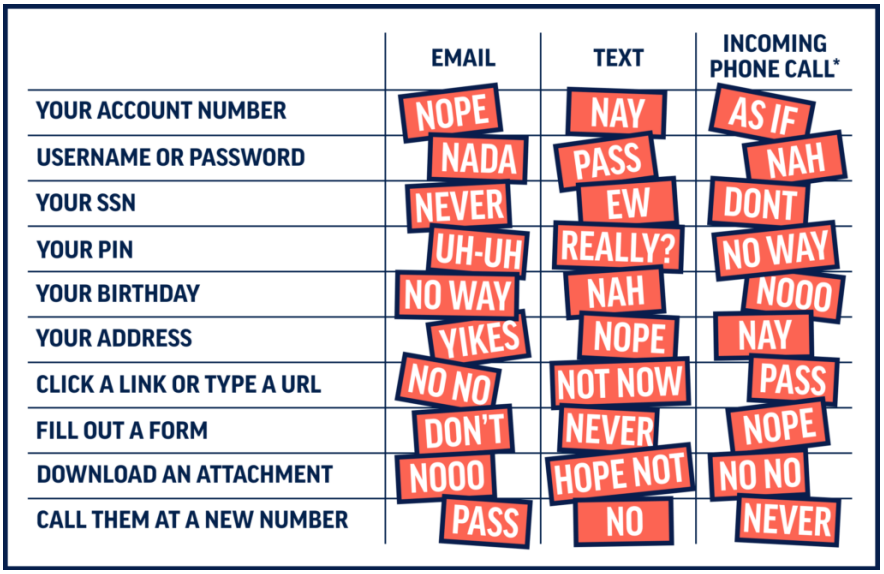
Heritage BANK

BANKS NEVER ASK THAT!

Watch for these red flags. Heritage would never ask for them.

If you receive an email, text, or phone call for any of this, it's a definite red flag. It's better to be safe than sorry. End the call, delete the text, and trash the email, because banks never ask that! Want to learn more?

*Note: You may be asked to verify confidential information if you call your bank, but rarely the other way around. If you're ever in doubt that a bank call is legitimate, or if a caller pressures you to stay on the line and provide bank information right away or something bad will happen, it is a scam. Hang up and call the number on the back of your card to talk to a real bank employee.



FAQs

What is phishing?

Phishing is a type of online scam where criminals make fraudulent emails, phone calls, and texts that appear to come from a legitimate bank. Every year, people lose hundreds, even thousands of dollars to these scams. The communication is designed to trick you into entering confidential information (like account numbers, passwords, PINs, or birthdays) into a fake website by clicking on a link, or to tell it to someone imitating your bank on the phone.

What to do if you receive a scam email, call, or text.

Email or Text: If you suspect that an email or text you receive is a phishing attempt:

- Take a deep breath. In most cases, it's perfectly safe to open a scam email or text. Modern mail apps, like Gmail, detect and block any code or malware from running when you open an email. The key is not to click links, or download any attachments.
- Do not download any attachments in the message. Attachments may contain malware such as viruses, worms or spyware.
- Do not click links that appear in the message. Links in phishing messages direct you to fraudulent websites.
- Do not reply to the sender. Ignore any requests from the sender and do not call any phone numbers provided in the message.
- Report it. Help fight scammers by reporting them. Forward suspected phishing emails to the Anti-Phishing Working Group at reportphishing@apwg.org. If you got a phishing text message, forward it to SPAM (7726). Then, report the phishing attack to the FTC at ftc.gov/complaint.

Heritage BANK

BANKS NEVER ASK THAT!

Call: If you receive a phone call that seems to be a phishing attempt:

- Hang up or end the call. Be aware that area codes can be misleading. If your Caller ID displays a local area code, this does not guarantee that the caller is local.
- Do not respond to the caller's requests. Financial institutions and legitimate companies will never call you to request your personal information. Never give personal information to the incoming caller.
- If you feel you've been the victim of a scam, did provide personal or financial information, contact your bank immediately at their publicly listed customer service number. Often, this is found on the back of your bank card. Be sure to include any relevant details, such as whether the suspicious caller attempted to impersonate your bank and whether any personal or financial information was provided to the suspicious caller.

What to do if you fall for a scam email, call, or text.

1. Contact Heritage Bank, and creditors
   - Speak with the fraud department and explain that someone has stolen your identity.
   - Request to close or freeze any accounts that may have been tampered with or fraudulently established.
   - Make sure to change your online login credentials, passwords and PINs.
2. Secure your email and other communication accounts
   - Many people reuse passwords and your email or cell phone account may be compromised as well.
   - Immediately change your accounts' passwords and implement multi-factor authentication – a setting that prevents cybercriminals from accessing your accounts, even if they know your password – if you haven't already done so.
3. Check your credit reports and place a fraud alert on them
   - Get a free copy of your credit report from annualcreditreport.com or call 877.322.8228.
   - Review your credit report to make sure unauthorized accounts have not been opened in your name.
   - Report any fraudulent accounts to the appropriate financial institutions.
   - Place a fraud alert on your credit by contacting one of the three credit bureaus. That company must tell the other two.
     - Experian: 888.397.3742 or experian.com
     - TransUnion: 800.680.7289 or transunion.com
     - Equifax: 888.766.0008 or equifax.com
4. Contact ChexSystems at 888.478.6536 to place a security alert on the compromised checking and savings accounts when a deposit account has been impacted.
5. Contact the Federal Trade Commission to report an ID theft incident: visit ftc.gov/idtheft or call 877.438.4338.
6. File a report with your local law enforcement
   - Get a copy of the report to submit to your creditors and others that may require proof of the crime.