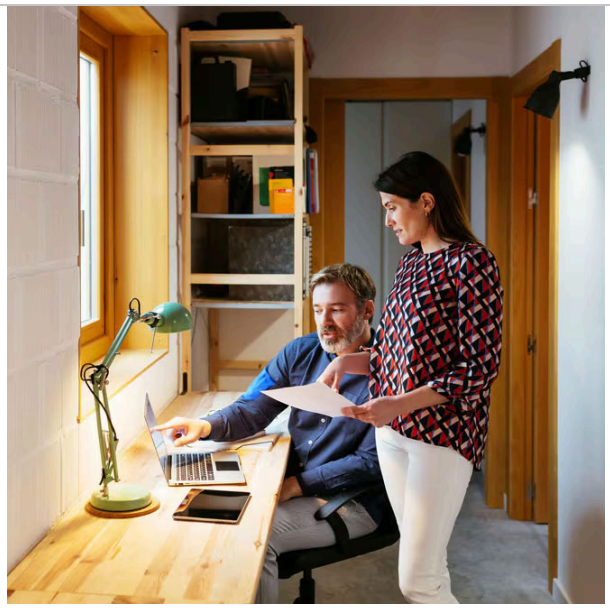
CHASE

Sign in



SECURITY CENTER

Scam Watch: How to spot fraud and scams

Scammers may be sophisticated, but working together, we can help stay ahead of them.

Spot scams

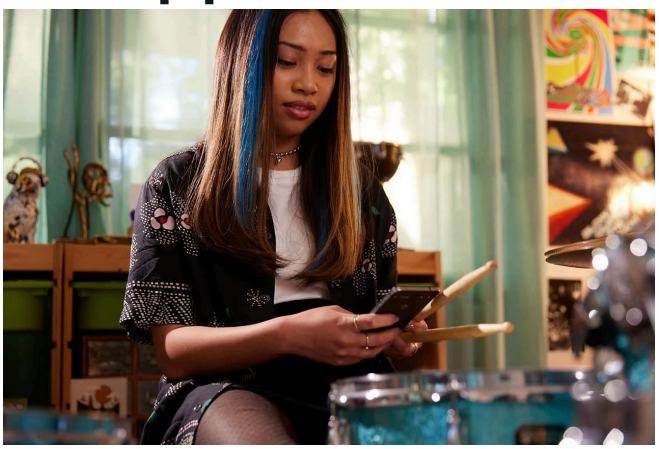
Know what's happening: Scammers are getting more resourceful and convincing every day

Social media marketplace scam

The 'great sale on your favorite brand' scam

Scammers create ads on social media offering merchandise at great prices and set up bogus websites that all look exactly like genuine retailers. They'll collect personal information or ask you to pay with a digital payment platform like Zelle® when you go to "check out".

How it can happen:



I was scrolling on social and saw a sale ad for one of my favorite brands. It looked just like other ads I'd bought from before. The discount was really good, so I clicked on it and went to what looked exactly like their website, even with the free shipping headline.

When I went to check out, I thought it was odd I couldn't find a place for my credit card, just options for digital payment platforms like Zelle®. But I thought no big deal and paid with Zelle®. I got suspicious when I didn't get a confirmation email right away like I usually do. I waited about three weeks, but the merchandise never showed up. I tried to put in a claim for fraud with my bank, but I was told there's no way to get my money back.

Help protect yourself

Always type in a company's website address yourself to see if special sales or promo codes are listed there. If not, the ad you're seeing and the website it's taking you to are likely a scam. **Where possible use your**

credit or debit card which offers protection features that may not be there if you pay by other means.

Tech support scam

Watch out for the latest tech support and computer virus scams

Scammers pretend to be tech support from a well-known company. They either call, text or try to trick you into clicking on a link in an email, text or pop-up window, claiming there's a problem with your computer like a virus or a billing issue. To fix it, you inadvertently give them remote access to your computer.

How it can happen:

I got a giant yellow "alert" that covered my computer screen, saying my computer had been hacked. My cursor was even moving on its own, so something definitely seemed wrong. Another alert appeared that looked legitimately from the same brand as my computer, telling me to call the tech support line.

