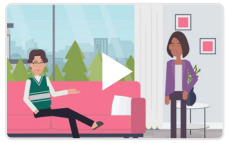
Avoid scams that pose as a financial institution

- **A text asking you for details to "confirm" it's you.** Your financial institution may well text you – for instance to confirm a transaction on PC – but financial institution texts will not, ever, ask you to confirm details or for passwords in a text. financial institutions also won't update their apps in this way. If you're suspicious, don't click links, and don't call any numbers in the text. Instead, call your financial institution on its "normal" number – Google it if you don't know – and check whether the text is from them.
- **Fake fraud alert scam.** The scheme tries to scare you into believing the scammers are representatives of your financial institution. The scammers will tell you that a fraudulent charge was made to your bank account through a digital instant payment app.
- **Give you a deadline of 24 hours before your financial institution account erases itself.** Many legitimate messages from your financial institution will be marked "urgent" – particularly those related to suspected fraud – but any message with a deadline should be treated with extreme suspicion. Cybercriminals have to work fast – their websites may be flagged, blocked, or closed down rapidly – and need you to click without thinking. financial institutions just want you to get in touch – they won't usually set a deadline.
- **Send you a link with a "new version" of your banking app.** Your financial institution will not distribute apps in this way – instead, download from official app stores, and ensure yours is up to date.
- **Use shortened URLs in an email.** Cybercriminals use a variety of tricks to make a malicious web page appear more "real" in an email that's supposedly from your financial institution – one of the most basic is URL-shortening services. Don't ever click a shortened link, whether in an SMS or an email from your financial institution. Go to the financial institution's website instead (the usual URL you use), or call them on an official number (i.e. not the one in the email).
- **Send a courier to pick up your "faulty" financial institution card.** The courier scam is a new one – your phone rings, it's your financial institution, and they need to replace a faulty financial institution card. One of the new services they offer is courier replacement – and the financial institution tells you that a courier will arrive shortly to collect the faulty card. A courier and turns up, asks for your PIN as "confirmation" – and your money magically vanishes. If your card is

Related Topics +

Red Flags + Next Steps

Video (Click to play)



faulty, a real financial institution will instruct you to destroy it, and send you a replacement by mail.

- **Call your landline and "prove" it's the financial institution by asking you to call back.** A common new scam is a phone call from either "the police" or "your financial institution", saying that fraudulent transactions have been detected on your card. The criminals will then "prove" their identity by "hanging up" and asking you to dial the real financial institution number – but they've actually just played a dial tone, and when you dial in, you're talking to the same gang, who will then ask for credit card details and passwords.
- **Email you at a new address without warning.** If your financial institution suddenly contacts you at your work address. Financial institutions will not add new email addresses without your permission. If you want to be ultra-secure, create a special email address just for your financial institution, don't publish it anywhere, or use it for anything else – that way, emails that appear to be from your financial institution probably ARE from your financial institution. As ever, stay cautious.
- **Use an unsecured web page.** If you're on a "real" online banking page, it should display a symbol in your browser's address bar to show it's secure, such as a locked padlock or unbroken key symbol. If that symbol's missing, be very, very wary. This is one reason why it's best to browse an online banking page from your PC – on a smartphone browser, it can be more difficult to see which pages are secure.
- **Address you as "Dear customer" or dear "youremail@gmail.com".** Financial institutions will usually address you with your name and title – i.e. Mr Smith, and often add another layer of security such as quoting the last four digits of your account number, to reassure you it's a real email and not phishing. Any emails addressed to "Dear customer" or "Dear [email address]" are instantly suspicious – often automated spam sent out in vast quantities to snare the unwary.
- **Send a personal message with a blank address field.** If you receive a personal message from your financial institution, it should be addressed to you – not just in the message, but in the email header. Check that it's addressed to your email address – if it's blank, or addressed to "Customer List" or similar, be suspicious.
- **Email you asking for your mother's maiden name.** When financial institutions get in touch – for instance in a case of suspected fraud – they may ask for a password or a secret number. What they won't do is ask for a whole lot more information "to be on the safe side". If you see a form asking for a large amount of information, close the link and phone your financial institution.

Examples of how bank or credit union impersonation scams work:

Bank or Credit Union Manager & Account Breach Scam:

- **Initial Contact:** The victim receives a call from someone claiming to be the bank or credit union manager or another high-ranking banking official.
- **Fake Alert:** The "manager" claims there's been suspicious activity on the victim's account and immediate action is required.
- **Request for Verification:** The victim is asked to confirm their account details, including passwords or PINs, so that the issue can be resolved.

