Mobile Banking App is HERE!

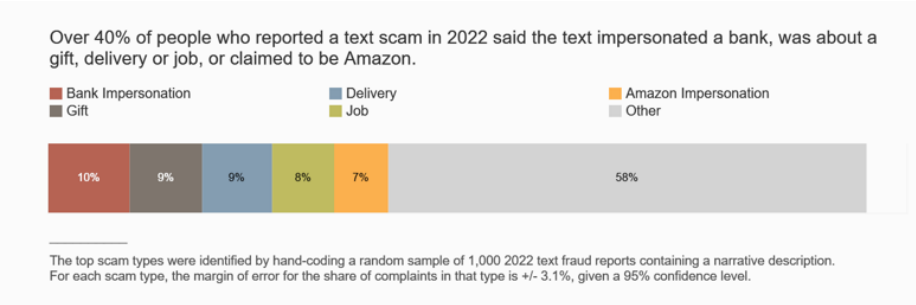
UNION BANK

July 2023

Can You Spot the 5 Most Common Text Message Scams?

According to reports in the FTC's Consumer Sentinel database, text message scams took consumers for $330 million in 2022. The latest Consumer Protection Data Spotlight focuses on this form of fraud. With reported losses more than doubling in 2021 and nearly five times what people reported in 2019, would you be able to spot the five most common text message scams?

First, some background about what may be behind the proliferation of this form of fraud. It's estimated that text message open rates are as high as 98%, compared to email open rates of 20% – and they cost next to nothing to send. So people may have grown accustomed to responding to that ping with an automatic click. The growth of text scams should be of particular concern to businesses. Aside from the fact that your family and friends may be among the consumers who have reported median personal losses of $1,000, a lot of the messages take on a distinctly "office-y" tone that may target staff – fake deliveries, bogus job offers, and the like. It should also concern businesses that scammers often do their dirty work by stealing the names of well-known companies, with 51% of reports of text fraud categorized in Consumer Sentinel as business imposters.



The Data Spotlight focuses on these five common text message scams:

1. Copycat bank fraud prevention alerts. According to the Data Spotlight, reports about texts impersonating banks are up nearly twentyfold since 2019 with median reported individual losses of $3,000 last year. People get a text supposedly from a bank asking them to call a number ASAP about suspicious activity or to reply YES or NO to verify whether a transaction was authorized. If they reply, they'll get a call from a phony "fraud department" claiming they want to "help get your money back." What they really want to do is make unauthorized transfers. What's more, they may ask for personal information like Social Security numbers, setting people up for possible identity theft.

2. Bogus "gifts" that can cost you. What about those texts claiming to be from a well-known company offering a free gift or reward? If people click the link and use their credit card to cover the small "shipping fee," they've just handed over their account information to a scammer. Reports to Consumer Sentinel tell us that fraudulent charges are likely to follow.

3. Fake package delivery problems. On any given day, what home or business *isn't* expecting a delivery? Scammers understand how our shopping habits have changed and have updated their sleazy tactics accordingly. People may get a text pretending to be from the U.S. Postal Service, FedEx, or UPS claiming there's a problem with a delivery. The text links to a convincing-looking – but utterly bogus – website that asks for a credit card number to cover a small "redelivery fee."

Continued on Page 2

EQUAL HOUSING LENDER Member FDIC

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

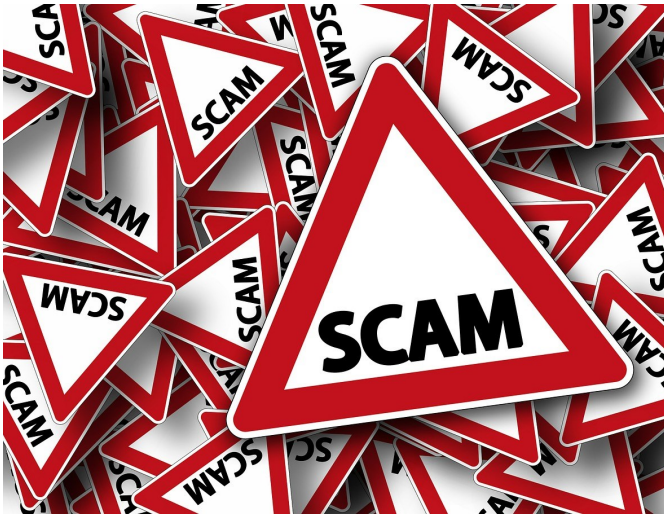
Ellenboro Office
90 Main Street Ellenboro, WV 26346
304-869-3232

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



4. Phony job offers. With workplaces in transition, some scammers are using texts to perpetrate old-school forms of fraud – for example, fake "mystery shopper" jobs or bogus money-making offers for driving around with cars wrapped in ads. Other texts target people who post their resumes on employment websites. They claim to offer jobs and even send job seekers checks, usually with instructions to send some of the money to a different address for materials, training, or the like. By the time the check bounces, the person's money – and the phony "employer" – are long gone.

5. Not-really-from-Amazon security alerts. People may get what looks like a message from "Amazon," asking to verify a big-ticket order they didn't place. Concerned about the security of their account, people call the number in the text and are connected to a phony Amazon rep who offers to "fix" their account. But oopsie! Several zeroes are mistakenly added to the "refund" and the "operator" needs the caller to return the overpayment, often in the form of gift card PIN numbers.

