



&



WHAT TO DO

if you've been scammed

originally published by the Federal Trade Commission



FEDERAL TRADE COMMISSION
CONSUMER ADVICE

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.

IF YOU 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





&



WHAT TO DO

if you've been scammed

continued from page 1

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.

IF YOU GAVE A SCAMMER YOUR PERSONAL INFORMATION

Did you give a scammer your Social Security number?

Go to IdentityTheft.gov to see what steps to take, including how to monitor your credit.

Did you give a scammer your username and password?

Create a new, strong password. If you use the same password anywhere else, change it there, too.

IF A SCAMMER HAS ACCESS TO YOUR COMPUTER OR PHONE

Does a scammer have remote access to your computer?

Update your computer's security software, run a

scan, and delete anything it identifies as a problem. Then take other steps to protect your personal information.

Did a scammer take control of your cell phone number and account?

Contact your service provider to take back control of your phone number. Once you do, change your account password.

Also check your credit card, bank, and other financial accounts for unauthorized charges or changes. If you see any, report them to the company or institution. Then go to IdentityTheft.gov to see what steps you should take.

REPORT A SCAM TO THE FTC

When you report a scam, the FTC can use the information to build cases against scammers, spot trends, educate the public, and share data about what is happening in your community. If you experienced a scam – or even spotted one, report it to the FTC at ReportFraud.ftc.gov.

Check out what's going on in your state or metro area by visiting ftc.gov/exploredata.

