I'm not a bot

You can’t perform that action at this time. You can’t perform that action at this time. Cash App is an American peer-to-peer payment service available in the US and the UK. And whether it’s splitting the bill after a night out on the town or sending money for your niece’s graduation, more people are relying on Cash App and similar services than ever before. It’s a quick and seamless way to make financial transactions trusted by millions of users.Cash App makes it easy to receive and send money and is renowned for its convenience. But while Cash App transactions are generally safe, users could still be susceptible to Cash App scams.Want to protect yourself from online scams? Get ProtectionCash App’s growing popularityPeer-to-peer (P2P) payment services and money transfer apps like Cash App are becoming more popular because of their convenience and reliability. Today, more than 8 in 10 consumers have used a P2P payment service to make a financial transaction. Cash App is one of the most widely used P2P payment services on the market, along with the likes of Venmo, PayPal, and Zelle.Cash App saves users time and effort when it comes to making payments. There’s no need to run to the ATM to withdraw cash, because you can directly transfer money with just a few clicks on a mobile device.Some ways that people use Cash App include:Splitting the bill at a restaurantPaying for odd jobs and errandsSending rent moneyGiving a birthday or graduation giftThanks to the rise of technology like Cash App payment services, paying has gotten much easier than it used to be. Cash App is growing in popularity because it makes money easy to manage and eliminates the need for traditional banking when making payments between peers.How does Cash App work?Cash App is currently available only in the US and the UK. Users start by creating a free account that lets them receive and send money from users in the same country. Once the application has been successfully downloaded, users choose a unique username called a “$cashtag.” The $cashtag helps Cash App users find one another in order to make financial transactions.Once the $cashtag is set up, Cash App customers can add funds to their account by linking it to an existing checking account or debit card. This allows funds to be transferred directly to the user’s bank account and also allows funds from the user’s bank account to be transferred to Cash App.The app’s two main functions are paying others and getting paid. Users can enter an amount of money by clicking the “$” icon at the bottom of the app and selecting “Request” or “Pay” along with the intended $cashtag. Users can also use an email address or phone number to find one another.US and UK-based users can also request a Cash Card, which is a free Visa-verified debit card connected to a particular Cash App account. The Cash Card can be used like a conventional debit card to withdraw cash at ATMs or for everyday purchases.Cash App offers a number of security features to protect customer’s accounts, including PIN verification, biometric authentication, sign-in codes, and account usage alerts. But with so many people now using P2P payment services, cyber criminals have plenty of opportunities to make a profit through scams.Is Cash App safe?Although users are vulnerable to scams, Cash App offers safety features in an effort to protect its users.Cash App’s safety featuresCash App offers a few particular safety features to protect its users.Encryption: Encryption is used to secure user data while fraud monitoring algorithms detect suspicious activitySecurity Locks: Cash App PIN verification, sign-in codes, and Face ID help to secure Cash App paymentsNotifications: Users are alerted of suspicious activity via text or emailRemote Disabling: Card spending can be disabled immediately when the card gets lost or goes missingFraud Protection: Cash App provides buyer protection and cash support to defend against unauthorized charges12 common Cash App scams1. Posing as Cash App supportCash App scammers often take advantage of users by posing as Cash App support or other Cash App employees. This gives the illusion of legitimacy as scammers reach out via direct message or phone.Cash App advises, “Cash App Support will never ask you to provide your sign-in code or PIN, and will never require you to send a payment, make a purchase, download any application for ‘remote access,’ or complete a ‘test’ transaction of any kind.”The odds are, if someone is contacting you about your account balance or usage, it’s likely a scammer. If you receive any communication from what appears to be Cash App support and wish to contact Cash App, Cash App recommends going directly into the app to contact support.2. Offering expensive goodsOne of the more popular scams on Cash App is scammers offering expensive — but fictitious — goods or services in return for payment. Cash App isn’t a marketplace and doesn’t facilitate the purchase or trade of personal items. Cash App reminds customers, “Cash App to Cash App payments are instant and usually can’t be canceled. So remember — if something sounds too good to be true, it’s likely a scam.”If some unknown person is suddenly offering concert tickets, expensive electronics, or other valuables in return for a Cash App payment, it’s possible that they’ll take your money and disappear without ever providing the goods you paid for.3. Random depositsWaking up to an unexpected deposit can be super exciting. Who doesn’t like free money? Unfortunately, receiving a random deposit in your Cash App account is often a sign of an impending scam.A random deposit is often used to lull users into a sense of trust with scammers. After all, what kind of scammer deposits $1,000 into your account? However, Cash App explains, Scammers might send you a payment ‘by accident’ and ask for you to send the payment amount back to them. The amount you send them back is from your account funds. These scammers will dispute the payment with their bank or credit card after you’ve sent the funds back. This means they will be reimbursed by both you and their bank.”.4. Claim your prizeUsers may be contacted with claims of fabulous cash prizes. But in order to receive the prize, they must first send money. Cash App doesn’t require any Cash App user to pay for any contests or promotions, so requests to send funds in order to claim a prize are likely fraudulent.5. SSN requestAnyone asking for a user’s Social Security number is almost certainly a scammer. In general, it is best to only share your Social Security number with trusted sources (for example, your employer, a financial institution, or a government institution), and you should avoid sharing important identity information from requesters on any app, including Cash App.6. Government relief paymentsSome scammers may offer the promise of cash in the form of a government grant or relief program. This type of Cash App scam has been running rampant since the start of the COVID-19 pandemic and can look quite legitimate depending on the skill of the scammer. But any request for financial information is a telltale sign of a scam.7. Cash flippersMuch in the same way that property flippers buy and renovate homes for profit, scammers may claim to be able to “flip” the funds of users in order to make more money. Cash flipping scammers will usually ask for a small sum, something to the tune of $5 or $10, which they will claim they can flip into multiple times the amount.Also known as a “money circle” a cash flipping scam is designed to take money from users without ever giving them a return on investment. As a rule, if anyone makes a financial promise and asks you to send them money first, it’s a scam.8. Fake refundsIf you’re selling something on an online marketplace, a scammer may reach out claiming that they’re interested in the item and will make a payment via Cash App — except you won’t receive the money, and they’ll claim they’ve sent payment multiple times. They’ll demand a refund of your own money for an item they never actually paid for in the first place.9. Bad romanceIf somebody reaches out to you via Cash App with romantic promises of expensive dates and lavish gifts, it’s probably a scam. In addition, if you meet someone on a dating app or social media site and they ask you to send them money via Cash App, exercise extreme caution. If someone you haven’t met in person is claiming romantic intentions and requesting money via Cash App or other means, you should treat them with suspicion.10. #CashAppFridays#CashAppFridays is a real cash giveaway promotion run by Cash App, but that hasn’t stopped scammers from taking advantage of it. Fake Cash App accounts will use the hashtag and contact users claiming that they’ve won the giveaway — but in order to claim their prize, they’ll need to provide payment or login information. Real winners of #CashAppFridays won’t ever be asked for credentials or payment.11. Phishing emailsA classic scam, phishing scammers will send a legitimate-looking email to trick users into verifying their login credentials or to click a malicious link that steals their information. Real emails from the Cash App team will never ask users to provide login info or use threatening language in their messages.Cash App explains that verified emails from Cash App will come from @cash.app, @square.com and @squareup.com.address, and that if you do receive what appears to be a phishing email, you should contact support through the app.12. Fake security alertsSimilar to phishing emails, some scammers may send a fraudulent email claiming that your Cash App account was compromised, and your personal information has been leaked. Scammers often include links to fake websites in emails that prompt you to change your login credentials, but this trick can actually steal your existing login information.Learn more about F-SecureLearn more and stay safe with F-SecureKeeping your personal data safe can be a challenge on your mobile device, especially when it comes to personal finances and banking account information. If you want to protect yourself from scams on P2P payment apps like Cash App as well as other mobile threats, F-Secure offers comprehensive security and privacy on Android and iOS mobile devices and Windows and