



**BANKS NEVER ASK THAT**

**CENTURY**  
SAVINGS BANK  
— Since 1865 —

## Become an Expert Scam-Spotter

Did you know that every day thousands of people fall victim to fraudulent emails, text messages and phone calls from scammers pretending to be their bank? A 2019 fraud report conducted by The Federal Trade Commission estimated that American consumers lost \$1.48 billion to phishing scams in 2018. And these scams are on the rise as the use of online banking has increased, especially with more consumers making the switch to bank remotely due to the COVID-19 pandemic.

Century Savings Bank has partnered with the American Banking Association to promote a campaign called “Banks Never Ask That” to help raise awareness and educate our customers on how to identify and avoid these type of scams. Hackers and scammers are professional thieves, but everyone can do their part to build a defense against the fraudulent activities they use. Thankfully, there are various ways to protect yourself, your personal information and your money.

## Questions Banks **WOULD NEVER ASK**

There are a series of questions that would make sense for your bank to ask you, but the threat of an intruder can be spotted by how you are contacted and the questions that are asked by the bank representative. Banks communicate with their customers in a few ways, however it's not normal for them to send an email or text message that asks you for account information, to call them or to click on a link to avoid any account issues.

**Ask for your account number in an email?**



*example*

**“What is your bank account number?”**

**Ask you to click a link in an email?**



*example*

**“Click this link to make sure your account doesn't get compromised!”**

**Ask you to call them via text message?**



*example*

**“Please call us at 1-800-222-2222 so we can update you about some suspicious activity on your account!”**



## WATCH OUT for the Red Flags

If you receive an email, text or phone call from your bank for any of the information below, it's a definite red flag. It's better to be safe than sorry so end the call, delete the text, and trash the email, because Banks Never Ask That! You may be asked to verify confidential information if you call your bank, but never the other way around. If you receive an incoming call from someone claiming to be your bank, hang up and call the number on the back of your card.

	EMAIL	TEXT	INCOMING PHONE CALL*
YOUR ACCOUNT NUMBER	NOPE	NAY	AS IF
USERNAME OR PASSWORD	NADA	PASS	NAH
YOUR SSN	NEVER	EW	DON'T
YOUR PIN	UH-UH	REALLY?	NO WAY
YOUR BIRTHDAY	NO WAY	NAH	NOOO
YOUR ADDRESS	YIKES	NOPE	NAY
CLICK A LINK OR TYPE A URL	NO NO	NOT NOW	PASS
FILL OUT A FORM	DON'T	NEVER	NOPE
DOWNLOAD AN ATTACHMENT	NOOO	HOPE NOT	NO NO
CALL THEM AT A NEW NUMBER	PASS	NO	NEVER

## TIPS to Help Avoid Falling for these Scams

**Beware of Links.** Banks will never send you a text or email that asks you to click a link. If you receive this type of message, don't respond – just delete it and call your bank to confirm they didn't send it.

**Beware of Scare Tactics.** Some scams pressure or even threaten you to respond, but don't! Instead, call your bank to see if it's a scam or not.

**Protect your Confidential Information.** Your bank will never ask for your account number, social security number, name, address or password in an email or text message. They will only ask you to provide this information to verify your identity when you call them directly.

**Call the Number on your Card.** If you receive an email, text or call and you have suspicions, play it safe by calling the number on the back of your card to speak to someone at your bank about the message you received.

**Watch for Misspelled Words.** It's very common to find typos in a fraudulent text or email. If you find one in the message, you know it's a scam!



## WHAT TO DO if You Fall for a Scam

**Contact your bank, financial institutions, creditors and others.** Speak with the fraud department and explain that your identity or personal data may have been compromised. Request to close or freeze any accounts that may have been targeted and immediately change your online login credentials, passwords and PINs. Contact **ChexSystems** at 888-478-6536 to place a security alert on the checking and savings accounts that have been impacted and report an identity theft incident to the **Federal Trade Commission** at: [ftc.gov/idtheft](https://www.ftc.gov/idtheft) or 877-438-4338.

**Secure your email and other communication accounts.** Many people use the same password for multiple accounts such as email and cell phone accounts. And even if you don't, once one account is hacked it can be easy for a criminal to get into your other accounts. Immediately change any account passwords and, if you haven't already done so, implement multi-factor authentication — a setting that prevents cybercriminals from accessing your accounts even if they know your password.

**Check your credit reports and place a fraud alert on them.** Get a free copy of your credit report from [annualcreditreport.com](https://annualcreditreport.com) or call 877-322-8228. Review your credit report to make sure unauthorized accounts have not been opened in your name and report any fraudulent accounts to the appropriate financial institutions. Place a fraud alert on your credit by contacting one of the three credit bureaus and that company will inform the other two.

- **Experian:** 888-397-3742 or [experian.com](https://www.experian.com)
- **TransUnion:** 800-680-7289 or [transunion.com](https://www.transunion.com)
- **Equifax:** 888-766-0008 or [equifax.com](https://www.equifax.com)

**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.

Do you think you can outsmart online scammers? Take this [quiz](#) to see how you score and you will also be entered to win a prize, courtesy of the American Bankers Association.

To do our part as your trusted financial partner, we will frequently share content and resources to help you become an expert scam-spotter! Together we can reduce the financial impact these crimes have on consumers and the banking industry.

If you believe your personal information has been compromised or you think you are a victim of identity theft, we're here to help! Please call our Operations Department at **844.9CSB4ME** Monday to Friday from 8:30 am to 5:00 pm.

Rest assured, we're here for you when you need us. As always, we appreciate your trust and confidence in Century Savings Bank.