Click Here

You're going about your day when a text from your bank pops up: "Unusual activity detected. Click here to secure your account." It feels urgent, serious, and maybe even a little terrifying. After all, no one wants their bank account compromised. But before you click that link or respond, ask yourself: Is this even real? The reality is that fake bank texts—or smishing scams—are on the rise, and scammers are getting better at making their messages look legit. If you're not careful, one quick reply or click could put your account—and your money—at risk. The good news? There are clear signs to watch for that can help you spot a scam before it goes any further. Let's break them down. 1. The Text Didn't Come From Your Bank's Known Short Code Banks use short codes—those 5- or 6-digit numbers—for official communications like fraud alerts. But short codes can be spoofed, so even if the number looks legit, don't let your guard down. Big red flag? The text came from: A 10-digit number, which banks don't typically use for alerts. An email address (yes, some scammers send texts this way). An iMessage or other messaging platform. Pro Tip: Never click a link or call a number in a text message. If you need to check your account, go directly to your bank's app or official website. If you're unsure, call the customer service number listed on your bank's website—not the one in the text. 2. It Creates a Sense of Panic Scammers rely on urgency to trick you into acting fast. They'll send messages like: "Your account has been locked." "Suspicious login attempt detected." "A large transfer was flagged on your account." If the text is designed to make you panic-click a link or call a number, that's a major red flag. Banks may alert you to potential fraud, but they'll never push you to act immediately without verifying the issue first. 3. It Asks for Sensitive Information Your bank already knows your account details. They'll never ask for: Your password Your PIN Your Social Security number Any one-time verification codes (OTPs) If a text is asking for personal or financial information, it's a scam. Full stop. 4. It Contains a Link—And It's Suspicious Fake texts often include links that: Use shortened URLs (like Bitly or TinyURL) to hide their true destination. Slightly misspell your bank's name (like "wellsfargo.com" or "chsae.com"). Redirect you to a site that mimics your bank's login page to steal your credentials. Pro tip: Never click links in texts claiming to be from your bank. Instead, go to their official app or website directly. 5. It Includes Weird Grammar or Formatting While scammers are getting better at mimicking real messages, many still get tripped up by: Awkward phrasing: "Your account is temporary block. Verify now!" Random capitalization or punctuation: "ACT NOW!!! To Secure Your Funds." Generic greetings: "Dear Customer" instead of using your name. Legitimate bank texts are typically polished and professional. 6. It's From a Bank You Don't Even Use This one's a no-brainer. If you get a fraud alert or update from a bank where you don't even have an account, it's a scam. Legitimate banks don't send texts to non-customers. 7. It Promises Free Money or Rewards Banks don't send texts out of the blue offering cash prizes, refunds, or rewards. If a text claims you've "won" something or need to "accept a deposit," it's a ploy to get your attention and your data. What to Do If You Get a Suspicious Bank Text Here's your most important takeaway: never trust the information in the text itself. If you're concerned about the message, always verify using a trusted source, like your bank's official website or app. Here's how: Use Your Bank's App or Website: Log in directly to check for any alerts or messages. Call the Number on Your Bank's Website: Don't call the number provided in the text—it could lead straight to a scammer. Use the official customer service number listed on your bank's website or on the back of your debit or credit card. Visit Your Bank in Person: For serious concerns, stop by your local branch to confirm. This golden rule is simple but powerful: if you didn't initiate contact, always verify using a trusted, independent source. Common Scams to Watch For Here are the most frequent fake bank texts: Account Locked: "Your account has been locked due to suspicious activity." Large Purchase or Transfer: "Did you authorize a $1,500 payment to Amazon?" Login Attempt: "Unusual login detected on your account." Update Information: "Please verify your account details to avoid suspension." Fake Deposits: "$750 has been sent to your account. Tap here to claim it." Password Reset Requests: "Your password reset code is 123456. If you didn't request this, click here." Share This Knowledge with Someone You Care About Here's the thing: Scammers don't just target you—they target your friends, family, and loved ones too. And the truth is, not everyone knows how to spot a fake bank text. That's why it's so important to share what you've learned. Think about it: Does your parent know not to click on suspicious links? Would your best friend recognize a spoofed short code? Could your partner spot a phishing attempt? Take a moment to talk to the people in your life about these scams. Send them this article, show them examples of fake texts, and encourage them to be cautious. The more people know how these scams work, the harder it will be for scammers to succeed. Sign up for our newsletter to get the latest scam alerts, practical security tips, real-life scam examples, and expert advice to keep you one step ahead of online threats. Scammers have grown more sophisticated in their efforts to deceive their victims, with one of their common tactics being fake bank text messages designed to trick people into sharing sensitive personal information. We'll show you how to recognize fake bank scam messages and help protect yourself from fraud. How fake bank text messages work Cybercriminals use malicious text messages to masquerade as legitimate financial institutions and deceive unsuspecting targets into revealing personal information, leaving them vulnerable to identity theft. Here's how bank phishing scams work: Targeting: A scammer identifies potential victims through data breaches, public records, or social media profiles. Crafting the message: The scammer creates a convincing and urgent text message that appears to be from a legitimate bank. Sending the message: The scammer sends the fake text message to a targeted victim. Tricking the victim: The victim falls for the scam and takes the requested action. Data theft: Once the victim taps a malicious link or provides personal information, the scammer can steal their data for fraudulent purposes. Exploiting the stolen information: The scammer uses the information to piece together their identity and commits identity theft, financial fraud, or other crimes. Will a bank ever send you a text message? Yes, banks may send security alerts, account updates, and transaction notification text messages to customers. However, they will never require you to confirm your account details or request other personal information via text. In any case, it's important to be cautious and verify the authenticity of an SMS before interacting with any messages purportedly from your bank. 7 Warning signs of bank phishing The best way to avoid being tricked by a fake bank phishing scam is to know the red flags to look out for. Whenever you suspect a text from your bank might be fake, keep these fake bank text message warning signs in mind: 1. Unknown number Be cautious of text messages from unfamiliar numbers, as legitimate banks almost always use their official contact information when communicating with customers. If you're unsure whether a number is from your bank, contact their customer service directly to verify it. A phone screen showing a bank scam text from an unknown number. 