Mobile Banking App is HERE!

UNION BANK

April 2022

4 Tricks Phone Scammers Are Using In 2022 – And How To Stop Them

EQUAL HOUSING LENDER Member FDIC

This tax season, stop scammers with free tools to identify and block potential threats.

Whether you're about to sit down to dinner, catching up with an old friend or simply taking a well-deserved nap, an unwanted robocall always seems to disrupt your day at the most inconvenient time.

But unwanted robocalls and scams are more than just annoying interruptions; they can actually be dangerous. Last year, the volume of scam call attempts exploded to record highs. They were the top complaint reported to the FCC and Americans lost some $30 billion to these ploys.

If you're concerned, or even just annoyed, you should be. There was a 116% increase in scam attempts last year alone, according to new network data reported by T-Mobile, and the bombardment of calls is set to soon pass pre-pandemic levels.

Despite efforts across the wireless industry, the tactics used by bad actors around the globe have become more aggressive over time and even more deceptive in their efforts to appear legitimate. Scammers are relentless – and they are not going to stop as long as they keep making money.

At the end of 2021, T-Mobile released its first-ever Scam and Robocall Report, which identified trends across the country, insights into scammer behavior and ways the company responded. T-Mobile's Scam Shield technology, for example, identified or blocked more than 21 billion scam calls for their customers in 2021 – more than double the number of calls in 2020. That's roughly the equivalent of 700 spam calls every second.

The T-Mobile report also shared some of the most common phone scams and ways to protect your information.

1. 'Neighborhood' calls

One location-based trick scammers use is called neighbor or neighborhood spoofing, in which they disguise their number to appear as if it is coming from a local number, using a similar area code or prefix to your number.

Continued on Page 2

Middlebourne Office
103 Dodd Street Middlebourne, WV 26149
304-758-2191

Sistersville Office
700 Wells Street Sistersville, WV 26175
304-652-3511

St. Marys Office
401 Second Street St. Mary's, WV 26170
304-684-2427

Hundred Office
3924 Hornet Hwy, Hundred WV 26575
304-775-2265

Ellenboro Office
90 Main Street Ellenboro, WV 26346
304-869-3232

Harrisville Office
1500 E. Main Street Harrisville, WV 26362
304-643-2974

Pennsboro Office
214 Masonic Ave. Pennsboro, WV 26415
304-659-2964

Marietta-Loan Production
Kroger Plaza 19 Acme Street Marietta, OH 45750
740-374-0010
This is not a full service location. Deposits/withdrawals cannot be processed at this location.

New Martinsville Office
638 N SR 2 New Martinsville, WV 26155
304-455-2967

T-Mobile's Scam and Robocall Report found certain areas of the country are more heavily targeted by scam calls than other parts. The states with the highest volume of scam call attempts in 2021 were Texas, Florida, Arizona and Georgia. Among those, Dallas/Fort Worth was the top metro area for receiving scam calls.

2. Legitimate businesses scams: fake auto warranties

One of the biggest concerns heading in to 2022 is scammers posing as legitimate businesses. If you've gotten a call from someone regarding your car's warranty, you're already familiar with this one. In 2021, the top scam was fake auto warranties, making up 51% of all scam call attempts.

Other common fraudulent calls were from individuals pretending to represent car insurance companies (6%), social security (10%), wireless providers (9%) and package delivery (4%).

What is particularly concerning about scams like the auto warranty scam is the caller may already have some personal details about your car or warranty. These calls often start with a robocall instructing you to press a number and stay on the line.

3. Time of year: tax season and health care scams

Scammers are savvy and will capitalize on seasonal events to ramp up call attempts. With tax season [here], phone scammers will often prey on people's anxiety surrounding their taxes.

To keep yourself protected, know that generally, the IRS will first mail a bill to any taxpayer who owes taxes. They also won't call about an unexpected tax refund. If you receive a call requesting immediate payment in the form of gift cards, threatening to bring in law enforcement for unpaid bills, or demanding payment without a bill or opportunity to question the amount, stay alert – it's likely a scam.

