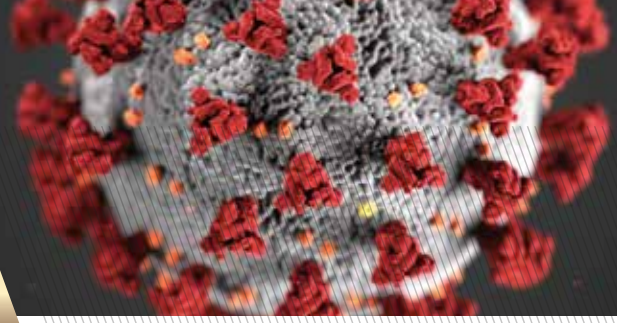
AVOID
CORONAVIRUS SCAMS



Scams related to the Coronavirus are spreading as fast the virus itself.

CENTURY SAVINGS BANK
Since 1865

In times like these, scammers will often take advantage of unsuspecting customers. Fraudsters are already setting up fraudulent websites and sending fake emails, texts, and social posts – all in an effort to compromise your personal information. While we use some of the most sophisticated security measures available to protect you and your money, you need to be aware of certain scams that can put you at risk.

Beware of Stimulus Check Scams

Experts say scammers will attempt to separate you from your stimulus in the coming weeks and recommend treating every call or email with suspicion. If you have questions, go right to the source.

The stimulus checks from the Federal Government are coming – but remember that the government WILL NOT contact you asking for your social security number, bank account or credit card information. And, you do not need to fill out an application to receive your check. So, any text or email asking you to do so is not legitimate.

Don't respond to texts and emails about checks from the government. The details are still being worked out. Anyone who tells you they can get you the money now is a scammer.

Ignore Robocalls trying to Profit from Coronavirus-related Fears

Criminals are using this outbreak to try to take advantage of people through misinformation and scare tactics. They're targeting small business owners, scaring them into buying counterfeit online listing services. They're also going after seniors, trying to sell them fake coronavirus tests and products.

In one scam robocall example on the FTC website, the caller says, "Because of the limited testing we are first taking medicare members. Will the free at home tests be just for you or for you and your spouse?"

In another example the caller says, "This is a call from the Social Security Administration. During these difficult times of coronavirus we regret to inform you we have gotten an order to suspend your socials immediately within 24 hours."

If you do get one of these calls, the FTC advises you to **hang up and not to press any numbers** if you're asked to do so. You should also consider using a call blocking app or device, or you can reach out to your phone provider to ask about call blocking tools.

If you do get this type of call, report it on the FTC website.

It's not just phone calls you should be leary of. Scammers changes their methods frequently.

"Whether it's phone, text, email or social media, please stop and think before you provide information, financial or otherwise, or even click on a link," Paula Fleming of the Better Business Bureau said. “These scammers are trying to get your personal information or trick you into downloading malware to your devices, which opens you up to identity theft and ransomware attacks. The Better Business Bureau has also heard from people who have lost money ordering fake Covid-19 testing kits, face masks and home cures from fraudulent sites.”

Be on the lookout for phony updates, testing, vaccines, and treatments

Watch out for emails claiming to be from the Centers for Disease Control and Prevention (CDC) or experts saying they have information about the virus, and beware of fake online coronavirus updates and bogus offers for vaccinations.

For the most reliable and up-to-date information about the Coronavirus, visit these websites:

- Centers for Disease Control and Prevention (CDC)
- World Health Organization (WHO)
- coronavirus.gov

Always do your research before making any donation or wiring funds

Be wary of fake charities. If you want to donate money to a charity, make sure you’re familiar with the organization. Do your homework when it comes to donations, whether through charities or crowdfunding sites. Don’t let anyone rush you into making a donation; and never wire funds or send cash or gift cards.

Wire Fraud – Given the remote working conditions that most businesses are now faced with, it’s important for companies to maintain dual control of their outgoing wires. If you receive an email request to send a wire (even if it appears to be from someone who usually makes these requests), call that person to confirm it did, in fact, come from them. The same vigilance should be used with all money transactions.

Tips to help you keep the scammers at bay

Hang up on robocalls. Don’t press any numbers. Scammers are using illegal robocalls to pitch everything from scam Coronavirus treatments to work-at-home schemes. The recording might say that pressing a number will let you speak to a live operator or remove you from their call list, but it might lead to more robocalls instead.

Ignore online offers for vaccinations and home test kits. Scammers are trying to get you to

buy products that aren't proven to treat or prevent the Coronavirus disease 2019 (COVID-19) — online or in stores. At this time, there also are no FDA-authorized home test kits for the Coronavirus. Visit the FDA to learn more.

Fact-check information. Scammers, and sometimes well-meaning people, share information that hasn't been verified. Before you pass on any messages, contact trusted sources. Visit What the U.S. Government is Doing for links to federal, state and local government agencies.

Know who you're buying from. Online sellers may claim to have in-demand products, like cleaning, household, and health and medical supplies when, in fact, they don't.

Never click on unfamiliar links, attachments or pop-up screens from sources you don't recognize. Phishing scams use fraudulent emails and websites to trick you into disclosing private account or login information, or to deliver viruses or malware onto your computer system or device.

Be careful when providing personal information. Don't give out your personal information over the phone, through the mail or over the Internet unless you initiated the contact or are sure you know who you are dealing with. **PLEASE NOTE: if Century Savings Bank contacts you, we will never ask you for personal or confidential information such as your password, account number or personal identification number (PIN).**

Keep personal information personal. Hackers can use social media profiles to figure out your passwords and answer those security questions in the password reset tools.

- Lock down your privacy settings and avoid posting birthdays, addresses, mother's maiden name, etc.
- Be wary of requests to connect from people you do not know.
- Avoid storing sensitive information like passwords or social security numbers on your mobile device.

We're here to help.

Century Savings Bank is proud to stand alongside our customers during these uncertain times. Our branch associates and Operations Department are staffed and ready to assist you as needed.

We'll continue to monitor the situation as it develops and provide the latest updates on centurysb.com.

Questions or Concerns?

If you have any questions or concerns about fraud prevention during this time, 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.