The man who answered was very professional and said they'd been seeing this attack happening a lot lately. He had me go to a website that had all sorts of cyber security

information on it and click on a link. He said it would let him see my screen to gauge how bad the attack was. He had me sign into some unimportant websites like a movie site and my pet store. He said everything looked fine, but I should sign into my bank account to also check it. He said he couldn't see my password as it showed up with just those dots in the password field. I told him there were no unusual transactions on my account, so he said it looked like it was all a false alarm and hung up.

Little did I know, that when I gave him remote access to my computer, he was able to see everything I typed. The scammers later signed into my bank account and transferred thousands out.

Help protect yourself

Scammers know "virus alerts" immediately put computer users into a panic. **Never click on virus alerts, even if they look like they come from your computer company or an anti-virus protection company.** If you think your computer was impacted, talk to a reputable service provider.

Scam alert: Check fraud

Be careful when writing or depositing checks

Checks you write

Scammers can steal checks from mailboxes or ones not properly destroyed after being deposited. They can then use chemicals to erase and rewrite the checks to themselves or may use your personal information, like name, address or account number, to sell your info or create counterfeit checks.

Follow these check-writing tips:

1. Use permanent ink so it's harder to erase.
2. Don't leave empty space before the payee or dollar amount.
3. Draw a line through the extra spaces.
4. Sign the same way every time.

Tips:

- Mail checks from inside the post office.
- Keep documents safe.
- Review statements regularly.
- Monitor your accounts and verify the payee and check amounts.

- Consider alternative payment methods like Chase Online℠ Bill Pay, Zelle®, or your Chase debit card.

Checks you deposit

Fake or stolen checks are often used in scams where someone might try to trick you into cashing or depositing the check. After you've deposited it, they might ask you to send some or all of the money back to them. This usually happens before the bank has a chance to process the check and discover that it's not real — which can take weeks. If you've spent the money, you may also be held accountable for the money lost if the check turns out to be fake.

Be on alert for check deposit scams like these

The Fake Job Scam

Scammers post fake job ads online, send you a "paycheck," then claim they overpaid and ask you to return

The Mystery Shopper Scam

Scammers pose as a mystery shopping company, send you a fake check, and tell

part of it. Later, your bank says the check was fake, leaving you out the money you sent plus the bounced check amount.

you to buy gift cards as part of your first "shopping assignment." Before you shop, they ask for the card numbers, spend the funds, and when the check they originally sent you bounces, you're out the gift card money too.

The Overpayment Scam

A buyer "accidentally" overpays, asks you to refund the extra, then the original check bounces. You lose both the item and the money you sent back.

The Lottery / Sweepstakes Scam

You're told you've won a prize and receive a fake check. Scammers then ask for "fees" or "taxes." By the time you find out the check bounces, they already have your money.

Tips:

- **Don't use the funds immediately,** especially if the check is from someone you don't know. It can take weeks for a bank to identify that the check was fake or if there were insufficient funds in the account to cover it.

- **Be aware that fake checks can look very real.** Scammers use advanced technology to produce counterfeit checks that closely resemble authentic ones.
- **Be extra alert if someone claims to have overpaid.** Scammers issue checks for a higher amount to trick you into returning the extra money.
- **Ask to be paid with digital payments instead of checks.** Consider convenient, fast and secure options like Chase Online℠ Bill Pay or Zelle®.

Scam alert: Gift cards

If you're told to pay with a gift card, stop and think, it might be a scam

Anytime someone says you need to pay with a gift card, it's most likely a scam. Be aware that if you buy gift cards and give the scammer the gift card codes, it's very unlikely you'll get your money back.

A common scam is the "Mystery Shopper Scam"

Scammers "hire" you as a mystery shopper and send you a check to cover your assignment. You're told to buy gift cards and give them the numbers — but the check you deposited is fake, and they drain the cards. You're left covering the cost.

Think twice before choosing gift cards as a payment method:

1. **Do not** buy gift cards for anyone who asks for them through phone, text, or email, especially if they're threatening you. It's most likely a scam.

2. **Do not** give the gift card number or the 3 or 4 digit security code under the scratch off section to anyone.

3. **Do not** send a picture of the gift card number or security code to anyone.