According to the Data Spotlight, reporting can help stop scam text messages. Forward the text to 7726 (SPAM). This helps your wireless provider block similar messages. Report it on either the Apple iMessages app or Google's Messages app for Android users. And report it to the FTC at ReportFraud.ftc.gov.

Here is additional advice for you:

- Don't click on links or respond to unexpected texts. If you aren't sure if a text legit, contact the company directly using a phone number or website you know is real – for example, the 24-hour toll-free number on the back of your credit or bank card. Don't use the information in the text message.
- Filter unwanted texts before they reach you. The FTC has advice on blocking unwanted texts.

Sources/Credit:
Article: Lesley Fair, June 8, 2023, FTC.gov
Images: Chart: FTC.gov; Traffic Sign: Author: geralt, Attribution: Pixabay, License Details: Pixabay Terms of Service; Traffic Signs Attention A Notice royalty-free stock illustration. Free for use & download

What To Do if You Were Scammed

Scammers can be very convincing. They call, email, and send us text messages trying to get our money or sensitive personal information — like our Social Security or account numbers. And they're good at what they do. Here's what to do if you paid someone you think is a scammer or gave them your personal information or access to your computer or phone. If you paid a scammer, your money might be gone already. No matter how you paid, it's always worth asking the company you used to send the money if there's a way to get it back.

Here are some steps to take if you unwittingly paid a scammer:

Did you pay with a credit card or debit card?

Contact the company or bank that issued the credit card or debit card. Tell them it was a fraudulent charge. Ask them to reverse the transaction and give you your money back.

Did a scammer make an unauthorized transfer from your bank account?

Contact your bank and tell them it was an unauthorized debit or withdrawal. Ask them to reverse the transaction and give you your money back.

Did you pay with a gift card?

Contact the company that issued the gift card. Tell them it was used in a scam and ask them to refund your money. Keep the gift card itself, and the gift card receipt.

Did you send a wire transfer through a company like Western Union or MoneyGram?

Contact the wire transfer company. Tell them it was a fraudulent transfer. Ask them to reverse the wire transfer and give you your money back.

- MoneyGram at 1-800-926-9400
- Western Union at 1-800-448-1492
- Ria (non-Walmart transfers) at 1-877-443-1399
- Ria (Walmart2Walmart and Walmart2World transfers) at 1-855-355-2144

Did you send a wire transfer through your bank?

Contact your bank and report the fraudulent transfer. Ask them to reverse the wire transfer and give you your money back.

Did you send money through a money transfer app?

Report the fraudulent transaction to the company behind the money transfer app and ask them to reverse the payment. If you linked the app to a credit card or debit card, report the fraud to your credit card company or bank. Ask them to reverse the charge.

Did you pay with cryptocurrency?

Cryptocurrency payments typically are not reversible. Once you pay with cryptocurrency, you can only get your money back if the person you paid sends it back. But contact the company you used to send the money and tell them it was a fraudulent transaction. Ask them to reverse the transaction, if possible.

Did you send cash?

If you sent cash by U.S. mail, contact the U.S. Postal Inspection Service at 877-876-2455 and ask them to intercept the package. To learn more about this process, visit USPS Package Intercept: The Basics.

If you used another delivery service, contact them as soon as possible.

For more information, check out the FTC's Consumer Advice website.

Are Public Wi-Fi Networks Safe? What You Need To Know

Public Wi-Fi networks, or hotspots, in coffee shops, malls, airports, hotels, and other places are convenient. In the early days of the internet, they often weren't secure. But things have changed. Here's what you need to know about your safety when you connect to a public Wi-Fi network.

How You Know Your Information Is Safe When You're Using a Public Wi-Fi Network

When you connect to a website, information travels from your device to the website. That could include sensitive data like the log in information for your financial, email, or social media accounts.

In the past, if you used a public Wi-Fi network to get online, your information was at risk. That's because most websites didn't use encryption to scramble the data and protect it from hackers snooping on the network.

Today, most websites **do** use encryption to protect your information. Because of the widespread use of encryption, connecting through a public Wi-Fi network is usually safe.

How do you know your connection is encrypted? Look for a lock symbol or https in the address bar to the left of the website address. This works on a mobile browser, too. It can be hard to tell if a mobile app uses encryption, but the majority do.

Best Practices for Protecting Your Personal Information Online

No matter how you get online, it's always a good idea to take some steps to protect your personal information. Start with these.

Protect your online accounts and devices

Create and use strong passwords and turn on two-factor authentication when it's available.

If you use a computer to get online, make sure your security software, operating system, and internet browser are up to date. Update your phone's operating system, too. And turn on automatic updates to keep up with the latest protections.

Recognize scammers

Scammers pretend to be someone they're not, like a representative from a well-known company or the government, to rip you off or steal your personal information. They also create fake websites and encrypt them to make you think they're safe when they're not. If you visit a scammer's website, your data may be encrypted on its way to the site, **but it won't be safe from scammers operating the site**.

Report Scammers

Report scammers to the FTC at ReportFraud.ftc.gov.

Sources: Article: FTC.gov Consumer Advice, February 2023

Image: Creator: User ID: 472301; Attribution: Pixabay; License Details: Pixabay Terms of Service; Wireless Technology Three Dimensional Shape royalty-free stock illustration. Free for use & download