Mac computers.With F-Secure Total, you can protect yourself against scams and keep your personal data safe with a single solution that automatically scans every site you visit and link you click, blocking scams and risks before they can cause harm. And it all happens quietly in the background.You’ll also get comprehensive identity theft protection. An identity theft expert is only a click away if you ever need help, and your identity is backed with $1 million in identity theft coverage. If you’re looking for easy-to-use security for all your devices that identifies and protects against all online threats, trust F-Secure.FAQsDo Cash App scams exist?Yes, bad actors deploy different types of Cash App-related scams that affect users every day. These may include phishing scams, fake security alerts, cash flipping scams, and more.Can someone steal your money with your Cash App name?Scammers will need more than just your $cashtag to access your account. Additional credentials are needed to gain access to your funds, which is why scammers go to great lengths to obtain login information.What happens if a random person sends you money on Cash App?If a random person sends you money on Cash App, contact Cash App support immediately. An unexpected deposit is often a sign of a scam.Why would someone want a screenshot of my Cash App?Screenshots are used by Cash App scammers to trick users into thinking that they’ve sent you money or a fake Cash App receipt.Will Cash App refund money if I’m scammed?Cash App payments are instant and usually can’t be cancelled. But Cash App takes precautions to monitor your account for suspicious activity and can cancel any fraudulent payments to prevent you from being charged.Cash App doesn’t require users to link their bank account, however, a linked bank account is necessary to verify your Cash App account and remove limits on the amount of money you can send and receive each week.Page 2Cash App is an American peer-to-peer payment service available in the US and the UK. And whether it’s splitting the bill after a night out on the town or sending money for your niece’s graduation, more people are relying on Cash App and similar services than ever before. It’s a quick and seamless way to make financial transactions trusted by millions of users.Cash App makes it easy to receive and send money and is renowned for its convenience. But while Cash App transactions are generally safe, users could still be susceptible to Cash App scams.Want to protect yourself from online scams? Get ProtectionCash App’s growing popularityPeer-to-peer (P2P) payment services and money transfer apps like Cash App are becoming more popular because of their convenience and reliability. Today, more than 8 in 10 consumers have used a P2P payment service to make a financial transaction. Cash App is one of the most widely used P2P payment services on the market, along with the likes of Venmo, PayPal, and Zelle.Cash App saves users time and effort when it comes to making payments. There’s no need to run to the ATM to withdraw cash, because you can directly transfer money with just a few clicks on a mobile device.Some ways that people use Cash App include:Splitting the bill at a restaurantPaying for odd jobs and errandsSending rent moneyGiving a birthday or graduation giftThanks to the rise of technology like Cash App payment services, paying has gotten much easier than it used to be. Cash App is growing in popularity because it makes money easy to manage and eliminates the need for traditional banking when making payments between peers.How does Cash App work?Cash App is currently available only in the US and the UK. Users start by creating a free account that lets them receive and send money from users in the same country. Once the application has been successfully downloaded, users choose a unique username called a “$cashtag.” The $cashtag helps Cash App users find one another in order to make financial transactions.Once the $cashtag is set up, Cash App customers can add funds to their account by linking it to an existing checking account or debit card. This allows funds to be transferred directly to the user’s bank account and also allows funds from the user’s bank account to be transferred to Cash App.The app’s two main functions are paying others and getting paid. Users can enter an amount of money by clicking the “$” icon at the bottom of the app and selecting “Request” or “Pay” along with the intended $cashtag. Users can also use an email address or phone number to find one another.US and UK-based users can also request a Cash Card, which is a free Visa-verified debit card connected to a particular Cash App account. The Cash Card can be used like a conventional debit card to withdraw cash at ATMs or for everyday purchases.Cash App offers a number of security features to protect customer’s accounts, including PIN verification, biometric authentication, sign-in codes, and account usage alerts. But with so many people now using P2P payment services, cyber criminals have plenty of opportunities to make a profit through scams.Is Cash App safe?Although users are vulnerable to scams, Cash App offers safety features in an effort to protect its users.Cash App’s safety featuresCash App offers a few particular safety features to protect its users.Encryption: Encryption is used to secure user data while fraud monitoring algorithms detect suspicious activitySecurity Locks: Cash App PIN verification, sign-in codes, and Face ID help to secure Cash App paymentsNotifications: Users are alerted of suspicious activity via text or emailRemote Disabling: Card spending can be disabled immediately when the card gets lost or goes missingFraud Protection: Cash App provides buyer protection and cash support to defend against unauthorized charges12 common Cash App scams1. Posing as Cash App supportCash App scammers often take advantage of users by posing as Cash App support or other Cash App employees. This gives the illusion of legitimacy as scammers reach out via direct message or phone.Cash App advises, “Cash App Support will never ask you to provide your sign-in code or PIN, and will never require you to send a payment, make a purchase, download any application for ‘remote access,’ or complete a ‘test’ transaction of any kind.”The odds are, if someone is contacting you about your account balance or usage, it’s likely a scammer. If you receive any communication from what appears to be Cash App support and wish to contact Cash App, Cash App recommends going directly into the app to contact support.2. Offering expensive goodsOne of the more popular scams on Cash App is scammers offering expensive — but fictitious — goods or services in return for payment. Cash App isn’t a marketplace and doesn’t facilitate the purchase or trade of personal items. Cash App reminds customers, “Cash App to Cash App payments are instant and usually can’t be canceled. So remember — if something sounds too good to be true, it’s likely a scam.”If some unknown person is suddenly offering concert tickets, expensive electronics, or other valuables in return for a Cash App payment, it’s possible that they’ll take your money and disappear without ever providing the goods you paid for.3. Random depositsWaking up to an unexpected deposit can be super exciting. Who doesn’t like free money? Unfortunately, receiving a random deposit in your Cash App account is often a sign of an impending scam.A random deposit is often used to lull users into a sense of trust with scammers. After all, what kind of scammer deposits $1,000 into your account? However, Cash App explains, Scammers might send you a payment ‘by accident’ and ask for you to send the payment amount back to them. The amount you send them back is from your account funds. These scammers will dispute the payment with their bank or credit card after you’ve sent the funds back. This means they will be reimbursed by both you and their bank.”.4. Claim your prizeUsers may be contacted with claims of fabulous cash prizes. But in order to receive the prize, they must first send money. Cash App doesn’t require any Cash App user to pay for any contests or promotions, so requests to send funds in order to claim a prize are likely fraudulent.5. SSN requestAnyone asking for a user’s Social Security number is almost certainly a scammer. In general, it is best to only share your Social Security number with trusted sources (for example, your employer, a financial institution, or a government institution), and you should avoid sharing important identity information from requesters on any app, including Cash App.6. Government relief paymentsSome scammers may offer the promise of cash in the form of a government grant or relief program. This type of Cash App scam has been running rampant since the start of the COVID-19 pandemic and can look quite legitimate depending on the skill of the scammer. But any request for financial information is a telltale sign of a scam.7. Cash flippersMuch in the same way that property flippers buy and renovate homes for profit, scammers may claim to be able to “flip” the funds of users in order to make more money. Cash flipping scammers will usually ask for a small sum, something to the tune of $5 or $10, which they will claim they can flip into multiple times the amount.Also known as a “money circle” a cash flipping scam is designed to take money from users without ever giving them a return on investment. As a rule, if anyone makes a financial promise and asks you to send them money first, it’s a scam.8. Fake refundsIf you’re selling something on an online marketplace, a scammer may reach out claiming that they’re interested in the item and will make a payment via Cash App — except you won’t receive the money, and they’ll claim they’ve sent payment multiple times. They’ll demand a refund of your own money for an item they never actually paid for in the first place.9. Bad romanceIf somebody reaches out to you via Cash App with romantic promises of expensive dates and lavish gifts, it’s probably a scam. In addition, if you meet someone on a dating app or social media site and they ask you to send them money via Cash App, exercise extreme caution. If someone you haven’t met in person is claiming romantic intentions and requesting