2. Tempting links Avoid tapping on links in text messages that appear suspicious or unusual—they could lead to phishing websites designed to steal your personal information. Instead of tapping the link, you can manually type the bank's website address into your browser to access your account. 3. Personal information requests Never share sensitive information like your account number, password, or PIN in response to a text message. Legitimate banks will never ask for this information via text. If you ever receive a message requesting such information, it's a scam. A phone screen showing a scam text requesting personal information. 4. Urgent demands Be cautious of messages that create a sense of urgency and pressure you into making hasty decisions. If you receive a message demanding immediate action, take a step back and assess the situation carefully. It's important to avoid making impulsive decisions when dealing with suspicious messages. 5. Poor grammar and spelling If the text message contains grammatical errors or misspelled words, it might indicate a scam. Legitimate banks typically maintain high communication standards, so if you notice any inconsistencies in the message, treat it as a red flag. A phone screen showing a text with poor grammar and spelling. 6. Unexpected deals Be skeptical of unsolicited offers that seem too good to be true. Legitimate banks will typically communicate promotions or deals through more official channels, such as email or their website. If you receive an unexpected offer via text, it's best to verify it with the bank directly. 7. Inconsistent information If the text message contains conflicting or inaccurate information about your account, it's very likely a sign of a scam. Legitimate banks will nearly always provide accurate and consistent information. Some inconsistencies you may notice include: Fake emails and phone numbers: Scammers often use addresses and numbers that closely resemble the bank's legitimate contact details but with minor alterations. Inconsistent logos or branding: Fake messages may contain poorly designed logos or branding that doesn't match the bank's usual style. Missing or incorrect bank name: Some messages may use vague phrases like "your bank" instead of naming the specific institution you use. Missing or incorrect account information: A legitimate text will typically contain accurate account information (e.g., the last four digits of your account number). Scammers might leave out these details or make errors. Generic or short codes: Banks usually send texts from easily recognizable short codes or branded names. If the number looks like a personal phone number or a generic short code, it could be fake. A phone screen showing an inconsistent information text. What to do if you receive fake bank text messages Receiving a fake bank text message can be a distressing experience. However, understanding the appropriate steps to take can help mitigate potential damage and prevent further scams. By following these guidelines, you can protect your personal information and safeguard your financial security: Do not respond: Never reply to suspicious text messages or tap any links they contain. Verify the sender: Contact your bank using a known phone number or website to confirm the message's authenticity. Report the scam: Notify your bank about the scam and provide them with details about the message using a verified channel. Change your passwords: If you believe your personal information may have been compromised, change your passwords for your bank account and other online services. Monitor your accounts: Keep a close eye on your bank and credit card statements for unauthorized activity. Educate yourself: Learn about common scam tactics and how to identify them. Be cautious of unsolicited offers: Be wary of unexpected deals or promotions that seem too good to be true. Remember, if you ever suspect a message is fraudulent, always contact your bank directly through verified channels to verify its authenticity. Bank Email Phone Bank of America abuse@bankofamerica.com 800-432-1000 Capital One abuse@capitalone.com 800-227-4825 Citigroup spoof@citi.com 800-248-4226 Fifth Third Bank 53investigation@security.53.com 800-972-3030 JPMorgan Chase Bank phishing@chase.com 800–935–9935 PNC abuse@pnc.com 800-762-2035 Truist emailabuse@truist.com 844-487-8478 U.S. Bank fraud_help@usbank.com 877-595-6256 USAA abuse@usaa.com 877-762-7256 Wells Fargo reportphish@wellsfargo.com 866-867-5568 Tips for protecting your bank information Knowing what to do when you get an online banking text alert that turns out to be malicious is important. But taking preventive measures to help safeguard your banking information is even better. Here's how you can help protect your finances from scammers, hackers, and other cybercriminals: Use strong passwords: Create strong passwords that are difficult to crack. Enable two-factor authentication: Add an extra layer of security to your accounts by using two-factor authentication. Be cautious of public Wi-Fi: Avoid conducting sensitive banking activities on unsecured public Wi-Fi networks. Keep your software updated: Ensure your system and software are always updated with the latest security patches. Be mindful of phishing scams: Be aware of common phishing tactics and avoid tapping on suspicious links or downloading attachments from unknown sources. Monitor your accounts regularly: Review your bank and credit card statements for any unusual activity. Shred sensitive documents: Properly dispose of documents containing personal information. Be cautious when sharing personal information online: Avoid sharing personal information on social media or other public platforms. Use caution when using ATMs: Be aware of your surroundings and check for signs of ATM skimming before using one. Report suspicious activity: If you suspect your bank account has been compromised, report it to your bank immediately. It's also good to stay informed about the latest scams, like Cash App scams. Knowing how these ploys work can also help you recognize new patterns and protect yourself better against fake SMS bank message alerts. Protect yourself against bank text scams No matter how careful you are, it only takes one scam text allegedly from your bank to slip past your guard to put your finances at risk. That's why you need LifeLock, a comprehensive identity theft protection service with strong financial protection features. Try LifeLock Standard free for 30 days to monitor key changes to your credit file and get support if your wallet is stolen. You'll also get alerts if we detect fraudulent use of your personal information and personal restoration advice from our U.S.