If you are involved in a situation that fits one of the following descriptions, it could be a scam and you should contact Centennial Bank immediately.

Job scams: You accept a job in which you receive a commission to facilitate money transfers through your account or apply for a job that asks you to set up a new bank account.

Job scammers use reputable online job boards to offer work-at-home jobs or accounting positions. These job scams may require employees to receive money into their existing bank account (or open new accounts) and then transfer the money to another account, often overseas. As payment, the job seeker is instructed to keep a small percentage of the transfer.

Lottery or sweepstakes scams: You receive notice that you are the winner of a lottery that you did not enter, but must pay a small percentage for fake taxes or other fees before you can receive the rest of your prize.

Dating scams: Someone you met through an online dating site or chat room asks you to send money for a variety of reasons, including a need for urgent surgery or to make travel arrangements to meet in person.

Internet scams: You receive a check for something you sold over the internet, but the amount of the check is more than the selling price. You are instructed to deposit the check, but send back the difference in cash.

OR

You receive a check from a business or individual different from the person buying your item or product.

OR

You are instructed to transfer money, or receive a transfer of money, as soon as possible.

Telephone scams: Unless you initiated the contact, do not give out personal information over the telephone. If the call is not initiated by you, always ask for a callback number. Use legitimate sources to verify Centennial Bank contact information

Mortgage scams: Mortgage scams can target both prospective and current homeowners. Prospective buyers should be leery of agencies that offer to falsify or alter information to obtain a favorable loan decision. Con artists may also target distressed homeowners with promises of non-legitimate foreclosure

rescue, short sale, or loan modification scams. While there are legitimate companies that offer these services, your mortgage lender is in the best position to work with you to understand your situation and look for solutions.

If you believe you are the victim of a scam involving your Centennial Bank mortgage, contact us immediately.

PROTECTING YOURSELF

1. Do not share any confidential information through suspicious emails, websites, social media networks, text messages or phone calls.
2. Protect your personal and account information, including your online banking username, password, and answers to security questions. Do not write this information down or share it with anyone.
3. Install, run, and keep anti-virus software updated.

Fraudulent emails (phishing)

Phishing is usually a two-part scam involving emails and spoof websites. Fraudsters, also known as phishers, send an email to a wide audience that appears to come from a reputable company. This is known as a phish email.

In the phish email, there are links to spoof websites that imitate a reputable company's website. Fraudsters hope to convince victims to share their personal information by using clever and compelling language, such as an urgent need for you to update your information immediately or a need to communicate with you for your own safety or security. Once obtained, your personal information can be used to steal money or transfer stolen money into another account.

Use caution if you receive an email expressing an urgent need for you to update your information, activate your online banking account, or verify your identity by clicking on a link. These emails may be part of a phish scam conducted by fraudsters to capture your confidential account information and commit fraud.

How fraudsters obtain email addresses

Fraudsters obtain email addresses from many places on the Internet. They also purchase email lists and sometimes guess email addresses. Fraudsters generally have no idea if people to whom they send banking-related phish emails are actual bank customers. Their hope is that a percentage of those phish emails will be received by actual bank customers.

If you receive a fraudulent email that appears to come from Centennial Bank this

does not mean that your email address, name, or any other information has been taken from Centennial Bank's systems.

Fraudulent websites (phish or spoof websites)
Fraudsters may attempt to direct you to spoof websites via emails, pop-up windows or text messages. These websites are used to try to obtain your personal information. One way to detect a phony website is to consider how you got to the site. Use caution if you may have followed a link in a suspicious email, text message, online chat or other pop-up window requesting your personal or account information.

Variations on phishing attacks:

Pop-up windows
Fraudsters may use pop-up windows – small windows or ads – to obtain personal information. These windows may be generated by programs hidden in free downloads such as screen savers or music-sharing software. To protect yourself from harmful pop-up windows, avoid downloading programs from unknown sources on the Internet and always run anti-virus software on your computer

Telephone or voice phishing
Known as vishing, or voice phishing, this tactic is a phishing attempt made through a telephone call, fax or voice message. If you are uncomfortable continuing a phone call that was not initiated by you, ask for a reference number and call Centennial Bank, using legitimate sources of contact information. This includes information found on hcsb.com, information on your bank statements, and phone numbers listed on your ATM, debit or credit card.