money via Cash App or other means, you should treat them with suspicion.10. #CashAppFridays#CashAppFridays is a real cash giveaway promotion run by Cash App, but that hasn’t stopped scammers from taking advantage of it. Fake Cash App accounts will use the hashtag and contact users claiming that they’ve won the giveaway — but in order to claim their prize, they’ll need to provide payment or login information. Real winners of #CashAppFridays won’t ever be asked for credentials or payment.11. Phishing emailsA classic scam, phishing scammers will send a legitimate-looking email to trick users into verifying their login credentials or to click a malicious link that steals their information. Real emails from the Cash App team will never ask users to provide login info or use threatening language in their messages.Cash App explains that verified emails from Cash App will come from @cash.app, @square.com and @squareup.com.address, and that if you do receive what appears to be a phishing email, you should contact support through the app.12. Fake security alertsSimilar to phishing emails, some scammers may send a fraudulent email claiming that your Cash App account was compromised, and your personal information has been leaked. Scammers often include links to fake websites in emails that prompt you to change your login credentials, but this trick can actually steal your existing login information.Learn more about F-SecureLearn more and stay safe with F-SecureKeeping your personal data safe can be a challenge on your mobile device, especially when it comes to personal finances and banking account information. If you want to protect yourself from scams on P2P payment apps like Cash App as well as other mobile threats, F-Secure offers comprehensive security and privacy on Android and iOS mobile devices and Windows and Mac computers.With F-Secure Total, you can protect yourself against scams and keep your personal data safe with a single solution that automatically scans every site you visit and link you click, blocking scams and risks before they can cause harm. And it all happens quietly in the background.You’ll also get comprehensive identity theft protection. An identity theft expert is only a click away if you ever need help, and your identity is backed with $1 million in identity theft coverage. If you’re looking for easy-to-use security for all your devices that identifies and protects against all online threats, trust F-Secure.FAQsDo Cash App scams exist?Yes, bad actors deploy different types of Cash App-related scams that affect users every day. These may include phishing scams, fake security alerts, cash flipping scams, and more.Can someone steal your money with your Cash App name?Scammers will need more than just your $cashtag to access your account. Additional credentials are needed to gain access to your funds, which is why scammers go to great lengths to obtain login information.What happens if a random person sends you money on Cash App?If a random person sends you money on Cash App, contact Cash App support immediately. An unexpected deposit is often a sign of a scam.Why would someone want a screenshot of my Cash App?Screenshots are used by Cash App scammers to trick users into thinking that they’ve sent you money or a fake Cash App receipt.Will Cash App refund money if I’m scammed?Cash App payments are instant and usually can’t be cancelled. But Cash App takes precautions to monitor your account for suspicious activity and can cancel any fraudulent payments to prevent you from being charged.Cash App doesn’t require users to link their bank account, however, a linked bank account is necessary to verify your Cash App account and remove limits on the amount of money you can send and receive each week.Page 3Cash App is an American peer-to-peer payment service available in the US and the UK. And whether it’s splitting the bill after a night out on the town or sending money for your niece’s graduation, more people are relying on Cash App and similar services than ever before. It’s a quick and seamless way to make financial transactions trusted by millions of users.Cash App makes it easy to receive and send money and is renowned for its convenience. But while Cash App transactions are generally safe, users could still be susceptible to Cash App scams.Want to protect yourself from online scams? Get ProtectionCash App’s growing popularityPeer-to-peer (P2P) payment services and money transfer apps like Cash App are becoming more popular because of their convenience and reliability. Today, more than 8 in 10 consumers have used a P2P payment service to make a financial transaction. Cash App is one of the most widely used P2P payment services on the market, along with the likes of Venmo, PayPal, and Zelle.Cash App saves users time and effort when it comes to making payments. There’s no need to run to the ATM to withdraw cash, because you can directly transfer money with just a few clicks on a mobile device.Some ways that people use Cash App include:Splitting the bill at a restaurantPaying for odd jobs and errandsSending rent moneyGiving a birthday or graduation giftThanks to the rise of technology like Cash App payment services, paying has gotten much easier than it used to be. Cash App is growing in popularity because it makes money easy to manage and eliminates the need for traditional banking when making payments between peers.How does Cash App work?Cash App is currently available only in the US and the UK. Users start by creating a free account that lets them receive and send money from users in the same country. Once the application has been successfully downloaded, users choose a unique username called a “$cashtag.” The $cashtag helps Cash App users find one another in order to make financial transactions.Once the $cashtag is set up, Cash App customers can add funds to their account by linking it to an existing checking account or debit card. This allows funds to be transferred directly to the user’s bank account and also allows funds from the user’s bank account to be transferred to Cash App.The app’s two main functions are paying others and getting paid. Users can enter an amount of money by clicking the “$” icon at the bottom of the app and selecting “Request” or “Pay” along with the intended $cashtag. Users can also use an email address or phone number to find one another.US and UK-based users can also request a Cash Card, which is a free Visa-verified debit card connected to a particular Cash App account. The Cash Card can be used like a conventional debit card to withdraw cash at ATMs or for everyday purchases.Cash App offers a number of security features to protect customer’s accounts, including PIN verification, biometric authentication, sign-in codes, and account usage alerts. But with so many people now using P2P payment services, cyber criminals have plenty of opportunities to make a profit through scams.Is Cash App safe?Although users are vulnerable to scams, Cash App offers safety features in an effort to protect its users.Cash App’s safety featuresCash App offers a few particular safety features to protect its users.Encryption: Encryption is used to secure user data while fraud monitoring algorithms detect suspicious activitySecurity Locks: Cash App PIN verification, sign-in codes, and Face ID help to secure Cash App paymentsNotifications: Users are alerted of suspicious activity via text or emailRemote Disabling: Card spending can be disabled immediately when the card gets lost or goes missingFraud Protection: Cash App provides buyer protection and cash support to defend against unauthorized charges12 common Cash App scams1. Posing as Cash App supportCash App scammers often take advantage of users by posing as Cash App support or other Cash App employees. This gives the illusion of legitimacy as scammers reach out via direct message or phone.Cash App advises, “Cash App Support will never ask you to provide your sign-in code or PIN, and will never require you to send a payment, make a purchase, download any application for ‘remote access,’ or complete a ‘test’ transaction of any kind.”The odds are, if someone is contacting you about your account balance or usage, it’s likely a scammer. If you receive any communication from what appears to be Cash App support and wish to contact Cash App, Cash App recommends going directly into the app to contact support.2. Offering expensive goodsOne of the more popular scams on Cash App is scammers offering expensive — but fictitious — goods or services in return for payment. Cash App isn’t a marketplace and doesn’t facilitate the purchase or trade of personal items. Cash App reminds customers, “Cash App to Cash App payments are instant and usually can’t be canceled. So remember — if something sounds too good to be true, it’s likely a scam.”If some unknown person is suddenly offering concert tickets, expensive electronics, or other valuables in return for a Cash App payment, it’s possible that they’ll take your money and disappear without ever providing the goods you paid for.3. Random depositsWaking up to an unexpected deposit can be super exciting. Who doesn’t like free money? Unfortunately, receiving a random deposit in your Cash App account is often a sign of an impending scam.A random deposit is often used to lull users into a sense of trust with scammers. After all, what kind of scammer deposits $1,000 into your account? However, Cash App explains, Scammers might send you a payment ‘by accident’ and ask for you to send the payment amount back to them. The amount you send them back is from your account funds. These scammers will dispute the payment with their bank or credit card after you’ve sent the funds back. This means they will be reimbursed by both you and their bank.”