-based specialists if you fall victim to identity theft. FAQs about fake bank text messages Still have questions about fake bank text messages? We've got answers. How can I tell if a text message from my bank is legit? To determine if a text message from your bank is legitimate, verify the sender's information and contact your bank directly to confirm the message's authenticity. A bank will never send a text asking for personal information. How do I stop fake bank texts? To help stop fake bank texts, block and report scam numbers, enable spam filters on your phone, and consider registering for Do Not Disturb (DND) services to reduce unwanted messages. Can a scammer steal your info through text? Yes, scammers can steal your personal information through text messages by tricking you into tapping malicious links or providing sensitive data. Be cautious of any unsolicited messages that request personal information. Editor's note: Our articles provide educational information. LifeLock offerings may not cover or protect against every type of crime, fraud, or threat we write about. Reading Time: 6 minutes Phishing attacks have become a prominent threat in the world of cybersecurity, targeting individuals and organisations through deceptive tactics designed to steal sensitive information. One of the most common methods used by attackers to execute phishing attacks is by sending fake security alerts that appear legitimate, often invoking urgency or fear. These fake alerts aim to trick users into clicking malicious links, downloading harmful attachments, or revealing sensitive personal information. In this article, we'll explore how phishing attacks use fake security alerts to deceive users, how they work, the potential consequences of falling victim to such attacks, and the steps you can take to protect yourself from this type of threat. A fake security alert is a type of phishing attempt in which the attacker sends an email, text message, or pop-up notification that impersonates a legitimate security service or institution. These alerts often claim that the victim's account, device, or network is at risk, requiring immediate attention. They typically ask the user to perform actions such as resetting a password, updating security settings, or verifying personal information, often through a link or form provided in the message. The primary objective of these fake alerts is to create a sense of urgency or fear in the recipient, encouraging them to act quickly without thinking. This tactic is effective because users tend to trust security-related messages, especially when they are made to look official or come from familiar sources like banks, antivirus providers, or social media platforms. The wait is over—Cyberly's brand-new forum is live! Step inside and connect with real ethical hackers, seasoned security professionals, and curious minds just like yours. Want to ask a hacker how they think? Or pitch your ideas directly to our founder, James William Steven Parker? Now you can. ⚡ Join the Forum & Start Talking to Hackers Phishing attacks using fake security alerts generally follow a structured approach designed to exploit human psychology. Here's a breakdown of how these fake alerts work: Attackers often spoof email addresses, phone numbers, or websites to make the fake security alert appear legitimate. The message may appear to come from a trusted source, such as a well-known bank, government agency, or IT provider. The sender's address might look similar to that of the real institution, or it could even use the same branding, logos, and fonts to further deceive the recipient. The goal is to make the alert look authentic enough that the user doesn't question its legitimacy. For example, a phishing email may look like it's from the victim's bank, warning them that their account has been compromised, with a link to "verify" their details. The URL might appear genuine at first glance, but when clicked, it directs the user to a fraudulent site that harvests their login credentials. Fake security alerts often employ emotional manipulation to create a sense of urgency. The attackers may state that the victim's account will be locked, their security has been breached, or that there is suspicious activity on their account. These types of alarming messages compel the user to act quickly, bypassing rational thinking in the process. Example phrases that attackers use to invoke fear and urgency include: "Immediate action required to secure your account." "Your account has been compromised, click here to reset your password." "Suspicious activity detected, please verify your identity now." By creating an urgent call to action, the attacker hopes the victim will respond before they have a chance to question the message. To further deceive the user, fake security alerts often imitate legitimate security actions that the user might expect to receive. These can include: Requests to update security information or change passwords Notifications about account activity that seems out of the ordinary Alerts about a device or account being compromised Notices about software or antivirus updates that must be installed immediately The user is more likely to trust the message if it mimics actions they are accustomed to receiving from legitimate service providers. Fake security alerts typically contain a link that redirects the user to a fraudulent website. These websites often resemble the official pages of a trusted institution, such as a bank or social media platform. Once the user enters their login credentials or personal details, the attacker steals that information for malicious purposes. For instance, the phishing email might instruct the victim to click a link to "verify their account details" on the bank's website. However, the link leads to a copycat website where the user enters sensitive information, unknowingly handing it over to the attacker. Fake security alerts often ask for personal or financial information, which is then used for identity theft, fraud, or other malicious activities. These requests can include asking users to provide: Login credentials (usernames and passwords) Social security numbers Payment card details Security questions