Similarly, scam calls relating to health care spiked during open enrollment for health insurance and Medicare in late fall and winter.

4. Technical support calls

Another avenue scammers use to weasel their way in is fake technical support calls. These calls can result in cyber criminals getting access to your data or planting malicious code on your phone or computer.

Fake technical support calls will often begin with the scammer saying they're with a well-known company and that an issue has been detected with your device. From there, they'll walk you through various steps to "fix" your phone or computer. Don't be fooled – scammers who pull this trick will be attempting to download dangerous software used to obtain your data.

As long as scammers are still able to make money off unsuspecting victims, their tactics will keep evolving. Thankfully, the technology used to protect people from these cyber criminals will continue to advance, as well – that's why it's crucial to utilize scam protection software to protect yourself.

Source: ***Cemile Kavountzis, for T-Mobile, Published 9:00 a.m. ET February 10, 2022***

Fraud Alert: COVID-19 Scams

The U.S. Department of Health and Human Services Office of Inspector General is alerting the public about fraud schemes related to the novel coronavirus (COVID-19). Individuals are using testing sites, telemarketing calls, text messages, social media platforms, and door-to-door visits to perpetrate COVID-19-related scams.

Fraudsters are offering COVID-19 services in exchange for personal details, including Medicare information. **However, these services are unapproved and illegitimate.**

These scammers use the coronavirus pandemic to benefit themselves, and beneficiaries face potential harm. The personal information collected can be used to fraudulently bill federal health care programs and commit medical identity theft.

Protect Yourself

- Be cautious of any COVID-19 testing site that requires your financial or medical information in order to receive a free test.
- Be mindful of advertisements for COVID-19 testing or treatments on social media platforms. If you make an appointment for a COVID-19 test online, make sure the location is an approved testing site. We encourage the public to check official government websites for a list of approved COVID-19 testing sites.
- Be careful! Scammers are selling fake and unauthorized at-home COVID-19 test kits in exchange for your personal or medical information. Make sure to purchase FDA approved COVID-19 test kits from legitimate providers.
- Do not purchase or reproduce fake COVID-19 proof of vaccination cards, and do not fill-in blank vaccination cards with false information.
- Offers to purchase COVID-19 vaccination cards are scams. Valid proof of COVID-19 vaccination can only be provided to individuals by legitimate providers administering vaccines.
- Photos of COVID-19 vaccination cards should not be shared on social media. Posting content that includes your date of birth, health care details or other personally identifiable information can be used to steal your identity.
- As volunteers go door-to-door to inform communities across the country about COVID-19 vaccines, be sure to protect yourself from criminals who are seeking to commit fraud. Do not provide personal, medical, or financial details to anyone in exchange for vaccine information, and obtain vaccinations from trusted providers.
- Be cautious of COVID-19 survey scams. Do not give your personal, medical, or financial information to anyone claiming to offer money or gifts in exchange for your participation in a COVID-19 vaccine survey.
- Be mindful of how you dispose of COVID-19 materials such as syringes, vials, vial container boxes, vaccination record cards, and shipment or tracking records. Improper disposal of these items could be used by bad actors to commit fraud.
- Beneficiaries should be cautious of unsolicited requests for their personal, medical, and financial information. Medicare will not call beneficiaries to offer COVID-19 related products, services, or benefit review.
- Be suspicious of any unexpected calls or visitors offering COVID-19 tests or supplies. If you receive a suspicious call, hang up immediately.
- Do not respond to, or open links in, text messages about COVID-19 from unknown individuals.
- Do not give your personal or financial information to anyone claiming to offer HHS grants related to COVID-19.
- Be aware of scammers pretending to be COVID-19 contact tracers. Legitimate contact tracers will never ask for your medical or financial information or attempt to set up a COVID-19 test.
- If you suspect COVID-19 health care fraud, report it immediately online or call 800-HHS-TIPS (800-447-8477).

Source: ***U.S. Department of Health and Human Services Office of Inspector Gen-***