.4. Claim your prizeUsers may be contacted with claims of fabulous cash prizes. But in order to receive the prize, they must first send money. Cash App doesn’t require any Cash App user to pay for any contests or promotions, so requests to send funds in order to claim a prize are likely fraudulent.5. SSN requestAnyone asking for a user’s Social Security number is almost certainly a scammer. In general, it is best to only share your Social Security number with trusted sources (for example, your employer, a financial institution, or a government institution), and you should avoid sharing important identity information from requesters on any app, including Cash App.6. Government relief paymentsSome scammers may offer the promise of cash in the form of a government grant or relief program. This type of Cash App scam has been running rampant since the start of the COVID-19 pandemic and can look quite legitimate depending on the skill of the scammer. But any request for financial information is a telltale sign of a scam.7. Cash flippersMuch in the same way that property flippers buy and renovate homes for profit, scammers may claim to be able to “flip” the funds of users in order to make more money. Cash flipping scammers will usually ask for a small sum, something to the tune of $5 or $10, which they will claim they can flip into multiple times the amount.Also known as a “money circle” a cash flipping scam is designed to take money from users without ever giving them a return on investment. As a rule, if anyone makes a financial promise and asks you to send them money first, it’s a scam.8. Fake refundsIf you’re selling something on an online marketplace, a scammer may reach out claiming that they’re interested in the item and will make a payment via Cash App — except you won’t receive the money, and they’ll claim they’ve sent payment multiple times. They’ll demand a refund of your own money for an item they never actually paid for in the first place.9. Bad romanceIf somebody reaches out to you via Cash App with romantic promises of expensive dates and lavish gifts, it’s probably a scam. In addition, if you meet someone on a dating app or social media site and they ask you to send them money via Cash App, exercise extreme caution. If someone you haven’t met in person is claiming romantic intentions and requesting money via Cash App or other means, you should treat them with suspicion.10. #CashAppFridays#CashAppFridays is a real cash giveaway promotion run by Cash App, but that hasn’t stopped scammers from taking advantage of it. Fake Cash App accounts will use the hashtag and contact users claiming that they’ve won the giveaway — but in order to claim their prize, they’ll need to provide payment or login information. Real winners of #CashAppFridays won’t ever be asked for credentials or payment.11. Phishing emailsA classic scam, phishing scammers will send a legitimate-looking email to trick users into verifying their login credentials or to click a malicious link that steals their information. Real emails from the Cash App team will never ask users to provide login info or use threatening language in their messages.Cash App explains that verified emails from Cash App will come from @cash.app, @square.com and @squareup.com.address, and that if you do receive what appears to be a phishing email, you should contact support through the app.12. Fake security alertsSimilar to phishing emails, some scammers may send a fraudulent email claiming that your Cash App account was compromised, and your personal information has been leaked. Scammers often include links to fake websites in emails that prompt you to change your login credentials, but this trick can actually steal your existing login information.Learn more about F-SecureLearn more and stay safe with F-SecureKeeping your personal data safe can be a challenge on your mobile device, especially when it comes to personal finances and banking account information. If you want to protect yourself from scams on P2P payment apps like Cash App as well as other mobile threats, F-Secure offers comprehensive security and privacy on Android and iOS mobile devices and Windows and Mac computers.With F-Secure Total, you can protect yourself against scams and keep your personal data safe with a single solution that automatically scans every site you visit and link you click, blocking scams and risks before they can cause harm. And it all happens quietly in the background.You’ll also get comprehensive identity theft protection. An identity theft expert is only a click away if you ever need help, and your identity is backed with $1 million in identity theft coverage. If you’re looking for easy-to-use security for all your devices that identifies and protects against all online threats, trust F-Secure.FAQsDo Cash App scams exist?Yes, bad actors deploy different types of Cash App-related scams that affect users every day. These may include phishing scams, fake security alerts, cash flipping scams, and more.Can someone steal your money with your Cash App name?Scammers will need more than just your $cashtag to access your account. Additional credentials are needed to gain access to your funds, which is why scammers go to great lengths to obtain login information.What happens if a random person sends you money on Cash App?If a random person sends you money on Cash App, contact Cash App support immediately. An unexpected deposit is often a sign of a scam.Why would someone want a screenshot of my Cash App?Screenshots are used by Cash App scammers to trick users into thinking that they’ve sent you money or a fake Cash App receipt.Will Cash App refund money if I’m scammed?Cash App payments are instant and usually can’t be cancelled. But Cash App takes precautions to monitor your account for suspicious activity and can cancel any fraudulent payments to prevent you from being charged.Cash App doesn’t require users to link their bank account, however, a linked bank account is necessary to verify your Cash App account and remove limits on the amount of money you can send and receive each week. You can’t perform that action at this time. You can’t perform that action at this time. You can’t perform that action at this time. For today’s consumers, convenience is king. And at the heart of the digital experiences that make our lives easier sits the smartphone. Over the years, these devices have become an extension of ourselves, slowly replacing our cameras, our PCs and now our wallets. But the popularity of the apps we use every day has made them an attractive target for fraudsters. And mobile payment apps like Cash App, Zelle or Venmo that allow users to send each other money are right at the top of their priority list. The rise of Cash App Cash App is used by tens of millions of people each month, especially because among other things, the app allows users to send and receive money instantly. Although it includes multiple features including PIN and biometric authentication, account usage alerts and a certain amount of protection from unauthorized charges, it can’t insulate you from fraud. In short, if you’re tricked into sending a fraudster money, that cash is most likely gone, never to return. Understanding exactly what these scams might look like is the first step towards staying safe. Top 10 Cash App scams 1. Super Cash App Friday impersonators The weekly cash giveaway event on the platform’s Instagram and Twitter accounts has, predictably, been hijacked by fraudsters. They’ll contact a participant via social media, tell them they’ve won and then request a fee in order to release the funds. 2. Cash flipping The Cash App Friday/$Cashtag scam is sometimes a premise for another increasingly common type of fraud leveraging the service. Users are contacted saying that if they send a specific amount of money, they will be sent back more than the original amount. As most such offers are, this “cash flipping” deal is too good to be true. 3. Fake support Scammers may set up fake support accounts on social media or use SEO poisoning to get fake websites featuring phony “Cash App support” phone numbers at the top of search results. When a user clicks through and rings up with a genuine complaint/request, they’re asked for log-in info, enabling the fraudster to hijack and clear out their accounts. 4. Selling items online Often, fraudsters try to sell non-existent items online – anything from a pure-breed puppy to tickets for a sold-out show. They might ask for a deposit, or even the whole amount, to be sent via Cash App. But unlike using a credit or debit card, there’s no buyer protection for the victim. In other examples, scammers may target online sellers, by sending fake payment notification screenshots and claiming the balance will only show up in the seller’s Cash App account after delivery. 5. Phishing messages and vishing calls Fraudsters also leverage the Cash App brand in classic email/SMS/phone-based social engineering efforts designed to trick victims into handing over their personal details. The aim, as in the fake support scams, is to get hold of information in order to hijack victims’ accounts. 6. Fake Cash App receipts Scammers claim that they’ve sent money to a victim’s Cash App account by accident and ask them to return the amount. A spoofed receipt screenshot adds legitimacy to the request. 7. Debit card scams Cash App also offers a debit card option for users. Scammers might use previously breached personal information to sign-up for one in a victim’s name, and have it sent to their home. They’ll request the recipient registers an app and scans a QR code to activate it. Such accounts could be used to launder funds from other scams. 8. Real estate rentals In many cities across Europe and the US, rental property is in short supply. Scammers take advantage of this surging demand by reposting previously advertised apartments and homes, and requesting ‘deposits’ and ‘application fees’ via Cash App. 9. Romance scams Romance scams resulted in losses of almost US$1 billion for victims last year, according to the FBI. Via fake profiles on dating sites, scammers will gain their victims’ trust, pretend to ‘fall in love’ with them and then request money via Cash App for expenses such as plane tickets, medical treatment and more. In some cases, sugar daddy scammers, too, may ask their targets to make upfront payments using Cash App or another peer-to-peer payment app with the promise of receiving larger sums of money later. 