FEDERAL TRADE COMMISSION

Consumer Information

consumer.ftc.gov

What To Do if You Were Scammed

Find out what to do if you paid someone you think is a scammer, gave them some personal information, or if they have access to your phone or computer.

- If You Paid a Scammer (#Paid)
- If You Gave a Scammer Your Personal Information (#PI)
- If a Scammer Has Access to Your Computer or Phone (#Access)
- Report a Scam to the FTC (#Report)

Scammers can be very convincing. They call, email, and send us text messages trying to get our money or our sensitive personal information — like our Social Security number 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.

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 (https://www.consumer.ftc.gov/articles/0219-disputing-credit-card-charges) or debit card (https://www.consumer.ftc.gov/articles/0213-lost-or-stolen-credit-atm-and-debit-cards#Limit). 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 (https://www.consumer.ftc.gov/articles/0196-automatic-debit-scams). 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 (https://www.consumer.ftc.gov/articles/paying-scammers-gift-cards#Report). Tell them it was used in a scam and ask if they can 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 (https://www.consumer.ftc.gov/articles/0090-using-money-transfer-services). Tell them it was a fraudulent transfer. Ask them to reverse the wire transfer and give you your money back. • MoneyGram at 1-800-MONEYGRAM (1-800-666-3947) • Western Union at 1-800-325-6000
Did you send a wire transfer through your bank?	Contact your bank and report the fraudulent transfer. Ask if they can 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 (https://www.consumer.ftc.gov/articles/mobile-payment-apps-how-avoid-scam-when-you-use-one) and ask if they can 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 if they can reverse the charge.
Did you pay with cryptocurrency?	Contact the company you used to send the money and tell them it was a fraudulent transaction. Ask to have the transaction reversed, if possible.
Did you send cash?	If you sent it 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 (https://faq.usps.com/s/article/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 (https://www.identitytheft.gov/) to see what steps you should take, including how to monitor your credit.
Did you give a scammer your username and password?	Create a new, strong password (https://www.consumer.ftc.gov/articles/0009-computer-

	security#passwords). 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 (https://www.consumer.ftc.gov/articles/0009-computer-security), run a scan, and delete anything it identifies as a problem. Then take other steps to protect your personal information (https://www.consumer.ftc.gov/articles/0272-how-keep-your-personal-information-secure).
Did a scammer take control of your cell phone number and account?	Contact your service provider to take back control of your phone number (https://www.consumer.ftc.gov/blog/2019/10/sim-swap-scams-how-protect-yourself). 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 (https://www.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 were scammed, report it to the FTC at ReportFraud.ftc.gov (https://reportfraud.ftc.gov/#/).

You can check out what is going on in your state or metro area by visiting ftc.gov/exploredata (https://www.ftc.gov/exploredata).

October 2020