Text-message phishing
A phishing attempt sent via SMS (Short Message Service) or text message to a mobile phone or device. This tactic is also referred to as smishing, which is a combination of SMS and phishing. The purpose of text message phishing is the same as traditional email phishing: convince recipients to share their sensitive or personal information.

Never disclose via text message any personal information, including account numbers, passwords, or any combination of sensitive information

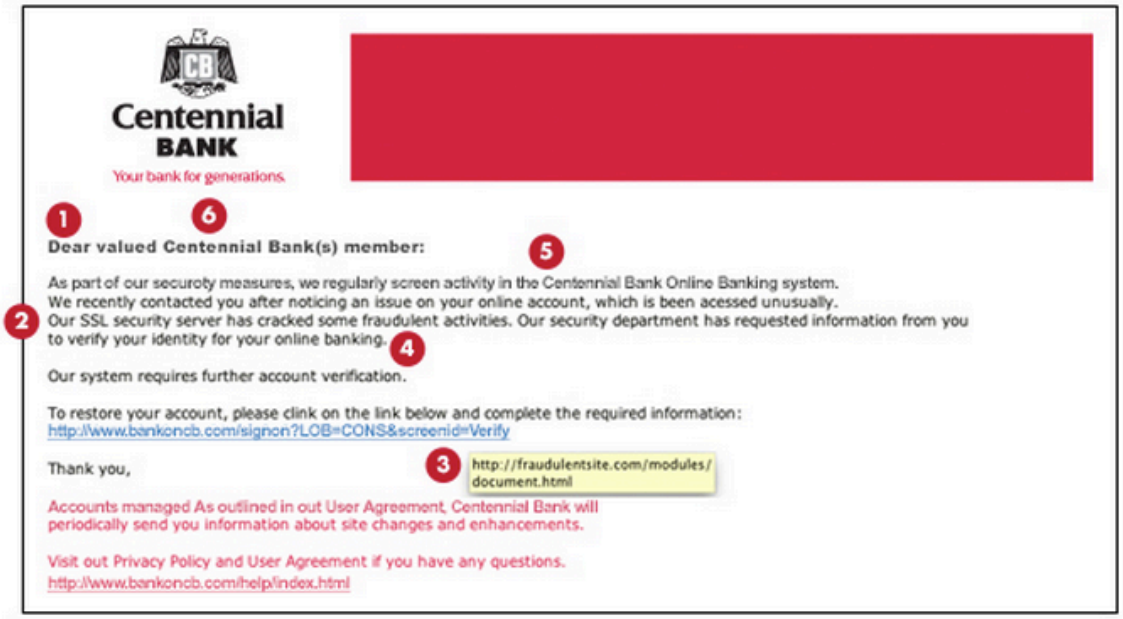
that could be used fraudulently. Use caution if you receive a text message expressing an urgent need for you to update your information, activate an account, or verify your identity by calling a phone number or submitting information on a web site. These messages may be part of a phishing scam conducted by fraudsters to capture your confidential account information and commit fraud.

Fraudulent emails

Fraudulent emails (phish) and websites can be very sophisticated and may look identical to Centennial Bank's emails and websites. Fraudsters can even tamper with the sender information in an email to make their phish look even more legitimate.

Although fraudsters use various tactics in their phish, there are common elements you should familiarize yourself with.

1. **Awkward Greeting** – A phish may address the customer with a nonsensical greeting or may not refer to the customer by name.
2. **Typos** – This isn't because fraudsters don't know how to spell – it's so the phish won't be blocked by email filters.
   Example: "accessed" "Our SSL security severs has…" "fradulent"
3. **Strange or Unfamiliar Links** – This link look official, but notice what happens when the mouse cursor rolls over it. The link's source code points to a completely different website. **Remember that you can always type a URL into your web browser instead of clicking on a link.**
4. **Incorrect Grammar** – Another tactic used to bypass email filters.
   Example: "Our SSL security sever has…"
5. **Compelling or Urgent Language** – An urgent need to communicate with you for your own security, or a request to update information immediately.
   Example: "We recently contacted you after noticing an issue on your online account, which has been acessed unusually." "Our security department has requested information from you to verify your identity for your online banking."
6. **Misspelled Company Name** – Another tactic used to bypass email filters.
   Example: "Centennial Bank (s)"



This is not a comprehensive list of phish email characteristics, but these examples will help you learn to recognize fraudulent emails.

Centennial Bank is dedicated to protecting your information. Learn about our security measures and what we do to protect your accounts online.