10. Investment scams This was another high-earning category of cybercrime, making nearly US$1.5 billion for scammers last year. Victims receive unsolicited emails/social media messages telling them about unbeatable (but fake) investment opportunities, often in cryptocurrency. As Cash App can be used legitimately to buy Bitcoin, it’s a natural channel for crypto scams. How to stay safe The good news is that it shouldn’t take much to keep the fraudsters at bay. By configuring the most secure settings in the app and treating any unsolicited contact with a healthy dose of skepticism, Cash App users can avoid most of the above scams. Consider the following: Stay phishing aware: Never click on links or reply to unsolicited emails, texts or social media messages. Note that legitimate Cash App emails only come from @square.com, @squareup.com, or @cash.app. And the firm’s support team will never request a sign-in code, PIN, Social Security Number (SSN), a payment or the downloading of a remote access app. Optimize account security: Turn on two-factor authentication in any linked email account, switch on notifications in Cash App to track payments and ensure that a passcode is required when making any payment. Secure your mobile device: Add a strong password or PIN and/or biometric authentication for lock-screen security. Never send money to people you don’t trust: Be skeptical of any requests – however small – for “deposits,” payments in exchange for “free” cash and similar. Minimize risk: Limit the amount of money stored in the Cash App account. Don’t Google Cash App support: Use the in-app chat function or these official channels suggested by the app. In the event you may have been scammed, report it to Cash App. That way, the firm can try to recover your money or at least help to keep other users safe. You can’t perform that action at this time. You can’t perform that action at this time. You can’t perform that action at this time. Cash App scams have sky rocketed recently mainly thanks to the ever increasing popularity of mobile payment platforms, like PayPal, Zelle, and Venmo.Cash App also offers lots of other great services and features to users. Customers can purchase stocks and Bitcoin on Cash App for as little as $1, get their paycheck up to two days early, and have access to free ATM withdrawals (if they have at least $300 coming in each month).With its free payments and all these other awesome features on offer, it’s not hard to see why Cash App is used by more than 40 million people.Sadly, there are a lot of Cash App scams that users need to be aware of. Need Easy Extra $300+/Month for Free? FreeCash: Get paid up to $497.82 per offer – test apps, play games, and complete surveys for fast cash! Start earning today! Earn Haus: Earn up to $25 per survey, plus get paid the same day via PayPal, Venmo, or check! Join Earn Haus now! InboxDollars: Over $57 million paid to members for watching videos, shopping, and completing surveys. Claim your $5 bonus instantly when you join! Product Report Card: Get paid to review products from home (payouts from $0.50 to $500)! Join for Free! KashKick: Earn money watching videos, shopping, surfing the web, and more – PayPal payments are fast! Start earning with KashKick now! Swagbucks: Watch videos, shop online, take surveys, and more – get $10 instantly when you sign up! Join now and start earning! Cash App is being used by scammers who are looking to scam people out of their money and sensitive personal information, such as their Social Security Number. Anyone can be scammed. So, it’s important to be aware and know what to avoid. After all, no one wants to go through the stress of being scammed. Cash App Fraud: Common Scams to Look Out For There are a lot of different Cash App scams. Here are some of the most common ones. 1. Cash App Flip Scams Cash App flip scams involve someone asking you to send them a smaller amount of money, which they say they will “flip” to get you even more money back. So, basically, the scammer claims to have the ability to “flip” your money and they promise to increase your cash if you first send them some money. For example, someone might ask you to send them $15 on Cash App and they’ll send you $150 back. Or they may ask for $100 and they’ll send you $800 back, etc. In fact, one of the most common ones is the Cash App $100 to $800 flip or Cash App game $800. This is a total scam. The scammer will accept your money, and then never send you anything in return. With the Cash App flip scam, the scammer may send you a message or put a post on social media. Sadly, the Cash App flip scam comes in many forms. For example, one person may say that there is a money glitch on the Cash App system, so you need to take advantage of the opportunity to get free cash before they fix the glitch on the app. Or, the scammer might say that they will invest the money you send them in the stock market or some other venture, and you’ll get way more money back than you put in. If someone promises you free money in return for sending them payment, it is a scam. 2. Customer support scam Another common scam, and one that is easy to fall for, is the customer support scam. With this one, the scammer will pretend to be a Cash App customer support agent or some other company representative, so that they can gain access to your account and steal your money. The scammer will reach out to your through text, phone call, or direct message masquerading as a Cash App customer support agent, or other company rep. A legit customer support agent will never ask you to do any of the following: Provide your sign-in code or PIN. Send payment. Make a purchase. Download any application for “remote access.” Complete a “test” transaction of any kind. If someone who claims to work for Cash App Support does any of the things above, they are a scammer who is trying to gain access to your account and steal money. 3. Random cash deposit scam Next on the list we have another really popular scam. This is the random cash deposit scam. With this one, a random person “accidentally” sends you money on Cash App. Reddit is full of posts from people saying, “Random person sent me money on Cash App. Is is legit?”. Obviously, it’s a scam. They do this to gain your trust. Scammers will often use the deposit as a means of luring you into a conversation, which can lead to other scams. Or, they claim it was a mistake and they ask you to refund them the amount they sent. But, they used stolen credit card numbers to fund their account. If anyone deposits money into your account randomly, then get in touch with Cash App support. Do not communicate with the sender. Contact Cash App and ask them to deal with the situation. 4. Payment Claiming Scam Another common Cash App scam is the payment claiming scam. With this one, the scammer will ask you to claim a payment that you deserve by sending money to them. Whenever someone offers to send you free money in return for you sending them a payment, it is usually a scam. So, keep your money safe, and don’t fall for it! These payment-claiming attempts are scams. Also, Cash App will never request money from you for any reason. On Cash App, there is actually no such thing as “claiming” a payment by sending money to Cash App. 5. The Security Alert Scam (and other phishing scams) Next on the list we have the security alert scam. Basically, with this one, you get a fake security alert that tells you that your Cash App account has been compromised. I’ve actually had these from a lot of companies, like Apple, and they’ve told me that my account has been comprised, and I have to follow the link in the email to login to change my password. Then, there’s this scam link, which I do not click because it’s just a scammer trying to steal information from me. I don’t even have an Apple account though, so joke’s on them! This is called phishing. Anyway, the security alert Cash App scam works in a similar way, where you get a message telling you that your account has been compromised, and they’ll include a link to a website where you can change your Cash App login credentials. Basically, the scammer is trying to trick you into revealing your account information by claiming that there are issues with your Cash App account. It’s awful because it preys on people’s fears, right? A lot of us worry about our passwords being compromised. I mean, there are real data breaches where passwords are actually compromised, so it’s not that much of a stretch for us to believe an email that tells us that has indeed happened, right? Sadly, this is a common scam. With the Cash App security alert scam, the scammer will use any information that you share to empty your account. So, do not follow links in any messages that claim that your account’s security has been compromised. If you get a security alert like this, it’s important not to panic. Don’t assume that your account has been compromised. I actually have a really, really simple rule that I use because these scammers have gotten way better at using email addresses that look legit, and they put the company logo in there and everything. So, it can be really hard to tell a scam email from a legit one. So, my rule is to never click a link within an email to change your login credentials. Always, always, go to the official site, and click on the change password or forgotten password option. That way, you know that you have only gone through a legit site and that your account is okay. So, if you are worried about your account being compromised, and you want to change your password, make sure you do it through the official site. Another option is to contact Cash App support and let them know. You can then ask if there have been any security issues with your account. 