How good are you at spotting Scams?

It may be a scam if....

Lottery Scam

You receive a letter and counterfeit check in the mail explaining you won a lottery and that you need to cash the check to pay your taxes on the winnings.

Tech Support Scam

You receive a phone call or email telling you that your computer has a virus and that a technical support person needs access to your computer. As soon as you follow their instructions, they will have access to your entire computer and will try to steal data, install malware, or access your online banking account to steal funds.

Unexpected Check Scam

You receive an unexpected check in the mail and are asked to cash it and send a portion or all of it back to an unknown individual.

Investment Scam (AKA Pig Butchering)

You receive a message on a dating or social media site from someone explaining how you can get rich with an investment (i.e., crypto, stocks, etc.) Once you transfer money, they'll tell you that your investment is doing great, but as soon as you attempt to cash out, you'll be told you have to pay a fee or that your investments cannot be sold.

Mobile Deposit Scam

You provide a fraudster access to your mobile banking app so they can deposit counterfeit checks. Once they do, they'll ask you to withdraw funds and transfer it using a third-party money transfer app (i.e., Zelle, CashApp, Venmo, etc.).

Adoption Fraud Scam

There are some unethical adoption providers that attempt to deceive and defraud prospective adoptive parents by either double matching families, fabricating a match, and/or asking for exorbitant upfront fees – but fail to provide services promised.

Virtual Kidnapping Scam

You receive a phone call in which the fraudster states your family member is being held captive and for them to be released, you need to transfer funds. In many of these scams, you will hear screaming or pleas for help in the background in an attempt to make believable.

Job Scam

You're lured to apply for a job then asked to pay upfront fees for required job equipment. Or they ask for your account info and send you stolen money with instructions to send to cryptocurrency wallets.

Bank Impersonation Scam

You receive a phone call or email impersonating a representative from your bank informing you of a discovered issue or fraud occurring inside the bank. The fraudster instructs you to close your account and deposit the funds at a secure ATM that accepts cryptocurrency so you can transfer it to a digital wallet.

Government Impersonation Scam

You receive a phone call or email claiming to be a state or federal official threatening you with prison time if you don't send them money to pay past due taxes or bail via a third-party transfer app (i.e., Zelle, CashApp, Venmo, etc.)

Romance Scam

You receive a message on a dating or social media site in which a fraudster befriends you only to ask for money to help them out.

Disaster Fraud Scam

When a high-profile disaster happens, you may receive emails, phone calls, or see social media posts asking for charity donations – do your research & check their website before donating to any charity!

TSB Torrington Savings Bank

TorringtonSavings.Bank
(860) 496-2152

MEMBER FDIC
EQUAL HOUSING LENDER

REV. SEP 2024

FREQUENTLY ASKED QUESTIONS

What should I do if I'm a victim of identity theft or a scam by either transferring money or giving access to my online/mobile banking account?

If you feel that you may be a victim of identity theft or a financial fraud scam, you should contact your financial institutions. If you are a customer of Torrington Savings Bank, please immediately contact our Customer Care Center by calling 860-496-2152.

What can I do to help protect my credit if I'm worried about being a victim of identity theft?

Customers of TSB can take advantage of our free credit monitoring tool - CreditSense. CreditSense is accessible in online & mobile banking.

Otherwise, you can freeze your credit by contacting the three major credit reporting agencies and submit a request online, by phone, or by mail.

- **Equifax** (Equifax.com)
- **Experian** (Experian.com)
- **TransUnion** (Transunion.com)

What should I do if I receive a suspicious email, phone call, or text message that claims it is from my financial institution?

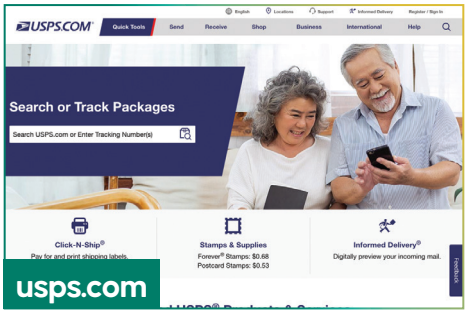
If you're unsure that the email, phone call, or text message is legitimate, it's best to hang up or not respond. If you are a customer of Torrington Savings Bank, please immediately contact our Customer Care Center by calling 860-496-2152 and explain your situation so you can be assisted.

How can I better protect myself from all these scams?

In most cases, criminals are attempting to use emotional triggers, such as fear, urgency, and greed to coerce you into performing an action (i.e., transferring funds or providing sensitive financial information) before giving you adequate time to think. The best way to prevent becoming a scam victim is to research the legitimate email or phone number for your institution by manually typing the website into your navigation bar. This will help ensure that you are speaking to a true representative at your institution so you can confirm if any suspicious activity exists on your account(s).

Other Helpful Resources:

Internet Crime Complaint Center – If you fell victim to a scam and transferred money via a wire, virtual currency, or money order, you should immediately file a complaint within the first 24 hours to the IC3 as they can help recover your assets.



U.S. Postal Service – You can sign up for "Informed Delivery" which will allow you to receive email alerts for mail that is being delivered to your mailbox. This can help you identify if mail has been stolen, such as checks, that can be used by fraudsters to try and steal money from you.

Federal Trade Commission – If you have been a victim of identity theft, you can report it to the Federal Trade Commission and receive helpful information to recover from being a victim.

Torrington Savings Bank

TorringtonSavings.Bank
(860) 496-2152

MEMBER FDIC
EQUAL HOUSING LENDER

REV. SEP 2024