Bank or Credit Union Audit & Compensation Scam:

- **Initial Contact:** The victim is told they've been selected for a special audit or review, usually due to some past banking error in their favor.
- **Promise of Compensation:** The "bank or credit union manager" mentions the victim might be entitled to compensation or a refund.
- **Payment Verification:** To "verify" the compensation amount, the victim is instructed to transfer a small amount, but fraudsters use this to gain access to their account.

Loan Approval & Advance Fee Scam:

- **Initial Contact:** The victim is informed that they've been pre-approved for a large loan, despite not applying for one.
- **Upfront Payment:** The "bank or credit union manager" says an upfront fee or deposit is needed to process the loan.
- **Result:** Once the fee is paid, the fraudster disappears, and no loan is provided.

Bank or Credit Union Merger & Account Update Scam:

- **Initial Contact:** The victim receives communication that their bank or credit union is merging with another and updates are needed.
- **Account Verification:** The "bank or credit union manager" asks the victim to click on a link or provide account details to ensure the smooth transition of their account to the new system.
- **Outcome:** The link leads to a phishing site or the information given is used for unauthorized transactions.

Bank or Credit Union Manager & Charity Event Scam:

- **Initial Contact:** The victim is told about a charity event or fundraiser the bank is supposedly supporting.
- **Personal Appeal:** The "bank or credit union manager" personally requests the victim to donate, emphasizing the importance or urgency of the cause.
- **Payment Method:** The victim is given specific, often unconventional, payment methods, like wiring money or using gift cards.

Common text message impersonation scenarios:

If you get an SMS message supposedly from your financial institution about a fraud alert, be wary. The scheme tries to scare you into believing the scammers are representatives of your bank or credit union. An automated SMS message will appear on your phone, claiming to be a fraud alert from a banking institution. It'll then ask if you recently made an instant payment in the thousands of dollars.

How it happens:

- Scammers will first research your online history to learn your past addresses, Social Security numbers, the last four digits of your bank accounts or any other identifiable information about you.
- You will receive a text message that states where and when the fraud took place.
- You will be prompted to press "Y for valid" or "N if unauthorized," and then guided to add in the CVV number from your card. If you respond to any of these prompts, the scammers will then proceed to call back by spoofing the 1-800 number from your banking institution. They'll then claim they work for the financial institution's fraud department and that there is potential fraud on your debit or credit card.
- Once the trust has been established, the scammers will tell you that the fraudulent charge was made to your banking account through a digital instant payment app. These payment apps are meant for the quick transfer of funds between registered users, with only the recipient's email or mobile number needed to initiate an instant payment transaction.
- The scammers will then walk you through the various steps to reverse the payment. But in reality, the cybercriminals are trying to steal your funds.
- Using your bank or credit union's legitimate website or application, the fraudster instructs you to remove your email address from your bank's digital payment app.
- The fraudster will then ask for your email address and send it to a bank account that they control.

- You will then be told to send another payment transaction, under the belief that the charge is being reversed and that you're merely sending the money back to yourself. However, you are transferring the money to the scammers.

How to stay safe:

- Inspect the sender’s information to confirm that the message was generated from a legitimate source, but don’t click on the link or call the number on the text.
- Do not respond to the text. Even writing STOP will let the scammer know your number is genuine, and they may sell your number to other scammers, making the problem worse.
- If a call or text is received regarding possible fraud or unauthorized transfers, do not respond directly, immediately hang up, and do not enter your CVV number. Even if they have the right caller ID. Using "caller ID spoofing," scammers can make it look like they're calling from your bank's phone number.
- Remember, never click on links provided in unsolicited text messages or emails. Your financial institution will never ask for a CVV or PIN number to verify fraud. Requests to do so, as well as poor spelling or grammar, are telltale signs of a scam.
- Always verify the identity of anyone claiming to be from your financial institution. The best way to protect yourself is to say, "Let me call you right back," and then you call the official bank number yourself. A legitimate representative from your bank will never take issue with you hanging up and calling the number on the back of your debit or credit card. Use the contact details you have for your bank or credit union, not the ones provided in the unsolicited communication.
- Never answer any questions from a random call from anybody. There may be a call from someone legitimate, but more often than not it's a scammer.
- Do not post sensitive information online. The less information you post, the less data you make available to a cybercriminal for use in developing a potential attack or scam.
- Avoid sharing personal or financial information over the phone or email.
- Keep an eye out for misspelled words which are used to bypass a phone carrier’s filter system for fraud.
- Block unknown senders from your cell phone. **Learn How** (https://efraudprevention.net/home/education/index.aspx?a=302)