6. The Social Security Number Scam Okay, so another scam to watch out for is the Social Security Number scam. Many scammers are after money, but some are also after your sensitive personal information, such as your Social Security Number. If someone asks you for your SSN on the app, do not give it to them. First of all, giving out your Social Security Number can lead to identity theft. The scammer could even open new bank accounts or credit cards in your name. Or, the scammer may pretend to be from a government agency and ask for payment through Cash App in exchange for Social Security benefits and services. Some might say that your benefits are going to be canceled, or that your card needs to be updated. They may use threatening language to get you to confirm your SSN, and then they’ll ask for payment through Cash App for the “service.” Government agencies will never ask for payment through Cash App. If you get a call that looks as though it comes from a government agency, then hang up and call back using the agency’s official, toll-free phone number (1-800-772-1213) or visit SSA.gov. 7. Apartment/Home rental scams Unfortunately, scammers are getting more creative over the years and there are more and more methods they use to try to scam people out of their hard-earned money. One of the ways scammers target people on Cash App is with the apartment/home rental scam. With this one, the scammer promises a cheap property, like an apartment at a much lower rate than normal, but you’re required to send a deposit first, like before you even tour the prospective rental. Well, that rental likely doesn’t exist at all. Instead, they are using the offer of this incredibly priced property to get you to send them money. You send the deposit, and you never see your money again. Do not send money to someone you don’t know who is promising to give you something, like an apartment rental, at a later date. It is likely a scam. 8. Cash App Giveaway Scam Cash App giveaway scams are pretty common. Now, because Cash App itself does actually offer giveaways, people are quite susceptible to this one. Sadly, scam accounts will use the same hashtags that Cash App does for its legit giveaways, such as #CashAppFriday, to get in touch with users to tell them they have won a giveaway. The scammer then says you will need to: Pay something to claim your giveaway. Provide your login credentials first. DM them your financial information to collect your prize. Cash App does not require users to send money to claim their prize. So, please do not fall for this one. Sadly, scammers create fake accounts where they claim to offer Cash App giveaways. Only enter giveaways that are from Cash App’s official social media accounts. These are all blue tick accounts. Unfortunately, some scammers will actually message people who reply in the original Cash App thread. So, you really have to be careful. If a social media account gets in touch saying you’ve won and asking for something in return whether that be money, your financial information, or your login credentials, this is a scam. 9. The Pet Deposit Scam One of the most awful things about scammers, aside from the fact that they, you know, steal from people, is that they play on people’s hopes and fears. A lot of people, love animals, myself included, and would love a new puppy or kitten to bring joy into our lives. But, pets can be expensive. Pedigree animals can be costly, and many can’t afford their dream dog or cat. Scammers take advantage of this type of situation. Scammers will claim to have an upcoming litter and will ask you to make a deposit in order to secure one of the puppies or kittens. They usually offer a pet, like a German Shepherd puppy or a Ragdoll kitten, at a much lower cost than they are typically offered for normally. These scammers post fake photos to lure you in. They offer you a pure-bred, highly sought-after animal at an affordable price. This is not a legit offer though. There is no pet, and the person is just trying to scam you out of money. Adopting a pet from a local shelter is a better choice. 10. Romance scams Like I said earlier, scammers prey on people’s hopes and fears. They play on people’s emotions to trick them into giving money. This could be the fear that their account has been compromised, like with the security alert scam, the excitement of potentially winning money which is often much needed by many people just to pay for bills and food, leads us to not really think through why we need to provide our financial information to claim a giveaway, or, in the case of this scam, the need for love and companionship. With the romance scam, people are scammed out of their money by a person who claims to “love and care” about them, but in reality, the scammer is just playing on their emotions to extort as much money as they can. Romance scams occur when scammers create fake accounts on dating sites, or social media platforms in order to build relationships with the people they plan to scam. They will start a rapport with the victim, and gain their trust. These types of scams often move quickly. The scammer will often tell the victim that they love them in a matter of days, and pressure the victim to say it back. This is all a scam. Despite the scammer professing their “love” and being so “open with their emotions,” actually meeting with you face to face is somehow too much trouble. Romance scammers always have an excuse as to why the relationship can only take place online. Once the scammer has gained the victim’s trust, they will ask for money through Cash App, and usually there’s some sort of sob story as to why they need the cash. Like, there’s been an emergency, and they need money fast. Or, that they are overseas, and can’t access their bank account. Basically, they will make up stories to get you to send them money. These are all lies. Any money you send them will be lost. Do not send anyone you have only met online money via Cash App or using any other payment method. 11. Cryptocurrency scams With Cash App, you can invest in Bitcoin with as little as $1. That’s awesome, right? If you are looking to invest money in Bitcoin, then I would recommend you do it directly through the Cash App platform. Sadly, there are scammers out there that will offer to invest in Bitcoin on your behalf. They will ask you to transfer money to them, and then they’ll invest it for you. This is a total scam though. You won’t see your cash again. Don’t allow a stranger to invest in Bitcoin for you. You can simply invest in Bitcoin yourself, and you won’t have to worry about being scammed. Some scammers will ask you to transfer Bitcoin from Cash App. This happened to a man named Joseph Thompson. He believed that he was talking with his son’s friend, when in fact, said friend’s account had actually been hijacked by a scammer. You can read more about that story here. 12. The Buy Online Scam Scammers will put something for sale online, and then they will ask for payment via Cash App. Now, Cash App is a great app for sending and receiving money, but only to people that you know. Using Cash App to pay for things from buyers online, on sites like Craigslist or Facebook Marketplace is not a good idea. The reason for this is that unlike PayPal or credit cards, Cash App doesn’t offer buyer protection. There’s a scam where people put fake listings on sites like Craigslist and Facebook Marketplace and ask for payment via Cash App. You send payment, and you never receive the item. As I said, Cash App doesn’t offer buyer protection, so you won’t be able to get that money back. P2P mobile platforms are not meant to be used to purchase things online from strangers. 13. Fake Cash App Payment scam It’s not just buyers who have to be wary of fraudsters online, but also sellers. Yes, sellers can be susceptible to scams as well. If you are selling something online, be wary of people who offer to pay you via Cash App. Yes, some people just like using the app, but it’s often used by scammers. With this scam, the fraudster will say they want to pay you via Cash App. Only, you don’t receive any money. The scammer then tries to convince you that they sent the money. They will send you an email saying there’s money in your account. You may even receive a Cash App payment notification email that looks real, but it’s not from an official domain. Oh, and sometimes these scammers even have a “receipt” to prove it, which is, of course, fake. This is a total scam of course. They then proceed to coerce you into refunding them, but they never even paid you in the first place! Crazy, right? The whole thing is a scam. And, if you call the scammer on this and tell them they haven’t sent you anything, they will often claim that you are the one scamming them. The audacity of these scammers is insane, really. But, this sort of thing happens. So, if someone claims to have sent you money that you never received, and they ask for a “refund” DO NOT send them any money. 14. The fake Cash App Debit Card Scam Like I said before, Cash App has a lot of great features that make it a really popular app. One of the features that Cash App has to offer is the Cash Card. The Cash Card is a free debit card that is connected to your Cash App balance. The Cash Card can be used anywhere that Visa is accepted. You can request a Cash Card from Cash App. Once you get your card, you can use it to shop online or in-store anywhere that accepts VISA. The card has a few other features that are really handy. For example, you can get Boosts through your Cash Card. All you need to do is get a Cash Card, and you’ll get Cash Boosts when you spend money. Boosts are basically discounts of between 5% and 15%. They are time-sensitive offers that can save you money on your purchases at coffee shops, restaurants, and other merchants. So, with the Cash Card, you can spend your balance wherever VISA is accepted, and it provides some great discounts with Boosts. You can also use Cash Cards to make ATM withdrawals with your Cash PIN at any ATM. Overall, it’s a really convenient card. Sadly, there’s a scam involving a fake Cash App card. Scammers send out unsolicited Cash App debit cards through the mail. And, they include instructions on how to download the app and scan a QR code to set it up. This is a total scam. Really, the scammer has opened a Cash App account in your name, and they’ve used your stolen information, such as your name and SSN, to do it. The scammer has the account login information, so once you fund the account, they will transfer the money to themselves. Unfortunately, fraudsters have stolen billions of pieces of personal information through hacking and data breaches in the past few years, giving criminals access to your sensitive information. If you receive a Cash App debit card in the mail, and you didn’t request one from Cash App, it’s an indication that your information is available online and that you could be at risk of identity theft. Make sure you contact Cash App through the app if you receive a card that you haven’t requested. 