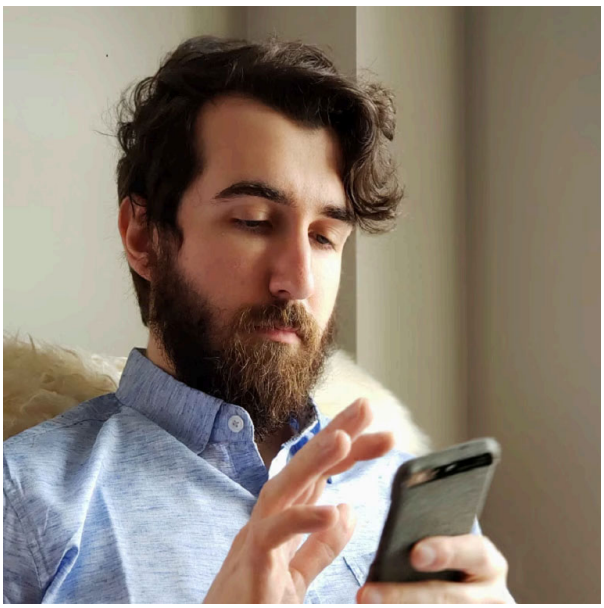
Tip: If you're asked to buy a gift card to pay for goods or services, it's a scam warning flag.

Watch out for charity scams

What's happening?

Scammers come out of the woodwork to prey on people who are looking to help relief efforts when disaster strikes.

Charity scams can appear as fraudulent websites, phishing emails, text messages, crowdfunding sites, phone calls, and postal mail. Being informed is key to protecting your donations. Tactics scammers use are:



- **Impersonation:** They mimic established charities or create new ones with similar names
- **Emotional appeals:** They use heart-wrenching stories and pictures
- **Technology:** They create and share links to websites that look like they're legitimate charities

Tips to help you stay safe:

- **Verify the charity:** Check the legitimacy of the charity and access their official website through CharityWatch or the BBB Wise Giving Alliance
- **Be cautious of unsolicited calls or texts:** If a charity reaches out unexpectedly, say you'll call back using the number listed in the CharityWatch or the BBB Wise Giving Alliance

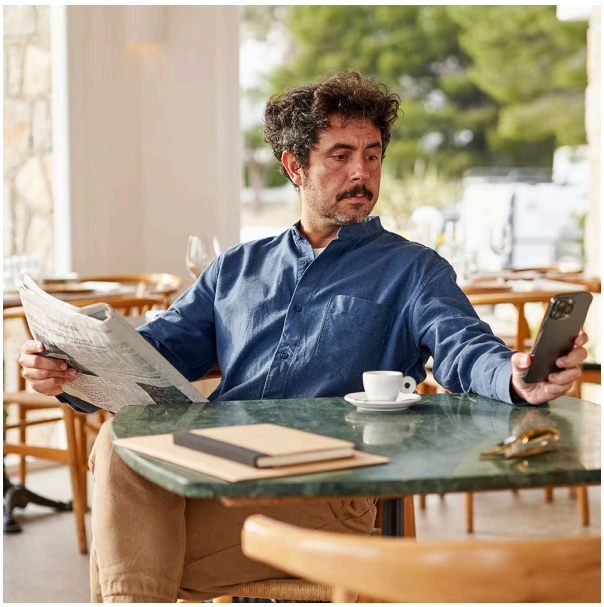
Scams can happen to anyone

Watch how scammers are using technology to target younger people

- Get helpful tips for how to protect yourself
- See how tools from Chase can help safeguard your money

Knowing about scammers' tricks can help you stay one step ahead of them

Here are some of the latest schemes to avoid:



Watch out for scammers impersonating banks

What's happening?

A scammer calls or texts pretending to be from Chase and says you need to send money to another account using a wire transfer. They may claim it’s to reverse fraud on your account. Don’t fall for it – it’s a scam!

We will never ask you to send money to yourself.

Tips to help you stay safe:

- Know who you're talking to: You can verify that you're speaking with us by hanging up and calling the number on the back of your Chase card or your account statement.
- Take a moment: Think about what they're asking for, and verify they are who they say they are, especially if it feels urgent or pressured — it could be a scam.
- Be careful when sending money: It's important to verify you're not sending money to a scammer. Once you send money you may not be able to get it back.

Keep tabs on common scams

To help protect yourself, always be suspicious of calls, emails, texts or any communication you receive from someone you don't know — particularly if they want money or your personal information. See below for examples of common scams and tips to be more secure.

For sale, hot deal

"Get a great price on these exclusive sneakers. You can pay using cash or a payment app."

TIP: Be wary of great "deals" on social

Someone you 'know'

"I'm with the IRS, and you owe back taxes. If not paid immediately, a lawsuit will be filed against you."

