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.

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 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 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.

How To Recognize and Avoid Phishing Scams

Scammers use email or text messages to trick you into giving them your personal and financial information. But there are several ways to protect yourself.

How To Recognize Phishing

Scammers use email or text messages to try to steal your passwords, account numbers, or Social Security numbers. If they get that information, they could get access to your email, bank, or other accounts. Or they could sell your information to other scammers. Scammers launch thousands of phishing attacks like these every day — and they're often successful.

Scammers often update their tactics to keep up with the latest news or trends, but here are some common tactics used in phishing emails or text messages:

Phishing emails and text messages often tell a story to trick you into clicking on a link or opening an attachment. You might get an unexpected email or text message that looks like it's from a company you know or trust, like a bank or a credit card or utility company. Or maybe it's from an online payment website or app. The message could be from a scammer, who might

- say they've noticed some suspicious activity or log-in attempts — they haven't
- claim there's a problem with your account or your payment information — there isn't
- say you need to confirm some personal or financial information — you don't
- include an invoice you don't recognize — it's fake
- want you to click on a link to make a payment — but the link has malware
- say you're eligible to register for a government refund — it's a scam
- offer a coupon for free stuff — it's not real

Here's a real-world example of a phishing email:
Image

Imagine you saw this in your inbox. At first glance, this email looks real, but it's not. Scammers who send emails like this one are hoping you won't notice it's a fake.

Here are signs that this email is a scam, even though it looks like it comes from a company you know — and even uses the company's logo in the header:

- The email has a generic greeting.
- The email says your account is on hold because of a billing problem.
- The email invites you to click on a link to update your payment details.

While real companies might communicate with you by email, legitimate companies won't email or text with a link to update your payment information. Phishing emails can often have real consequences for people who give scammers their information, including identity theft. And they might harm the reputation of the companies they're spoofing.

How To Protect Yourself From Phishing Attacks

Your email spam filters might keep many phishing emails out of your inbox. But scammers are always trying to outsmart spam filters, so extra layers of protection can help. Here are four ways to protect yourself from phishing attacks.

Four Ways To Protect Yourself From Phishing

1. Protect your computer by using security software. Set the software to update automatically so it will deal with any new security threats.

2. Protect your cell phone by setting software to update automatically. These updates could give you critical protection against security threats.

3. Protect your accounts by using multi-factor authentication. Some accounts offer extra security by requiring two or more credentials to log in to your account. This is called multi-factor authentication. The extra credentials you need to log in to your account fall into three categories:

- something you know — like a passcode, a PIN, or the answer to a security question.
- something you have — like a one-time verification passcode you get by text, email, or from an authenticator app; or a security key
- something you are — like a scan of your fingerprint, your retina, or your face

Multi-factor authentication makes it harder for scammers to log in to your accounts if they do get your username and password.

4. Protect your data by backing it up. Back up the data on your computer to an external hard drive or in the cloud. Back up the data on your phone, too.

What To Do if You Suspect a Phishing Attack

If you get an email or a text message that asks you to click on a link or open an attachment, answer this question:

Do I have an account with the company or know the person who contacted me?

If the answer is "No," it could be a phishing scam. Go back and review the advice in How to recognize phishing and look for signs of a phishing scam. If you see them, report the message and then delete it.

If the answer is "Yes," contact the company using a phone number or website you know is real — **not** the information in the email. Attachments and links might install harmful malware.

What To Do if You Responded to a Phishing Email

If you think a scammer has your information, like your Social Security, credit card, or bank account number, go to IdentityTheft.gov. There you'll see the specific steps to take based on the information that you lost.

If you think you clicked on a link or opened an attachment that downloaded harmful software, update your computer's security software. Then run a scan and remove anything it identifies as a problem.

How To Report Phishing

If you got a phishing email or text message, report it. The information you give helps fight scammers.

- If you got a phishing **email**, forward it to the Anti-Phishing Working Group at reportphishing@apwg.org.
- If you got a phishing **text message**, forward it to SPAM (7726).
- Report the phishing attempt to the FTC at ReportFraud.ftc.gov.

Holiday Shopping Fraud Continues to Target Consumers During a Season of Joy

A new 2024 AARP Fraud Watch Network™ report highlights the ways criminals are targeting consumers this holiday season. The report shows four-in-five (82%) U.S. consumers have experienced some type of fraud this year – including gift card scams, counterfeit products, phishing attempts disguised as delivery notifications, and more. The research also shows many consumers are not aware of the types of fraud they may come across when shopping online.

This year, more than half (56%) of consumers reported receiving a notification from someone saying they were from USPS, FedEx, or UPS about a shipment problem that ultimately turned out to be fraudulent, which nearly doubled compared to 2022 (29%). Likewise, nearly two-thirds of consumers (64%) are unaware that online retailers will not ask for personal login information to provide them with customer support.

Ads on social media continue to be a source for targeting consumers with over a third (35%) saying they experienced fraud when purchasing a product through an online ad. This highlights the importance of safe internet browsing and using caution when clicking ads that may appear legitimate.

In addition to the survey on consumers' personal experiences with scams, AARP asked survey respondents to answer a 10-question fraud knowledge quiz. Disturbingly, knowledge on some questions has declined over the last two years. Here's some important advice for consumers:

- Retailers will never request your login information to provide customer support.
- Be wary of free trial offers as they often lead to expensive subscriptions that are difficult to cancel.
- Peer-to-peer payment apps do not carry the same consumer protections as a credit card. Only use these apps with people and businesses you know and trust.
- It's risky to do a web search for a company's customer support number because criminals buy ads impersonating those companies. Check billing and credit card statements for customer service, use the number on the back of your credit cards, or go directly to the company online by typing in their web address, like www.aarp.org.