15. COVID Scams Like I’ve said a few times now in this article, scammers play on people’s emotions. One of the things that scammers have used to try to steal money from people is the coronavirus pandemic. Basically, scammers pretend to offer to help people through various fake programs, such as: Coronavirus relief-related giveaway. They might say that because you’re vaccinated you’ve won money. But, then they ask for money or bank account information. So, it’s a scam. A new vaccine or COVID-19 cure. Don’t believe anyone who claims to offer a miracle cure or a new vaccine. Fake grants and relief programs. Scammers create fake sites or send out phishing emails, which claim to offer support to those in need. But to get this service, you have to pay a fee via Cash App. Of course, the service doesn’t exist, and they are just trying to get money from you. Often, it’s not just money that the scammer is looking for. Some might ask for sensitive healthcare information, like your Medicare number. Scammers use this information to conduct medical identity theft and steal your benefits. Some of these scammers will get in touch via phone. You may get a phone call that looks as though it is from a legit government organization. However, scammers can spoof phone numbers to trick your caller ID. So, even though a call may look as though it’s from a government organization, it isn’t. It’s a scam call. So, to be sure that the person who is calling you is legit, hang up and call back using the organization’s official phone number. How to Avoid Cash App Scams You know being scammed is awful, and it happens to millions of people. I know people that have been scammed, and it’s really a terrible thing. That’s why it’s important to be cautious and aware of the types of scams that are out there, and what to look out for. In this section, I just want to share some tips with you that can hopefully prevent you from falling victim to these fraudsters. No one wants to have their money stolen or be the victim of identity theft. Here are some tips you can follow to avoid scams. Never pay for anything online using Cash App Cash App is great for sending and receiving money, but it is not a great payment method for online purchases. Cash App does not offer buyer protection. So, if a scammer is selling a product that doesn’t actually exist, and they ask you to pay by Cash App and you do, then you will never see your money again. When purchasing anything online, be sure to only use payment methods that offer buyer protection, such as PayPal or a credit card. Don’t send sensitive information to someone claiming to be from Cash App support As I said earlier, one of the most common Cash App scams is people pretending to be one of the company’s customer support agents. This is so they can gain access to your account and steal your money. Customer support agents won’t ask you to do any of the following: Provide your sign-in code or PIN. Send payment. Make a purchase. Download any application for “remote access.” Complete a “test” transaction of any kind. If they do, it’s likely a scammer. If someone does get in touch with you claiming to be a support agent, then the best thing you can do is ignore them. Then, contact Cash App using one of its official support channels. This brings me to my next tip. Get in touch with support if you’re unsure if something is legit If you suspect that something is a scam, or if you’re just not sure of whether something is legit, then get in touch with the company. It could be that you have received an email asking you to confirm your account details and you’re not sure if it’s from Cash App. Or it could be that someone says they’ve paid you for something, but they haven’t actually sent any money. In any of these types of situations, get in touch with Cash App support. Doing this can allow you to verify whether correspondence with someone online is actually legit, or if it’s just a scammer. Here are the ways to contact Cash App: Through the app The company says that the best way to get in touch with them is through the app. Here’s how you can contact Cash Support through the app: Tap the profile icon on your Cash App home screen. Select Support. Select Start a Chat and send a message. Or Navigate to the issue and tap Contact Support. By phone While Cash App states that getting in touch through the app is the best way to contact support, you can also call the company. Cash App states that if you are unable to get help through your app, then you can call the company on 1 (800) 969-1940. On social media You can also contact Cash Support on social media. Here are the company’s official social media accounts: Via mail You can also contact Cash App by mail. Here’s the company’s address: Cash App 1455 Market Street Suite 600 San Francisco, CA 94103 Check email addresses Scammers use phishing to try to collect personal and/or financial information through social media, email, phone, or text messages. Often, victims of phishing scams are prompted to click on a link, which goes to a fake site that

looks legit, where they are asked to enter their information. Like I said above, avoid entering information on sites that you have reached via a link in an email, text, or social media message. These are usually phishing scams. Also, check to see who the email is from. Verified emails from Cash App are always sent from the following addresses: @cash.app @square.com @squareup.com If you have an open brokerage account, then you may receive emails from support@drivewealth.com. So, unless an email is from one of those accounts, it is likely a scam. If you get an email, text, or social media message that looks suspicious – i.e., it's asking you to verify your account information, or it's asking for sensitive information of any kind, then contact support. Don't send money to someone claiming to offer something at a future date What a lot of these scams have in common is that they ask for money first, and then claim to deliver something, whether that be more money, an apartment, a pet, or concert tickets, at a later date. This is the case with the Cash App flip scams, the apartment/home rental scam, and the pet deposit scam, for example. You should never pay money in order to get money. Sending someone money so they can flip it for you is always a scam. There are legit ways to get free Cash App money but sending cash to someone so they can flip it for you is not one of them. As soon as someone starts asking you for money, assume it's a scam, and end any correspondence with them. Make sure that giveaways are legit As I mentioned earlier, one of the most common scams on Cash App is the Cash App giveaway scam. Now, Cash App does offer legit giveaways. It often runs sweepstakes that you can enter to win free money. You can keep up to date with Cash App's sweepstakes by following the company on its official Twitter page and/or Instagram page. With these sweepstakes, Cash App often gives away $100s in free cash that's deposited right into your Cash App account. Sometimes, it even offers Bitcoin as the prize. Sadly though, scammers take advantage of these official giveaways in an attempt to scam users out of money. Scammers get in touch with victims to tell them they've won money, but that they have to pay a fee to get their prize. So, you need to be careful with giveaways. Be on the lookout for scams. Only enter sweepstakes from the company's official Twitter account and/or Instagram account. Both are blue tick accounts. If someone contacts you claiming that you have won a Cash App giveaway, and it's not from one of those official blue tick accounts, then it is a scam. Also, it's important to keep in mind that a legit sweepstake will never require you to: Provide anyone with your sign-in code or PIN. Ask you to send a payment. Ask you to make a purchase. Download any application for "remote access." Complete a "test" transaction of any type. If the person who's claiming you have won a giveaway does any of the above, then it is a scam. Never share sensitive personal data If someone gets in touch with you and starts asking for information like your full bank card number or your Social Security Number, it is a scam! No one from Cash App will ever ask you for your sensitive information, like your full debit card number, your bank account information, or your Social Security Number. Like I said above, you have to be aware of people pretending to be customer support agents from the company. But, that's not all. Scammers use multiple methods to extract sensitive personal data from users. They might send a phishing email asking you to verify your account, or they might say you have won a giveaway, but they need your bank details. If anyone online, via text, or by phone ever asks you for details like your Social Security Number, or your banking information, it could be a scam. You should be very cautious. Here are some best practices: Never give out your Social Security Number to people who randomly contact you online, by text, or by phone. A lot of scammers pretend to be someone trustworthy, like a Cash App employee or a government official. If someone calls claiming to be from a government agency, hang up, and call them back on the official number. If you get a text or email that claims to be from an official government agency, ignore it, and again, call them on their official number. Never give out your entire bank account or card number. Cash App may ask you for certain account details so it can verify that it is assisting the right person. But, it will only ask for the last 3 to 4 digits of a linked bank account or card, not the entire number. Don't keep large sums of money in your account Having a large sum of money in your Cash App balance can be risky. If anyone gains access to your account, they could take all of your cash. So, it's best to only keep small amounts of money in your account. If you have a Cash Card, then the money in your Cash App account balance is covered by the FDIC through the company's partner banks (FDIC "pass-through" insurance) in the event of bank failure. The FDIC covers eligible accounts up to $250,000 per Cash App customer. It's important to note that Bitcoin and investing balances aren't covered by FDIC insurance. Your money is only protected though if you have a Cash Card. So, it's best