and answers This information can be used to access online accounts, commit fraud, or carry out identity theft. Phishing attacks using fake security alerts are often executed using common themes or approaches. Here are a few examples of fake security alerts: A common fake security alert is one that pretends to be from the victim's bank, informing them of suspicious activity or a security breach on their account. The alert might state that their account has been locked, that an unrecognised transaction has occurred, or that their login credentials need to be updated immediately. Example Alert: "Dear Customer, we've detected unusual activity on your account. Please click here to secure your account immediately or your access will be suspended." Phishing emails may appear to be from antivirus companies or software providers, warning users that their system is infected with Malware or that they need to update their security software. The email may contain a link to a fake website that requests payment for a software update or download of a malicious program. Example Alert: "Your computer is infected with a virus. Please update your antivirus software by clicking here immediately to avoid losing your files." Phishing emails targeting online shopping or e-commerce platforms often use fake security alerts to claim there's a problem with a user's order, payment, or account verification. These emails may ask users to click on a link to resolve an issue, leading to a fraudulent website that collects their credit card information. Example Alert: "We couldn't process your payment. Click here to update your payment details and complete your order." Fake security alerts are also common on social media platforms. Attackers may impersonate the platform to warn users of unauthorised login attempts or suspicious activities. The email might ask users to click a link to "verify" their identity or reset their password. Example Alert: "There was an attempt to access your account from an unrecognised device. Click here to secure your account and change your password." Phishing attacks that use fake security alerts can lead to a wide range of serious consequences for victims. Here are some potential outcomes: If attackers successfully gain access to sensitive personal information such as social security numbers, banking details, or credit card information, they can engage in identity theft. This can result in fraudulent loans, unauthorized transactions, and a host of other criminal activities that can significantly damage the victim's financial standing and credit score. For individuals, phishing attacks can result in financial losses due to unauthorised access to bank accounts or payment card details. Attackers can drain accounts, make purchases, or transfer funds. For businesses, the financial impact can be even more severe, particularly if customer information is compromised. In some cases, clicking on a link or downloading an attachment from a fake security alert can result in Malware infections. Ransomware, spyware, and viruses can damage systems, encrypt files, or steal sensitive data. Once Malware is installed, it can spread across networks and systems, causing widespread damage. If an organisation falls victim to phishing attacks that impersonate their own security protocols, the resulting breach of trust can have long-lasting effects. Customers may lose confidence in the company's ability to safeguard their personal information, leading to a loss of business, legal ramifications, and reputational damage. While phishing attacks using fake security alerts can be convincing, there are several measures you can take to protect yourself: Always verify the sender of any security alert, especially if the email or message is unexpected or contains alarming language. Contact the organisation directly using verified contact details, such as their official website or customer service phone number, to confirm the authenticity of the alert. Before clicking on any link, carefully inspect the URL. Phishing websites often use slightly altered domain names to appear legitimate. Ensure that the link starts with "https://" and that the domain name matches the official website of the institution you believe the message is from. Be wary of any unsolicited attachments or downloads, even if they appear to come from trusted sources. Opening these attachments can lead to Malware infections. Enable multi-factor authentication on all your accounts, especially those related to financial transactions, emails, and social media. MFA adds an extra layer of protection, ensuring that even if an attacker obtains your password, they cannot access your account without a second verification step. Install and regularly update antivirus and anti-Malware software on your devices. These programs can detect and block malicious links or attachments before they have a chance to cause harm. Stay informed about the latest phishing tactics and regularly review common warning signs of phishing. Educating yourself and your employees, family members, or colleagues can help reduce the risk of falling for these types of attacks. Fake security alerts are one of the most effective methods used in phishing attacks due to their ability to exploit a victim's fear, trust, and urgency. By impersonating legitimate security sources, creating a sense of panic, and tricking users into clicking malicious links, attackers can steal sensitive information or infect devices with Malware. However, by staying vigilant, verifying alerts, avoiding unsolicited links and attachments, and employing additional security measures, such as multi-factor authentication, you can significantly reduce the risks posed by phishing attacks. The wait is over—Cyberly's brand-new forum is live! Step inside and connect with real ethical hackers, seasoned security professionals, and curious minds just like yours. Want to ask a hacker how they think? Or pitch your ideas directly to our founder, James William Steven Parker? Now you can. ⚡ Join the Forum & Start Talking to Hackers Disclaimer: This post may contain affiliate links. If you make a purchase through one of these links, Cyberly may earn a small commission at no extra cost to you. Your support helps us continue providing free tutorials and content. Thank you! When Kelli Hinton got a text message asking if she'd attempted to wire $7,500 out of her Chase Bank account, Kelli's heart sank.After replying "NO" she quickly received a phone call from someone claiming to be a Chase Bank fraud investigator who convinced her to transfer her entire savings — over $15,000 — to a "safe" account [*]. It was, in fact, a complete scam.Over 40% of people who reported a text scam said the text impersonated a bank, was about a gift, delivery or job, or claimed to be from Amazon [*].With scammers regularly assailing your bank account, it's important to be able to tell a fake bank text message from a real one.