Scam, Scams and More Scams

From a Capital One email

1

Payment scams

Be wary if you are urged to make a purchase with the promise of compensation, or if someone offers to make a payment for you, or provides you with bank account info with which to make a payment.

If something sounds too good to be true, it probably is. If you use a payment method you are not familiar with, you run the risk of ultimately being held responsible for the amount paid.

2

Tech support scams

Tech support claims your computer has malware and requests payment to fix the defects or access your computer.

3

Employment scams

Be vigilant in validating employment opportunities, especially when exclusively online or working from home.

Be suspicious if someone claims to have overpaid you for a job, promises to reimburse for equipment, or asks you to send equipment to an IT dept. The equipment may never be returned, and reimbursements or overpayments may be illegitimate, leaving you liable for the funds.

Never divulge personal information online to an unreliable source or through deceptive job

4

Impersonation scams

Scammers pose as a legitimate company (like Capital One) or a utility company and request personal information or a payment transfer in order to make things "right" on your account.

They might also use a fake caller ID that could show up as a legit company's number and/ or request remote access to your device.

Scammer posing as a utility company might warn you to pay your balance within a limited time or else the utility will be shut off.

5

Fake rental

A house is legitimately listed for sale online, but scammers have set up a fake website and listed the house as a rental. You send your first month’s deposit to a scammer pretending to be the landlord/owner.

6

QR code scams

When scanning QR codes, use your smartphone's default camera app to avoid scams and potential fraud.

Scammers use 3rd party QR code scanner apps and/or the ads within the apps to direct users to fake or malicious websites designed to obtain your personal information.

7

Fake websites

Legitimate-looking websites are being created by scammers, and a quick Google search will lead you to a real-looking phone number.

When you call, they'll try to obtain your sign-in details or other information.

8

Overpayment scams

You receive an overpayment for an item you're selling, immediately followed by a request to deposit the check (which turns out to be a bad check) and then send the difference via a wire or gift card.

9

Check cashing

You're approached outside a bank branch and asked to cash a check for someone who claims they don't have an account or left their ID home.

The bad check will be held against your account when it doesn't clear.

10

Romance scams

If you are asked for financial support from a new partner in a relationship that’s been exclusively online, you’re likely a target of this elaborate scheme.

11

Charity scams

You receive a request to donate to a charity that you've never heard of and for which you can’t find an official website.

12

Debt relief

You receive a request for payment in order to establish a service relationship to pay, settle or get rid of debt.

13

FTC / IRS scams

Scam artists are pretending to be IRS officials to get your money. They'll call, email, or text you claiming you owe back taxes or there's a problem with your tax return.

They even rig caller ID to make their call look official.

They play on your fears.

14

Investment scams

You receive a request to invest in a business opportunity with promises of high returns and/or getting rich quickly.

15

Lottery scams

You receive a request to prepay fees or taxes in order to receive a large prize you supposedly won.

16

Grandparent scam

You receive a call or text message from someone claiming to be a grandchild or loved one asking for money to help with an emergency, plus instructions on where to send the funds.

17

Puppy scam

Scammers post fake litters online or pretend to be someone they're not (usually an existing breeder) to take advantage of puppy sales.

18

Online Merchant/Marketplace Scams

When responding to ads or interacting in marketplaces on social media, research sellers and products independently to ensure legitimacy.

Notice the red flags like a high-ticket item for a price too-good-to-be-true or a buyer who “accidentally” overpaid you for an item or someone asking for personal information or redirecting to an unfamiliar/strange looking URL.

19

Mortgage closing

You receive an email or text message that looks similar to your real estate agent’s contact info that indicates there is a last minute change to the wiring instructions, and tells you to wire closing costs to a different account.

20

Business email compromise scams

You receive an email from your supplier/vendor requesting to send money to a different account. The supplier/vendor email appears to be familiar. But this could be a fraudster who obtained access to the network of your supplier/vendor.

21

Suspect you've been a victim of a scam?

Here's what you do.

- Contact us (CapitalOne) at 1-800-227-4825. If you are outside the U.S., call us collect at: 1-804-934-2001.
- Forward the email or text to Abuse@capitalone.com so we can look into it on our end.
- Report the scam to the BBB Scam Tracker and the government via the FTC ReportFraud site. You may also want to report scammers directly to the FBI.

22

AVOID SCAMS AND SAFEGUARD YOUR FINANCES

When in doubt, hang up the phone and call the number listed on the back of your debit or credit card.

Fraudsters will try to spoof the number calling you to appear as if it is coming from Capital One.

If it sounds too good to be true, it probably is.

Be wary of "get rich quick" or "easy money" schemes, especially if unsolicited.

Verify SMS text or email origins.

Scammers may target you with text messages to gain sensitive information. Verify the SMS texts or emails are coming from the usual Capital One email domain and short code (a 5 or 6 digit phone number that is used to send text messages at scale).

23

Resist the pressure to act immediately.

While high-pressure sales tactics are also used by some legitimate businesses, it typically isn't a good idea to make important financial decisions quickly. Take your time. Where your finances are concerned, you should have space to make the best decision for you and talk it over with those you trust.

Use extreme caution when dealing with anyone you've met online.

Scammers use dating websites, social media and many other sites to reach potential targets. They can quickly feel like a friend or even a romantic partner, but that is part of the con for you to trust them.

Make sure your transactions are traceable and secure.

Do not pay by wire transfer, prepaid money card, gift card or any other non-traditional payment method. Say no to cash-only deals, high pressure sales tactics, high upfront payments, overpayments or handshake deals without a contract. Read all of the small print on the contract and understand the terms before you buy.

The End

24