not to keep too much money in your Cash App account. Only send money to people you know and trust One of the simplest tips you can use to stay safe on Cash App and avoid being scammed is to only send money to people that you know, like your friends and family members. And, make sure that you double-check that the recipient's username is correct before you send any payment to confirm that you are sending money to the right person. Also, you can check the recipient's profile to help determine if it is the correct person you're sending the money to. It's so important to verify that you are indeed sending the money to the right account as Cash App to Cash App payments are instant and usually can't be canceled. This means that if you send the money to the wrong person by mistake, Cash App won't usually be able to cancel the transaction or refund you the money. If you only send money to people you know, then you can avoid being scammed by fraudsters who're looking to steal your money. Enable the security lock setting on your account Another really easy tip that I have is to enable the Security Lock setting on your account. When you enable the Security Lock setting, every Cash App payment requires a passcode. So, you can enable a security lock on your account so that a PIN or Touch ID is required to make payments from your Cash App. Here's how: Tap the profile icon on your Cash App home screen Select Privacy & Security Toggle on the Security Lock Enter your PIN or Touch ID Please note that this PIN and your Cash Card PIN are the same. Setting this up makes it harder for hackers and scammers to make payments from your account. So, it's a good idea. Enable payment notifications To avoid scams and keep your Cash App account safe, you want to take as many security measures as you can. One thing you should do is enable notifications so that you are notified after every Cash Payment. You can enable notifications via text message or email so that if a payment is made, you are notified. You can adjust these settings in the profile section of your Cash App. Then, if you see any payments that you haven't made yourself, then you'll be able to change your login details, and report it to Cash App right away. What to Do if You've Been Scammed So, what if you have already been scammed? What do you do then? First of all, don't panic, and don't blame yourself. Anyone can be the victim of a scam. Scammers can be incredibly convincing, and they often use technology such as fake websites or emails that look real. And, they often play on your emotions too. Being scammed sucks, but it happens. I've covered what to do if you've been scammed on Cash App, whether you have had your money taken, your personal information stolen, or a scammer has gained access to your phone or computer. What to do if you sent money to a scammer A lot of scams involve taking money from people. If you have sent money to a scammer, here's what you should do. Contact Cash App Support If you think that you have been scammed out of money on Cash App, then the first thing that you should do is contact customer support. The company says that the best way to get in touch with them is through the app. Here's how you can contact Cash Support through the app: Tap the profile icon on your Cash App home screen Select Support Select Start a Chat and send a message Or Navigate to the issue and tap Contact Support You can also get in touch with customer support by phone. I mentioned this in the "Get in touch will support if you're unsure if something is legit" subsection of the "How to avoid Cash App Scams" section of the post. In case you missed it before, the official Cash App contact number is 1 (800) 969-1940. So, if you find any unauthorized payments or think that you have paid a scammer, make sure that you report it to Cash App. Report the scam to the FTC You should also report the scammer to the FTC. If you paid a scammer on Cash App, then you can report it to the Federal Trade Commission at ReportFraud.ftc.gov. It's a good idea to report the scam to the Federal Trade Commission because you help the FTC and other law enforcement agencies to stop scams. What to do if you gave the scammer your personal information It's not just money that scammers try to steal, but also your personal information. If you have shared personal information, such as your Social Security Number, with a scammer, then go to IdentityTheft.gov to report it. If you gave the scammer your Cash App PIN, then make sure that you change it to a new one. What to do if a scammer has access to your phone or computer If a scammer has remote access to your computer, then make sure that you update your computer's security software, run a scan, and delete anything it identifies as a problem. If a scammer has taken control of your cell phone number and account, then contact your service provider to regain control of your phone number. And, once you do, be sure to change your account password. Also, make sure you check your credit card, bank, or any other financial accounts for unauthorized charges or changes. And, if you see any, then report them to the company or institution, Then, visit IdentityTheft.gov to see what steps you should take. Cash App Scams Summary While Cash App is a legitimate app that allows you to send and receive money easily, it's prone to scammers. So, it's important to be aware of the Cash App scams that are out there so that you can avoid them. Avoiding scams allows you to keep your money, and your personal information safe. So, be aware of the scams that we listed above, and make sure you follow our tips on how to avoid Cash App scams. If you have been scammed, then please follow the tips in our "What to do if you've been scammed section above." Hopefully, this post helps you to be more aware of the Cash App scams that are out there and use Cash App safely. Portland, OR, USA - Jan 5, 2022: Payment apps like PayPal and Venmo are seen on an iPhone on top of ... More Form 1099-k. Third-party payment apps now have to report transactions more than USD600 to the IRS.getty It's amazing how many ways you can send money to your friends. I still remember when PayPal PYPL was the only way, but nowadays, you can send money through Venmo, Cash App, Zelle, and several others. The challenge with all of them is they each work slightly differently, and the average person can be quite unsuspecting. When it becomes this easy to send money, scammers have figured out ways to trick people into sending it to the wrong person. And with many of these apps, it's hard to recover your money if you make this mistake. To protect yourself and your money, it's essential to know how these Cash App scams work so you can see the common red flags and avoid being taken advantage of. Cash App was developed by a company called Block SQ . Block is a publicly traded mobile payment company that runs several other apps, such as Square, Afterpay, and Tidal. Cash App is Block's payments app, and it's a financial services platform — partnering with Lincoln Savings Bank and Sutton Bank — that offers bank-like services. The benefit of using Cash App is the convenience. You can send money to a friend without paying a fee, which is helpful if you're splitting a bill or otherwise owe someone some money. As you'd expect with an app that makes it easy to send money to someone else, scammers have tried to figure out ways to use it to their advantage. There are a lot of Cash App scams. Here are a few examples: Scam Payment Requests Scammers can target Cash App users by sending them payment requests with misleading or fake information. They may use fake profiles, posing as friends or familiar businesses to trick users into accepting these payment requests. Sometimes, they even send money to the Cash App user and then say it was an accident. Then they ask for a refund, but the money was initially sent from a hacked or stolen account. The user sends back the money, but now they're left with the headache of dealing with the original fraud. Fraudulent Or Spoofed Cash App Support Calls Another common scam is when someone contacts you and claims to be part of the Cash App support staff. This happens with credit cards and banking very often. They will contact you and ask you for sensitive information, such as your password or PINs. Sometimes they'll ask you just to confirm some information, which seems innocent but has an ulterior motive. If someone ever calls you claiming to be from Cash App's support team, politely hang up and call the bank yourself. This is the only way to know whether you're speaking to someone legitimate. Winning Prizes Or Sweepstakes You Never Entered Have you ever won a prize for a contest you never entered? No, it's not plausible. But scammers will try to trick you into believing you've won something; you just need to pay a small fee to get your reward. Maybe you won a car and can claim it once you've paid the taxes for it. Perhaps you won a sweepstakes and need to give them your banking information so they can deposit it. Scammers are very sneaky and very clever. But if you really won a Cash App prize or sweepstakes, the company would have your information already and can deposit it into your account directly. How To Avoid Cash App Scams The key to avoiding all Cash App scams, and many scams in general, is to be skeptical about everything. Don't respond to messages, calls, or requests from strangers. Don't give your information out to anyone. Don't believe anything anyone says unless you know them and can see them in front of you. You avoid many common Cash App scams by being extraordinarily cynical and skeptical. What To Do If You're Scammed Sadly, even the most diligent users can still get scammed. We all make mistakes. If it does happen to you, report it to Cash App. Open Cash App on your phone Tap your profile picture at the top right Scroll down and tap "Support" Scroll down to "Chat" Explain your situation and the scam Alternatively, you can call 800-969-1940 Next, you'll want to let any affected bank or credit card companies know that you've been scammed. Based on the specifics, they along with Cash App can advise you on what to do next. Finally, you can file a complaint with your local police department or the Federal Trade Commission.