Usenet post about stealing AOL passwords gave the internet the word 'phishing' in January 1996.

It shows how scammers borrow the trust already built into familiar brands - Microsoft was the most impersonated brand in phishing attempts in both the Q4 2025 and Q2 2026 Check Point Brand Phishing Reports, named in roughly one in five attempts each time - and how they hook targets with money (a prize, an inheritance, a large payment) or with fear (a fake tax, court or bank warning).

The video sets out the actual scale: US reported fraud losses reached $20.9 billion in 2025, up 26% on 2024, according to the FBI's Internet Crime Complaint Center; Americans aged 60 and over alone reported $7.7 billion of that, roughly 60% higher than 2024. Imposter scams were the single most-reported US fraud category for a fifth straight year, with $3.5 billion in reported losses and a $700 median loss among those who lost money, per the FTC.

It then walks through the three channels in turn - phishing by email, smishing by text, vishing by phone - showing what a real fake-brand email, a fake delivery text and a fake bank call actually look like, including the newest twist: an AI-cloned voice, built from as little as three seconds of real audio to roughly 85% accuracy, per McAfee research.

It ends with the checklist every version shares - unexpected contact, urgency, a request for money or a code, a mismatched link - and the practical response: don't click, verify through a number you already trust, and report it.

Educational documentary. Not financial or investment advice.

## Chapters

1. What a scam actually is
2. What social engineering means
3. Where the con began
4. Borrowing a brand's trust
5. Money as the hook
6. Fear and urgency as the lever
7. Why they send millions
8. Phishing: the email con
9. Smishing: the text con
10. Vishing: the phone con
11. How to spot any version
12. What to do when it lands

## 1. What a scam actually is



A scam is a trick. Someone convinces you to hand over money, or access to your accounts, by lying to you — not by breaking in, and not by force. Fraud is the legal word for the same thing: getting money or property from someone through deliberate deception.

The difference from theft is the handshake. A thief takes something without your consent. A scammer gets your consent — but only because you were lied to first. You handed over the money, the password, or the code yourself, believing a story that was not true.

That single fact, that the victim acts willingly, is why a scam is so hard to stop with a lock or a firewall. The weak point a scammer is aiming at is a decision, not a door.

Every scam in this video follows the same three-step shape. First, a lie designed to be believed. Second, a reason to act now, before you can check it. Third, a way to move your money or your access out of your hands. Everything from here is a variation on those three steps.

## 2. What social engineering means



The term for tricking a person this way is social engineering. It means hacking the person in front of the screen, not the computer behind it.

Social engineering works on three levers: trust, urgency and fear. Trust makes you believe a message really is from your bank, or Microsoft, or a courier. Urgency stops you pausing to check. Fear pushes you to act before you think it through. A scammer only needs one of the three to land.

No password strength and no antivirus software blocks a lever like that, because none of them touches how a person reads a message under pressure. The computer can be perfectly secure, and the person using it can still be talked out of their money.

Put trust, urgency and fear together and they point the same way: toward a decision made too fast to check. That single mechanism sits behind every version of the con this video covers.

## 3. Where the con began






None of this is new. Confidence tricks, persuading a stranger to hand over money by winning their trust first, go back at least to the eighteen-forties, when American newspapers coined the term "confidence man" for a swindler who simply asked strangers to trust him with their watch or their cash.

That old trick has moved through distinct ages. The eighteen-forties gave English the phrase "confidence man." The nineteen-nineties gave the internet the word "phishing," born out of America Online. More recently, scammers have added a new twist: cloning a real person's voice with artificial intelligence, which chapter ten covers in full.

America Online is where the online story really starts, because it was the biggest way ordinary people reached the internet in the mid-1990s.

These are AOL's own promotional CD-ROMs from that era, the free discs the company mailed out by the millions to get people online. In January 1996, a Usenet post about stealing AOL passwords used the word "phishing" for the first time on record, spelled with "ph" the way earlier hackers had spelled "phone." AOL had just blocked one trick, fake, randomly generated credit card numbers, so scammers switched to a new one: posing as AOL staff and simply asking users for their password directly.

## 4. Borrowing a brand's trust



Scammers rarely invent a story from nothing. They borrow trust that already exists, by pretending to be a brand you already believe.

