BankOnITUSA®

INFORMATION SECURITY BRIEF

SEPTEMBER 2021

4 WAYS TO SPOT A SCAM

THEY COME AS FRIENDS
Frauds typically act like they are contacting you on behalf of the government or a company that you know, like a utility, a tech company, or even a charity soliciting donations.

YOU'VE EITHER WON OR YOU'RE IN TROUBLE
Some scammers try to scare you into thinking you are in trouble with the government, like you owe the IRS. Perhaps they say a family member is having an emergency, your computer has a virus, or there's a problem with your account — all they need is to verify some personal info. On the flipside, they may congratulate you on winning a lottery or contest, but they need a fee so you can claim your prize.

YOU HAVE TO ACT NOW
Scammers want to get your info before you have time to second-guess yourself. They don't want you to have time to double-check their story. They might even threaten to arrest or sue you.

ONLY ONE WAY TO PAY
Scammers often insist that you send money through a transfer company or put money on a gift card. Others will send you a fake check, tell you to deposit it, and then send them money.

BankOnIT's Information Security E-Newsletter is now Information Security Brief. The publication is still intended to keep you informed about ways to protect yourself and your bank from threats to information security.

In Case of Emergency

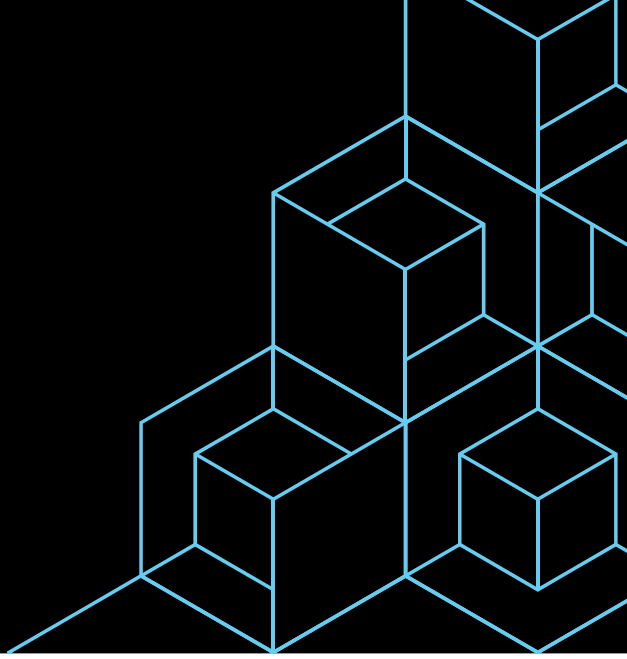
Scammers target recent victims of natural disasters – don't let them add insult to injury

October is the time we start to look forward to trick-or-treaters — but the real tricksters don't wait for Halloween. Scam artists work year-round trying to snatch personal information and bilk you out of your hard-earned money. And a particularly callused kind of scammer is targeting people at their most vulnerable moment: while trying to recover from a natural disaster.

These days, hurricanes, wildfires, tornados, floods, and even earthquakes seem like a weekly occurrence, completely upending the lives of people living in harm's way. But while there isn't much we can do to defend against mighty Mother Nature, there are key steps we can take to protect ourselves against opportunists who would add insult to our injury. The Federal Trade Commission has recently outlined several ways to avoid the most common post-disaster scams:

- **Be wary of anyone promising quick clean-up and debris removal:** Some scammers may quote prices that are too high, require payment before doing the job, or just lack the necessary skills to do the job properly.
- **Check them out:** Before you hire someone for clean-up, ask for ID, credentials, licenses, and proof of insurance. Get any promises in writing.
- **Make any payment traceable:** Avoid wire transfers, gift cards, cryptocurrency, or paying in cash. And always wait until the job is done to your satisfaction before making payment.
- **Safeguard your personal info:** No legitimate agent will claim to be a government official and then demand you credit card, bank account, or Social Security information.

INFORMATION SECURITY BRIEF



- **No application fees:** FEMA doesn't require them. If someone asks for money to help you qualify for government relief funds, it's probably a scam.
- **Watch out for rental listing scams:** If you need to temporarily rent or lease a property, stay away from people who ask you to wire money or ask for security deposits or rent before you've met or signed a lease.
- **Spot disaster-related charity scams:** Even if you haven't been impacted by a disaster, you might want to help those who have. Check out the FTC's advice on donating wisely and avoiding charity scams.

The FTC suggests several steps you can take to avoid this or any other type of scam.

- Block unwanted calls and text messages on your phone.
- Do not give out your personal or financial info in response to an unexpected request.
- Resist any pressure to act immediately.
- Never pay someone who insists you do so via gift car or by using a money transfer service.

And if you suspect a scam or think you or someone you know has been victimized, contact the FTC at www.ReportFraud.ftc.gov. You can also sign up for the FTC's consumer alerts about the latest reported frauds and scams.