'Accidental' payment

"I didn't mean to send you that money! Please send it back to me right away."

TIP: Never return any unexpected funds

media sites. Once you send money you may not get it back.

TIP: Be cautious if you're told to take action right away. Think about what they're asking for and verify that they are who they say they are.

without calling Chase first.

Romance

"I'm having a medical emergency and need money. I promise to pay it back quickly. Can you help?"

TIP: Don't send money to anyone you've only spoken to online or by phone.

Computer virus

"We've detected malware on your computer. Give me access remotely so I can fix that for you."

TIP: Never give anyone remote access to your computer unless you can 100% verify who they are.

ATM withdrawals

"Hey, don't forget to use the tap feature on the ATM. I can show you how it works."

TIP: Don't accept help from strangers at the ATM. Pay attention to your surroundings and watch out for people looking at your screen.

You've won!

"Congratulations! You've won the lottery! We will need to collect taxes prior to your payment."

TIP: Do not send money to claim a prize. Chances are it's a scam.

Home closing

"These are the wire instructions to close on your house."

TIP: Be very cautious of last-minute changes to payment instruction and call your agent or loan officer directly to verify wire instructions before you send money.

Investment

"You've registered to receive notifications on investment opportunities. Are you ready to invest? I have a once-in-a-lifetime opportunity!"

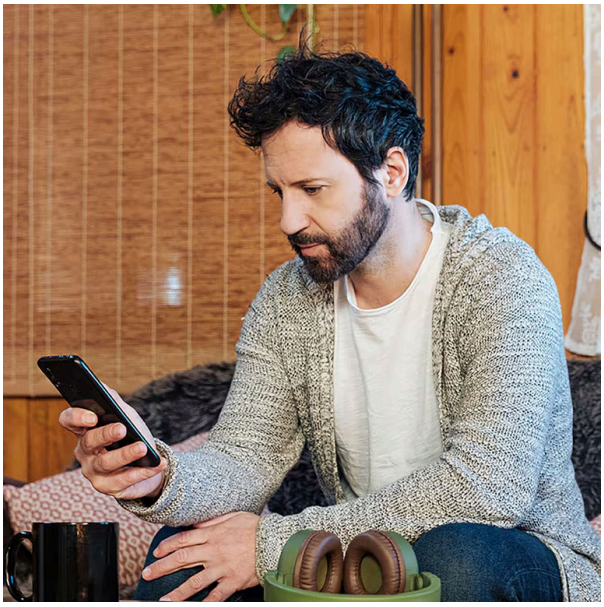
TIP: Research the person or company you're dealing with, and make sure they're legitimate.

Learn to recognize 'spoofing' and 'phishing'

Scammers will try to trick you into giving them your passwords, Social Security number or other sensitive information to get access to your accounts or steal your identity.

They could do this through a call, email, text or fake websites. Learn more about their methods and how to protect yourself.

Spoofing: Look out for scammers in disguise



Scammers can "spoof" phone numbers. The caller ID can say the call or text is from Chase even though it's not. They do this to trick people into providing their personal or financial information or to get you to send money.

Remember:
Even if your caller ID says a call or text is from Chase, it could be a scam. When in doubt hang up and call us directly.

Learn how to identify Chase texts >

Phishing: Watch out for suspicious calls, emails and texts

"Phishing" is when you get an email that looks reputable but asks you to call a fraudulent number, respond to the email or go to a website and enter personal information. You may be asked to look at an attachment, which then gives bad actors access to your computer if you open it.

Remember:
Suspicious messages may have typos or grammatical mistakes. Don't click on links or attachments in an email if you're not sure who it's from.

You can report a suspicious email to us by reporting it to phishing@chase.com.

You may also want to report suspicious calls, emails, and text messages by visiting, https://ReportFraud.ftc.gov.

Learn how to spot them

Think you've been the victim of identity theft?

It is important to take action quickly. Read our guide to take your first steps toward recovering your identity.

Continue to PDF >

Contact us to report fraud

If you see an unauthorized charge or believe your account was compromised, let us know right away. Learn what to do and how to contact us.

Get in touch

Frequently asked questions

- I've reported the fraud. Now what?
- What do I do if I've responded to a phishing attempt?
- Does Chase Bank buy or exchange Iraqi dinar (IQD) currency?
- Can Chase get back money I've sent to a scammer?
- What is identity theft?