Researchers who track fake login pages and phishing emails rank the brands criminals copy most often. Microsoft topped that list in two successive reports checked for this video, named in about one in five phishing attempts each time. Google, Amazon, Apple and the big banks fill out most of the rest.

The trick works because of a habit, not a mistake. You already trust Microsoft's logo, or your bank's own colours, so a scammer who copies them borrows years of trust built by someone else, inside a single email.

## 5. Money as the hook






However a scam arrives, the reason you keep reading is almost always money.

This is a real advance-fee scam letter, the paper ancestor of the emails and texts the rest of this video covers. Investigators call this pattern a "419" scam.

It takes its name from the section of Nigeria's criminal code that covers fraud, because so many early versions were traced there. This particular letter was posted from Spain to a real recipient, proof the trick travels wherever a stamp can reach.

There are three baits scammers use again and again, and this letter is one of them.

The first is a prize: you've won a lottery, a gift card, a free phone. The second is an inheritance — a stranger, often posing as a lawyer, says you're owed a fortune you never knew about, exactly what this letter claims. The third is a payment: a message claiming you were charged a large amount, with a link to "dispute" it.

Every one of those three baits ends the same way. To collect the prize, the inheritance or the refund, you are told to pay a small fee first. That fee is the actual scam. The prize was never real.

## 6. Fear and urgency as the lever





Money as a carrot is one lever. The flip side is fear: a warning designed to make you act before you can think.

This is the headquarters of the US Federal Trade Commission, the agency that tracks reports like these. It counts a whole category built entirely on fear: imposter scams, where someone poses as your bank, a court, or a tax office, warning that you owe money, face arrest, or missed a deadline.

Imposter scams were the single most-reported kind of fraud in the United States for a fifth year running in 2025, with $3.5 billion in reported losses. Among the people who actually lost money, the typical loss was $700, though the Commission says some people lost far more than that.

A tax warning, a court summons, a bank fraud alert: the content changes, but the goal is always the same. Adrenaline first, verification never.

## 7. Why they send millions





If a scam message is obviously fake, why do scammers still send millions of them?

This is FBI headquarters in Washington, home of the agency's Internet Crime Complaint Center, which tracks reported losses across the whole country. Its own numbers make the logic plain: the response rate on a single scam message can be tiny, and the campaign can still be enormously profitable, because sending another million messages costs almost nothing.

Picture a scammer sending one million messages at once. Almost all are deleted, ignored or reported. But even a response measured in a fraction of one per cent still means hundreds of replies, and each of those replies can be worth thousands of dollars.

That arithmetic is why the messages do not need to convince everyone. They only need to convince the small number of people who, that day, are tired, distracted, or already anxious about money.

Reported fraud losses reached $20.9 billion in 2025, up 26% on the year before. More than a million complaints fed into that total. Americans aged 60 and over alone reported $7.7 billion of it, roughly 60% higher than 2024, the age group scammers target hardest.

## 8. Phishing: the email con



The oldest of these three channels is email. This is phishing: a fake message, sent by email, pretending to come from a real bank, company or government agency, built to get you to click a link or hand over details.

A real phishing email usually gets small things wrong even when the logo is perfect: a sender address close to the genuine one but not quite right, a generic "Dear Customer" instead of your name, and a link that leads somewhere other than where it claims.

Four tells to check, every time. The sender's actual email address, not just the display name. Where a link truly points, seen by hovering over it rather than tapping it. Poor spelling or an odd tone. And any request to "verify" a password or card number by clicking straight through.

## 9. Smishing: the text con



The same trick sent by text message has its own name: smishing, from "SMS" and "phishing." It is now one of the fastest-growing versions of the con, because almost everyone opens a text within minutes of it arriving.

The most common smishing texts pose as a delivery courier with a "missed parcel" fee to pay, a road toll left unpaid, or a bank warning of suspicious activity, each one built around a link that looks almost right.

Two extra tricks show up here more than anywhere else. A shortened link hides the real web address behind a short code, so you cannot see where it actually leads. A QR code, printed on a fake parking ticket or poster, does exactly the same hiding job with a picture instead of text.

