Quick Security Tips to Keep You Safe!

Presented by:
Harvest Bank and the American Bankers Association

Banks will NEVER unexpectantly contact you and ask for account or personal information by text, email, or phone. If you do receive a request like this, chances are it's a scam! Every day, thousands of people fall victim to scams. Scammers are getting better and better at deceiving people. Being educated and aware is the best defense against scammers.

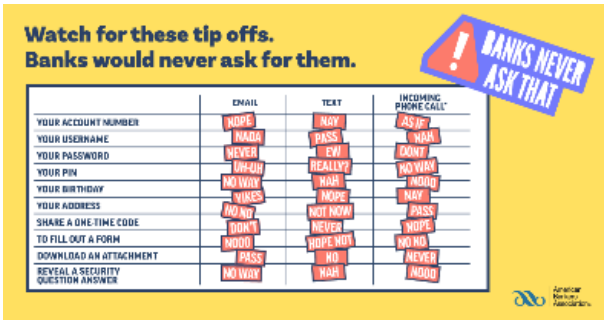
What to do if you receive an unsolicited email or text asking you to click or provide sensitive information:

- Always think BEFORE reacting
- Look for typos or phony email addresses; if those exist, it is likely a scam
- Do not download any attachments or click any links
- Do not reply to sender
- Delete the message

Business Email/Text Compromise:
Scammers can impersonate a company employee (Amazon, a financial institution, McAfee, etc.) by email or text to request a change in your account information. The email or text can look and sound very authentic. Do not respond, click links, or call any numbers associated with the email/text. Use a trusted phone number for the company and call to validate it was a legitimate request.

What to do if you receive a scam phone call:

- Do not rely on caller ID, scammers can mask their phone numbers
- Never give out sensitive information
- Do not respond to the caller's demands, even if it sounds urgent
- Hang up
- Contact Harvest Bank immediately if you feel you have shared any information with the caller



Debit Card Security:

Debit cards with Harvest Bank come equipped with Shazam fraud alerts.

- As part of our debit card protection program, you may automatically be alerted via text message when suspicious activity is detected on your debit card.
- The text message will ask you to confirm a transaction by only requiring a "yes" or "no" response; the text will NEVER ask for any more information. You must respond to the text message in order for your card to function again.
  - A "no" response will trigger the fraud process to continue and the card will be canceled.
  - A "yes" response will let Shazam know that the transaction was legitimate and the card will be unblocked.
  - If you do not reply to the text message, or your phone number on file is not a mobile number, Shazam will attempt to reach you via automated voice call.
- Harvest Bank and Shazam will NEVER unexpectantly request card or account information via text, phone, or email.

In addition to Shazam fraud alerts, Shazam Brella is available for set up free of charge for further debit card account monitoring. The Shazam Brella app is available for free download from your phone's app store.

- Get transaction alerts whenever your card is used to help you detect fraudulent activity immediately
- Turn debit card on/off to disable a lost/stolen card or cease unauthorized activity

Enhanced Online Accounts Security:

Use long, complex retainable passwords/passphrases that do not contain personal information and multi-factor authentication (MFA) when available for any account that you create. MFA requires the user to enter an additional piece of information, other than a username or password. This is an extra step in the login process to further help protect your account from hackers. Image selection and challenge questions are two examples that Harvest Bank uses with online banking.

For business customers who would like to further secure their online banking access, tokens are also available. This provides an offline option for MFA to further protect your business accounts from hackers.

What if you do get scammed?

- Contact your bank immediately to report fraudulent activity
- Monitor account activity, freeze accounts, and change online passwords or PINs
- Change email account passwords and set up MFA if scam was initiated via email
- Get a free copy of your credit report at www.annualcreditreport.com -review to make sure no fraudulent activity is occurring under your name
- Place a fraud alert with any of the three credit bureaus: Experian, TransUnion or Equifax
- Contact the FTC to report ID theft at identitytheft.gov or call 1-877-438-4338
- File a report with local law enforcement