{{show-toc}}How Do These Fake Bank Text Messages Work?Fake bank text messages are a type of smishing where fraudsters use text messages to impersonate financial institutions and phish for sensitive information or dupe victims into sending them money. Scammers spritz their victims with fake fraud alerts, payment confirmations, or account suspensions.If you respond, they ask for credit card or bank account numbers, or personally identifiable information (PII) to "fix the problem."Robotexts saw a 37% increase, while robocalls decreased by 25% in December — more evidence that SMS is a preferred method to con recipients [*].While there are numerous types of fake bank text message scams, they all follow a similar pattern: Scammers send you a text message claiming to be from your bank. The message contrives a sense of urgency by claiming that there was suspicious activity or that someone made a large purchase from your account. As a result, the message asserts, your account will be locked, suspended, or closed if you don't act quickly. To secure your account, you're asked to click on a link or call a number. Scammers know that most people will react quickly to a fraud alert from their bank — so they provide easy and legitimate-looking options for you to contact them. You're taken to a fake website that looks like your bank's login page. When you type in your credentials, scammers steal them and gain access to your online bank account. Hackers may even secrete malware within these links, to spy on your online activity or steal sensitive data from your device. Or you're connected to a scammer pretending to be from your bank's fraud department. A "customer service representative" may ask you for your banking details and other personal information that they can use to drain your bank account or open lines of credit in your name.If you respond with YES, NO, STOP, or anything else, you receive a call from an imposter. Replying indicates that you received the text message and are actively engaged with SMS. Knowing this, scammers will continue to target you, or may sell your "active" number on the Dark Web. Protect yourself from scam texts with AI. Aura's award-winning digital security solution uses artificial intelligence to block spam calls and text messages. Try Aura free for 14 days.How To Tell If a Bank Text Is Fake: 6 Warning SignsWhile some fake text messages are obvious frauds with mangled spelling and suspicious links, others are much harder to spot. Modern scammers copy legitimate alerts that banks send via text messages to trick victims into replying. They may even spoof the bank's phone number or use a believable email address to make you think it's the real thing.Example of a fake bank text message scam. Source: RedditBut upon further examination, scam text messages always have one or more telltale signs of fraud. Here are six ways to identify a fake text message scam: It doesn't come from your bank's short code or number. If a bank texts you, it will come from a five or six-digit "short code." For example, Chase Bank's fraud department will only text you from 28107, 36640, or 72166 [*]. It comes from an email address that looks like your bank's address. Scammers send texts from email addresses to make them seem more legitimate. Your bank will not send you text messages from an email address.It includes strange phrasing and grammatical errors. Scammers often use random capitalization, unusual punctuation, and may begin a text with generic greetings like "Dear Valued Customer."The link is suspicious or shortened to hide where it's taking you. Before you click on a link, double-check where it is taking you. Beware of Bitly or TinyURL links or links with jumbled variations of common website names (like "goo.gl").The link takes you to a site that's not on your bank's official domain. If you do click on a link in a text message, make sure it hasn't taken you to a fake website. For example, a Wells Fargo scam text may contain a link to "wellsfarrgo.com" or "welllsfargo.com." (Note the misspellings of "wellsfargo.")It's from a bank you don't use. Banks cannot send you any promotional materials unless you've opted in — and they certainly won't alert you about fraud on accounts that don't exist. If you get a fraud alert from a bank that you don't use, it's a scam. Safeguard your finances with award-winning protection. Aura's digital security app has been rated #1 by Money.com, USNews.com, Forbes, and more. Try Aura free for 14 days.Will a bank ever send you a text message?Yes, banks will text you about legitimate fraud alerts. They may also send marketing communications or balance alerts via SMS if you've signed up for those notifications.When communicating with customers, banks use specific short codes or numbers to signify that the text is from a real bank. The exact digits may also refer to specific types of texts — for example, you may receive a text from one short code to notify you about a loan update and a text from a different short code regarding your account security.Here are some short codes for fraud and security alerts used by some major banks:Chase: 28107, 36640, 72166Bank of America: 322632 (credit card security), 39989 (debit card security), 96264 (small business credit card), 86006 (check fraud), 55983 (banking security), 56433 (account takeover), 80814 (Zelle)Citibank: 95686Wells Fargo: 93557, 93733, 93729, or 93236Note: Beware of spoofed phone numbers. Scammers have ways to mask or hide the true number they're using to contact you (such as by using restricted phone numbers). Always look for signs of fraud — even if it comes from a legitimate-looking phone number. The 6 Most Common Fake Bank Text Messages To Watch For1. Your account has been locked due to suspicious activityIn this type of text message scam, crooks dangle the fear of losing access to your bank account to get you to relinquish sensitive information — including your username and password. The scam is simple: fraudsters claim that someone has illegally accessed your account and that it has been locked for your protection.In order to regain access, you'll need to "verify" your identity or provide financial information.If you click on the link, you'll be taken to a fake website that looks like your bank's login page. But any information that you enter will go straight to scammers, giving them full access to your bank account. How to stay safe: Don't click on links in text messages claiming to be from your bank. Instead, always log in to your account directly by using your bank's mobile app or its official website. If there's an issue with your account, you'll see it when you try to access your account. Related: How To Protect Your Bank Account From Identity Theft →2. There was a large purchase or transfer made from your accountIn another common scam, fraudsters notify you of an apparent large purchase from a store like Amazon, Target, or Walmart — using your bank