

How to Spot a Scam

A five-minute training for adults on how phone, text, and online scams work and what you can do to protect yourself.

What social engineering means

Social engineering is when a criminal tricks a person into giving up money, information, or access, instead of breaking in through technology.

It works by taking advantage of normal reactions, like wanting to help someone or worrying about your money.

Every scam in this training is a form of social engineering.

How much is being lost to scams

\$11.4 billion

reported lost to fraud by Americans aged 50 and over in 2025, more than half of all losses reported to the FBI that year.

Source: FBI Internet Crime Complaint Center, 2025 Internet Crime Report, pages 6 and 44.

ic3.gov/AnnualReport/Reports/2025_IC3Report.pdf

Scams today are run by organized groups who do this as a full-time job.

Falling for one does not mean you were careless. It happens to people of every age and profession.

Warning signs of a scam

Unexpected Problem

Any call, text, email, or pop-up that you did not ask for, about a problem you did not know you had.

Pressure

You are told that you must do something in the next few minutes or face sudden negative consequences.

Secrecy

You are asked not to consult a friend or trusted contact before continuing the call.

Sensitive Information

You are asked for a password, a security code, gift cards, money, or personal information.

How a fake call might sound

WHAT THE CALLER MIGHT SAY

WARNING SIGN TO SPOT

- | | | |
|---|---|--|
| 1 | <i>“This is the fraud department at your bank. We saw a suspicious charge on your account.”</i> | This is the Unexpected Problem warning sign. |
| 2 | <i>“We must act quickly to prevent further charges from hitting your account.”</i> | This is the Pressure warning sign. |
| 3 | <i>“To verify your identity, I need your username and password.”</i> | This is the Sensitive Information warning sign. |
| 4 | <i>“Do not hang up or ask anyone else for assistance with this.”</i> | This is the Secrecy warning sign. |



THE MOST IMPORTANT POINT

No one should call you to ask for your password, your PIN, or a code that was sent to your phone.

The same is true for banks, law enforcement, hospitals, Medicare, Social Security, the IRS, or any company you do business with. If a caller asks for one of these, treat the call as a scam and hang up.

How to check whether a call is real

1

End the call

You do not need to explain yourself or be polite about it. A person calling for legitimate reasons will understand.

2

Verify the number

Find a saved contact, a support number on a company website, or any other trusted location where you find the number yourself.

3

Call trusted number

Tell them you received a call from an unknown number claiming to be them. If it was legitimate, no harm no foul.

The same steps work when the caller says they are from Medicare, Social Security, the IRS, a utility, or a technology company like Microsoft or Apple.

Other scams to know about

Tech support pop-ups

A warning on your screen tells you to call a number. Turn the computer off and back on, and never let a caller connect to it.

Delivery and toll texts

A text says you missed a package or owe a toll. Do not use the link, and check through the company's own app or website.

Family emergency calls

A caller sounds like a relative who urgently needs money. Voices can now be copied, so hang up and call them yourself.

Romance and investments

A person you only know online asks for money or recommends an investment. Do not send money to someone you have not met.

Habits that lower your risk

- 1 Let calls from unknown numbers go to voicemail.** A real caller will leave a message, and you can call back on a number you trust.
 - 2 Use a different password for each important account.** A password app or a notebook that stays at home can help you keep track.
 - 3 Turn on two-step verification for your important accounts.** Do not share the codes it sends with anyone.
 - 4 Install updates on your phone and computer when they are offered.** Updates fix the weaknesses that criminals take advantage of.
-

What to do if it happens to you

- 1 Stop all contact.** Hang up, stop replying, and do not send any more information.
 - 2 Call the company involved right away.** Use a number you look up yourself, and let them know what happened.
 - 3 Secure your accounts.** Change any password you shared, and have your computer checked by a trusted contact.
 - 4 Report it and get free help.** Report it at ReportFraud.ftc.gov, or call the AARP Fraud Watch Network Helpline at 877-908-3360.
-

Do not be embarrassed to speak up.

SUMMARY

What to remember

01

Be suspicious of any unexpected call, text, or email that pushes you to act quickly.

02

If you are unsure, hang up and call back at a number you found yourself.

03

Do not share passwords, PINs, or security codes with anyone who contacts you.

If you have any further questions, feel free to reach out at **tbrucker@bruckercyber.com**.