## 10. Vishing: the phone con



The phone version of this con is called vishing, short for "voice phishing." A caller claims to be your bank's fraud team, or tech support from a company like Microsoft, and talks you through "fixing" a problem that never existed.

The newest and most alarming version uses artificial intelligence to clone a real person's voice. Researchers at the security firm McAfee found that just three seconds of someone's voice, taken from a video or a voicemail, is enough to build a clone that matches the real voice about 85% of the time.

That means a scammer no longer needs to sound like your bank. A call can be made to sound like your own child asking for emergency money, cloned from a clip posted online.

Whether the voice is real or cloned, vishing depends on the same rule as every other version here. A genuine bank or tech company will never ask you to move money, or read out a one-time code, over a call you did not start yourself.

## 11. How to spot any version



Strip away the channel, email, text or phone call, and every scam in this video shares the same four warning signs.

Unexpected contact you did not ask for. Pressure to act immediately, before you can check. A request for money, a gift card, or a one-time code. And a link or number that does not quite match the real organisation's own details. Any one of those four is a reason to stop.

## 12. What to do when it lands



If a message like this reaches you, the response is the same every time, whatever channel it arrived on.

Don't click the link, and don't call the number in the message. Instead, look up the real organisation yourself, your bank's number on the back of your card, or the company's official website, and check directly through that.

If you do lose money, or come close to it, report it. In the United States, that means the FBI's Internet Crime Complaint Center or the FTC; in the UK, Action Fraud. Reporting does not just help you. It is also how the figures in this video get counted in the first place.

None of this depends on being an expert with computers. A scam is a very old trick, and every version of it, by email, by text or by phone, is still just someone asking you to trust them with something valuable, faster than you can check. Slow down, verify through a number you already know, and the trick stops working, no matter which channel it arrives on.

# Sources and credits

## Primary sources

- FBI Internet Crime Complaint Center (IC3), 2025 Internet Crime Report, published 2026 - $20.9bn (1,008,597 complaints, up 26% on 2024) total US reported fraud losses, and $7.7bn / ~60% increase for the 60+ age group.
- US Federal Trade Commission, press release 'FTC Data Show People Reported Losing $3.5 Billion to Imposter Scams', published 15 June 2026 - $3.5bn imposter-scam losses, fifth straight year as the top category.
- FTC Consumer Sentinel Network data spotlight, June 2026, as reported 26 June 2026 - the $700 median loss among imposter-scam victims who lost money.
- Check Point Research, Brand Phishing Report, Q4 2025 and Q2 2026 editions - Microsoft as most-impersonated brand, 22% and 23% of brand-phishing attempts respectively.
- UK Office for National Statistics, 'Nature of fraud and computer misuse in England and Wales', year ending March 2025.
- Kaseya, 'The History of Phishing', 2025 - the AOL/AOHell account of the word's coining; does not itself give an exact day, which is why the video states only 'January 1996'.
- deepstrike.io, 'Vishing Statistics 2025', citing McAfee voice-cloning research - three seconds of audio producing a voice clone matching the real voice at about 85% accuracy.

## Photo credits (Wikimedia Commons)

- FBI headquarters (J. Edgar Hoover Building), Washington D.C. - source of the IC3 fraud-loss figures: Carol M. Highsmith, Public domain - https://commons.wikimedia.org/wiki/File%3AFBI_Headquarters_Building%2C_Washington%2C_D.C_LCCN2013634629.tif
- Federal Trade Commission headquarters (Apex Building), Washington D.C. - source of the imposter-scam loss figures: Harris & Ewing, photographer, Public domain - https://commons.wikimedia.org/wiki/File%3AExterior_of_the_Apex_building%2C_new_home_of_the_Federal_Trade_Commission_LCCN2016872023.jpg
- Real Nigerian 419 advance-fee scam letter/envelope sent from Spain to a victim: XxDestinyxX, Public domain - https://commons.wikimedia.org/wiki/File%3ANigerian_419_scam_envelope_from_Spain.jpg
- AOL promotional CD-ROMs, late 1990s/early 2000s - the AOL era where the word 'phishing' was coined: Jeran Renz (talk), CC0 - https://commons.wikimedia.org/wiki/File%3AAOL_promotional_CDs_in_Canada.jpg

Not regulated financial advice.