account.Example of a fake text message claiming that a purchase was made from your account. Source: RedditThe goal is to make you afraid that you'll be held responsible for a fraudulent purchase. But replying, clicking on a link, or calling the phone number provided puts you one step closer to identity theft.How to stay safe: Review all purchases by logging in to your bank account either via the bank's mobile app or its official website. If you're still unsure, call your bank's fraud department to double-check. Related: How To Spot a Chase Phishing Email (5 Examples) →3. Someone tried to log in to your bank accountSwindlers know that you'll be alarmed if there's suspicious activity on your account, so they use that to trick you into responding to their texts.Posing as your bank, they may say an unauthorized user attempted to log in to your bank account or that they've detected fraudulent activity.Example of a fake bank text message claiming your account was compromised. Source: RedditLike other bank text message scams, these texts usually include a link to reactivate your account or a request to call customer support. Instead of resolving the "issue," scammers excise your personal information.How to stay safe: Again, verify any claims of fraud directly — either by logging in to your bank account or calling the customer service phone number listed on your bank's website. A representative will be able to confirm whether there has been any fraudulent activity that you should worry about. Related: Can You Get Hacked By Responding To a Text? →4. You need to update your account informationFrom time to time, banks will ask you to update personal details like your address, telephone number, email, or even income. However, they'll never ask you to reveal that information via texts or email attachments. Scammers send fake text messages that look like routine account maintenance, asking you to update your password.Other times, fraudulent texts claim there's unusual activity on your account, and you need to update your information.Example of a fake text message claiming that you need to verify your account details. Source: AuraHow to stay safe: Don't take the bait. If a bank truly needs you to update your information, it will ask you to do so in person or via its secure online banking portal. Related: Is It Safe To Link Bank Accounts? 7 Risks To Know →5. Someone is sending you moneyIt's natural to be curious if someone unexpectedly sends you money via Venmo, Zelle, or Cash App. But it's almost certainly too good to be true — and the "deposit" link will take you to a scammer's website. If you've already signed up for these platforms, money sent to you will automatically be deposited into your account. Remember, you'll only receive notifications if you've signed up to get them.Example of a fake text message claiming that you've received a money transfer. Source: AuraNote that grifters sometimes take the opposite approach, making you think someone else used a money transfer app on your account to send money to themselves or someone else.How to stay safe: An easy way to confirm whether or not this is true is to check your bank or payment app to see if the transfer was really made. Also, never accept unexpected Zelle, Cash App, or Venmo transfers. Related: How To Spot a Citibank Phishing Email (With Examples) →6. Fake password reset or 2FA code text messagesBanks now encourage or require users to enable two-factor authentication (2FA) on their accounts. Unfortunately, scammers have picked up on this trend.Some fake bank text messages ask for PINs or prompt victims to reset their passwords using a link that goes to a fake website. If the victims click on these links, they risk infecting their phones with malware or giving away their usernames and passwords.How to stay safe: Never share passwords, PINs, or 2FA codes with anyone — even coworkers, friends, or family members. Scammers may have already hacked into their accounts and will use the information you give them to hack your accounts, too.Did You Receive a Fake Bank Text?You're not in immediate danger if you've only received or replied to a scam text. However, you should still take precautions to protect your account if you've given scammers any information. Here's what to do: Contact your bank's fraud department. Share what happened and ask them to close your current accounts and cards. They will help you open new ones and send you brand-new cards.Freeze your credit. If you gave away any sensitive information (particularly your Social Security number), initiate a credit freeze with Experian, Equifax, and TransUnion. A credit freeze will prevent scammers from taking out loans or opening any new credit lines in your name. You may also want to set up continuous credit monitoring to catch other criminal activity.Report the scam. You should report unwanted calls or texts to the Federal Trade Commission (FTC) at DoNotCall.gov and file a complaint with the Federal Communications Commission (FCC).Scan your device for malware. First, disconnect your devices from your Wi-Fi and mobile network. Then, use antivirus software to detect and eliminate any harmful code. Also update your devices and apps to remove any security vulnerabilities in outdated software.Secure your other online accounts. Scammers can use your personal information to target other online accounts. Change passwords on all of your accounts — especially your online banking profile, social media, and email — and enable 2FA whenever possible.Download a Safe Browsing app. These identify (and stop you from going to) malicious sites. Using a secure, reliable virtual private network (VPN) can also hide your online activity from fraudsters.Consider signing up for spam protection. Aura's all-in-one intelligent safety app includes an AI-powered assistant that can automatically block spam or scam calls and texts. Try Aura free for 14 days. Zoom out: Block suspicious phone numbers. If you're an iPhone user, tap the "Delete and Report Junk" option to delete a suspicious text. If you're an Android user, touch and hold the conversation, tap "Block," and then tap "Report spam." How To Protect Yourself Against Fake Bank Text MessagesKeep your accounts safe and avoid fake bank texts by:Using secure and unique passwords that hackers can't guess or use to access other accounts.Enabling 2FA on your accounts to add another layer of protection against cybercriminals.Never giving out passwords, PINs, or one-time use codes that bad actors could use to drain your bank accounts or sell on the Dark Web.Not clicking on links in text messages so that you can avoid installing dangerous viruses or malware onto your phone.Getting familiar with your bank's short codes to better identify, delete, and block scam texts before you accidentally share any information.For added protection, consider signing up for Aura's digital safety app. With Aura, you get top-rated identity theft