For Businesses

Beware of Scams

Fraudsters will take advantage of customer's:

Fear of uncertainty

Government Loans

Need of quick funding

WE
CAN
HELP

Fraud Tips for Business Customers

Important Information

American Savings Bank is working hard to help address customer's need to government funding.

No Financial Institution or organization can guarantee that they can obtain early access to government funding.

Every organization needing funding must go a new application process to obtain government funding.

Do not send payments to obtain early funding or payments from government programs.

Fraud Tips: Who contacts you

The **US government** will NOT be

- Texting you (How would they have your cell number?)
- Calling you (How would they have your phone number?)
- Email (How do they know your email?)
- Most contact will be done through the U.S. Postal Service mail since that information is provided in tax filings.

American Savings Bank – if we contact you via

- Text — We will never ask for account, password/PIN information.
- Call — There should be a person on the line. We do **not** use automated calling.
- Email — Is to notify you to check your secured message box in online banking.

Your Vendors

- Know your vendors and how they normally contact you for any changes.
- If the contact method has changed, determine if a follow-up call is needed.

Fraud Tips for Business Customers

Prevention Tips – When your are contacted:

- Before responding, ask these questions:
  - Do I know the person/organization who is contacting me?
  - Is this how this person/organization normally contacts me?
  - Are they asking me for my PIN, Online banking log in and password, asking me to send money?

Beware of unsolicited calls!

Fraud Tips for Business Customers

Prevention Tips – When your are contacted:

- Thoroughly check the email address of the Email Senders
  - **On your phone**: Click on the name of the person/organization sending the email to reveal the sender's email.
  - **On you computer:** Using your mouse, hover over the name of the person sending the email to reveal the sender's email.
  - Emails can say it is from a company, but when you review it, the sender email is different. Example - email address that normally says Jdoe@123Company.com, but new email is from Jdoe@Company.com.

Fraud Tips for Business Customers

Prevention Tips – When your are contacted:

- Validate the Contact – Look up the contact's information online or through the phone book. Call that number and ask for the person.

- If at any time you are asked for private information (your account number, online banking log in an password, or card number and PIN), STOP the conversation.

Fraud Tips for Business Customers

Prevention Tips – When your are contacted:

- Contact from your Vendor requesting changes
  - Be careful of vendors asking you through an email to send invoice payment to an alternate bank account and/or beneficiary.
  - Make sure to speak to the vendor. Let them know you received and email asking you to redirect payment. Ask them to validate the change.

Fraud Tips for Business Customers

Prevention Tips – When your are contacted:

- Email request from a Executive/High level Manager in company.
  - Establish a call back verification process before releasing any company information or sending funds out.

- Beware of emails with attachments.
  - Do not open emails from senders you do not know.
  - Do not click on links or attachments with .exe extensions.
  - Suspicious emails can have virus or malware.

Fraud Tips for Business Customers

Prevention Tips for Account Fraud

Review your Account Activity/Statements regularly

- Use online banking/mobile banking to review account activity for unauthorized transactions. Review daily if possible.

- Carefully review electronic transactions (ACH, debit card transactions) posted to your account.

- Notify the Bank immediately of any unauthorized transactions.

Fraud Tips for Business Customers

Prevention Tips for Account Fraud

- Try to ensure that no one employee has the authority to oversee every process of a payment operation.
- If possible, have outgoing payments verified by second person.
- Regular review of account activity/statements by a person who does not process payments.

Internal (Employee) Fraud

- In this difficult time, company employees may be concerned about paying financial debts, which can lead to internal fraud.

Fraud Tips Business Customers

What should I do if I am a victim of Fraud?

- Contact your bank immediately for assistance
  - Provide as much information as you can about what happened.
  - If and how you were contacted and by who.
  - Indicate what information you may have given out.
  - Review account and notify bank of any unauthorized transactions.

- As applicable, file a police report.