protection with the industry's fastest fraud alerts,3 AI-powered spam and scam call/text protection, a full suite of digital security tools for your cell phone and computer, 24/7 U.S-based White Glove Fraud Resolution support, and $1 million in identity theft insurance — all for a low monthly membership. Keep your bank account safe from scammers. Try Aura free for 14 days. Text messages are a favoured tool for scammers. The mobile network EE reported that it blocked more than 45 million scam texts in 2023.Texts sent by fraudsters, also known as smishing, can be devious scams seeing you lose money immediately by entering your details into a dodgy website, or over months by being groomed by criminals pretending to be a job recruiter.Here we detail the text scams we've seen recently and share advice on how to spot and avoid a text scam.Our emails will alert you to scams doing the rounds, and provide practical advice to keep you one step ahead of fraudsters.Sign up for scam alerts1. Fake bank textsA scam text impersonating HSBCA typical recent example of a fake bank text claims to be from HSBC. It's sent from a random mobile number and tells you that you've spent a certain amount of money at a particular brand.It states that the transaction was attempted on your account and to call a number if it wasn't you who made the transaction. This most likely leads to a vishing scam where a scammer then calls you impersonating the bank, and your personal and financial details will be asked for.It also includes a fake reference number to appear legitimate. On Who Calls Me, a website which collects data on scam numbers, a recipient reported that after calling the number they were then asked for their card details for a suspicious payment to be checked.The police force in Jersey recently warned of a scam circulating around the Channel Islands after it received 14 individual reports of a particular bank impersonation text scam between 4 and 9 January. Victims' total losses amounted to £138,000. The police noted that the scam texts it had come across cited 'CryptoCom' as the company the suspicious transaction had been paid to, and that the message asked you to reply 'Y' if you made the transaction and 'N' if you didn't. A response then prompted the scammer to call you.2. Recruitment scamsA scam text impersonating a recruitment companyOut-of-the-blue messages that claim to be from recruitment companies are also circulating. Sometimes the texts impersonate a legitimate person or company.These texts are the start of job scams, which go on to steal your money in various ways. Once you engage with the fraudster, they may ask you for money upfront, such as for work equipment, and then vanish after the money is sent. Or they ask for scans of documents like passports or driving licences to steal your identity.Fraudsters also send texts that advertise simple work-from-home jobs such as completing surveys. These will appear legitimate as you start doing the 'job'. However, you'll eventually be asked to invest some of your own money to complete more tasks, for example, and you'll never be able to withdraw what you've earned.3. Missed delivery textsAs so many of us wait for deliveries, scammers bank on us clicking on dodgy links in 'missed delivery' texts. These scam messages impersonate popular delivery companies including DPD, UPS, Evri and the Post Office.In one message we found, a text impersonating the Post Office and the Royal Mail tells you that your parcel is unable to be delivered and prompts you to follow a malicious link to 'reschedule a redelivery'.The link leads to a convincing fake Royal Mail website which asks for your postcode before asking you to pay £1.45 for your parcel to be redelivered. This is where your personal and financial data will be stolen.We've also seen scam texts imitate delivery company Evri, which also leads to dodgy phishing websites impersonating the brand. Both texts ask you to follow the link to arrange the redelivery of a missed item and are sent from random mobile numbers.Which? shared this scam with the Post Office and it confirmed that it was a scam. It also advised that it doesn't deliver mail, so a message like this claiming to be from the Post Office is a definite scam. 4. Wrong number scamsScammers attempt to groom you into their elaborate fraudulent schemes by sending 'wrong number' texts.These texts begin by saying something you would say to a friend, such as: 'It was nice seeing you the other day,' in anticipation of you replying asking who it is.The scammer will then say a random name and you'll tell them that they have the wrong number. This typically leads to a conversation which ends with a dodgy crypto investment scheme being promoted by the scammer.5. HMRC refund textScammers are impersonating HMRC in a bogus tax refund text which tells you that you're owed £277.It then prompts you to follow a malicious link to 'claim your tax refund'.If you receive a text claiming to be from HMRC, log in to your official HMRC online services account to verify any information in it.HMRC does send texts to some customers, but it will never ask for personal or financial information. Never click on links in messages claiming to be from HMRC. Avoiding and reporting scam textsUnsolicited texts are always something to be wary of. If you do receive a text like this:Avoid following any links in the message.Be suspicious of texts asking for personal information.To verify the legitimacy of a text, contact the company that it claims to be from directly or log in to your online account with the company using its official website.Don't reply to the message as this will let the scammer know that the number is active.You report scam texts by forwarding the message to 7726. If you have been scammed, call your bank immediately using the number on the back of your bank card and report it to Action Fraud, or call the police on 101 if you live in Scotland. If you receive a suspicious text message that claims to come from a bank, it's very likely part of a phishing scam, especially if you don't do any business with that financial institution. Such messages often claim there's an issue with your account; a problem with a previous purchase; or a transfer of money that you need to stop by clicking a link. These are often referred to as "bank alert text scams." We strongly advise against clicking any links in these kinds of messages. Instead, delete the texts from your phone. Such links can compromise your accounts and lead to fraudulent pages that scammers created to seem like official bank websites. For example, the phishing links in these text messages might send you to a website that appears to be an official page for Bank of America, Chase, Citibank, Wells Fargo, or another banking institution. In reality, though, scammers designed the website to try to convince you of their "legitimacy," and into spilling your login details for online banking, personal information, and financial data. One example of a bank alert text scam message claiming to be from Chase surfaced on Twitter in July 2022. The text message read, "Chase: Your debit card has been temporarily disabled; in order to reinstate it, go over all of your personal info carefully." The link in the message led to a phishing attempt; It did not go to the bank's official website, Chase.com. In another example, a Twitter user described being targeted by scammers who were pretending to be associated with Bank of America. That scammy text message read, "BofA: As of 07/27/22 your account has been placed on hold. To regain access visit [link] and confirm your information." We reviewed the link and found it to be dangerous, just like the one that claimed to come from Chase. In another tweet, a user included a screenshot of a message showing scammers pretending to be associated with Citibank. "Did you try sending $5,000.11 to Michael P from your Citi Checking Account? To confirm your transfer reply YES. If this was NOT you, Cancel immediately at: [link]." Yet again, we looked into the link and it, too, led to a scammer's website. The U.S. Federal Trade Commission and the Better Business Bureau both published guidance on these kinds of text scams. We recommend reviewing their tips if, or when, you fall victim to these types of messages. You're going about your day when a text from your bank pops up: "Unusual activity detected. Click here to secure your account." It feels urgent, serious, and maybe even a little terrifying. After all, no one wants their bank account compromised. But before you click that link or respond, ask yourself: Is this even real? The reality is that fake bank texts—or smishing scams—are on the rise, and scammers are getting better at making their messages look legit. If you're not careful, one quick reply or click could put your account—and your money—at risk. The good news? There are clear signs to watch for that can help you spot a scam before it goes any further. Let's break them down. 1. The Text Didn't Come From Your Bank's Known Short Code Banks use short codes—those 5- or 6-digit numbers—for official communications like fraud alerts. But short codes can be spoofed, so even if the number looks legit, don't let your guard down. Big red flag? The text came from: A 10-digit number, which banks don't typically use for alerts. An email address (yes, some scammers send texts this way). An iMessage or other messaging platform. Pro Tip: Never click a link or call a number in a text message. If you need to check your account, go directly to your bank's app or official website. If you're unsure, call the customer service number listed on your bank's website—not the one in the text. 2. It Creates a Sense of Panic Scammers rely on urgency to trick you into acting fast. They'll send messages like: "Your account has been locked." "Suspicious login attempt detected." "A large transfer was flagged on your account." If the text is designed to make you panic-click a link or call a number, that's a major red flag. Banks may alert you to potential fraud, but they'll never push you to act immediately without verifying the issue first. 3. It Asks for Sensitive Information Your bank already knows your account details. They'll never ask for: Your password Your PIN Your Social Security number Any one-time verification codes (OTPs) If a text is asking for personal or financial information, it's a scam. Full stop. 4. It Contains a Link—And It's Suspicious Fake texts often include links that: Use shortened URLs (like Bitly or TinyURL) to hide their true destination. Slightly misspell your bank's name (like "wellsfargo.com" or "chsae.com"). Redirect you to a site that mimics your bank's login page to steal your credentials. Pro tip: Never click links in texts claiming to be from your bank. Instead, go to their official app or website directly. 5. It Includes Weird Grammar or Formatting While scammers are getting better at mimicking real messages, many still get tripped up by: Awkward phrasing: "Your account is temporary block. Verify now!" Random capitalization or punctuation: "ACT NOW!!! To Secure Your Funds." Generic greetings: "Dear Customer" instead of using your name. Legitimate bank texts are typically polished and professional. 6. It's From a Bank You Don't Even Use This one's a no-brainer. If you get a fraud alert or update from a bank where you don't even have an account, it's a scam. Legitimate banks don't send texts to non-customers. 7. It Promises Free Money or Rewards Banks don't send texts out of the blue offering cash prizes, refunds, or rewards. If a text claims you've "won" something or need to "accept a deposit," it's a ploy to get your attention and your data. What to Do If You Get a Suspicious Bank Text Here's your most important takeaway: never trust the information in the text itself. If you're concerned about the message, always verify using a trusted source, like your bank's official website or app. Here's how: Use Your Bank's App or Website: Log in directly to check for any alerts or messages. Call the Number on Your Bank's Website: Don't call the number provided in the text—it could lead straight to a scammer. Use the official customer service number listed on your bank's website or on the back of your debit or credit card. Visit Your Bank in Person: For serious concerns, stop by your local branch to confirm. This golden rule is simple but powerful: if you didn't initiate contact, always verify using a trusted, independent source. Common Scams to Watch For Here are the most frequent fake bank texts: Account Locked: "Your account has been locked due to suspicious activity." Large Purchase or Transfer: "Did you authorize a $1,500 payment to Amazon?" Login Attempt: "Unusual login detected on your account." Update Information: "Please verify your account details to avoid suspension." Fake Deposits: "$750 has been sent to your account. Tap here to claim it." Password Reset Requests: "Your password reset code is 123456. If you didn't request this, click here." Share This Knowledge with Someone You Care About Here's the thing: Scammers don't just target you—they target your friends, family, and loved ones too. And the truth is, not everyone knows how to spot a fake bank text. That's why it's so important to share what you've learned. Think about it: Does your parent know not to click on suspicious links? Would your best friend recognize a spoofed short code? Could your partner spot a phishing attempt? Take a moment to talk to the people in your life about these scams. Send them this article, show them examples of fake texts, and encourage them to be cautious. The more people know how these scams work, the harder it will be for scammers to succeed. Sign up for our newsletter to get the latest scam alerts, practical security tips, real-life scam examples, and expert advice to keep you one step ahead of online threats.