Protecting Yourself From Gift Card & QR Code Scams

Be Aware !!!!!!!

Gift Card Scams Are Very Sophisticated

FBI: EL PASO, TX — Gift cards have become a staple for any special occasion. They are readily available at any store for our shopping ease. Scammers have come up with another way to take money from the gift cards we purchase for family and friends.

Scammers place fake barcodes on the back of real gift card barcodes in the stores. When you purchase the card, the cashier scans the fake barcode at the checkout, which quietly pushes your money into the scammer's gift card account, leaving you with a zero balance.
Protect yourself by examining the back of the gift card before buying it. Check for signs of tampering. Make sure the gift card's barcode number, which is visible through the window on the back of the gift card's packaging, matches the number on the packaging itself. Don't purchase if the barcode is on a sticker, or if the package is ripped, wrinkled, bent, or looks tampered with.
Don't pull off the first gift card from the rack. Try to get one in the middle or the back. Even then, there's no guarantee that it hasn't been tampered with so make sure you're closely inspecting all gift cards.
Pay attention to what's displayed when it's scanned at checkout to make sure it matches.

If you have been victimized by an online crime, make a report to the FBI. You can file an online report at the FBI's Internet Crime Complaint Center at www.ic3.gov or call the FBI El Paso Field Office at (915) 832-5000.

Gift Card Consumer Scam Tips

Only scammers will tell you to buy a gift card, like a Google Play or Apple Card, and give them the numbers off the back of the card. No matter what they say, that’s a scam.

No real business or government agency will ever tell you to buy a gift card to pay them.

Always keep a copy of your gift card and store receipt.
Use them to report gift card scams to the gift card company and ask for your money back.

How Gift Card Scams Work

Gift card scams start with a call, text, email, or social media message. Scammers will say almost anything to get you to buy gift cards — like Google Play, Apple, or Amazon cards — and hand over the card number and PIN codes. Here are some common tactics scammers use in gift card scams:

Scammers will say it's urgent. They will say to pay them right away or something terrible will happen. They don't want you to have time to think about what they're saying or talk to someone you trust. Slow down. Don't pay. It's a scam.

Scammers will tell you which gift card to buy (and where). They might say to put money on an eBay, Google Play, Target, or Apple gift card. They might send you to a specific store — often Walmart, Target, CVS, or Walgreens. Sometimes they'll tell you to buy cards at several stores, so cashiers won't get suspicious. The scammer also might stay on the phone with you while you go to the store and load money onto the card. If this happens to you, hang up. It's a scam.

Scammers will ask you for the gift card number and PIN. The card number and PIN on the back of the card let the scammer get the money you loaded onto the card — even if you still have the card itself. Slow down. Don't give them those numbers or send them a photo of the card. It's a scam.

Common Gift Card Scams

Scammers tell different stories to get you to buy gift cards so they can steal your money. Here are some common gift card scams:

Scammers say they're from the government. They say they're from the IRS, the Social Security Administration, or even the FTC. They say you have to pay taxes or a fine. But government agencies won't contact you to demand immediate payment, and they never demand payment by gift card. It's a scam.

Scammers say they're from tech support. They say they're from Microsoft or Apple and there's something wrong with your computer. They ask for remote access, and say to pay them to get it fixed. Don't give them access to your computer. It's a scam.

Scammers say they're a friend or family member with an emergency. If the scammer uses voice cloning, they may even sound just like your loved one. They ask you to send money right away — but not tell anyone. It's a scam. If you're worried, contact the friend or relative to check that everything is all right.

Scammers say you've won a prize. But first, they tell you to pay fees or other charges with a gift card. It's a scam. No honest business or agency will ever make you buy a gift card to pay them for a prize. And did you even enter to win that prize?

Common Gift Card Scams

Scammers say they're from your utility company. They threaten to cut off your service if you don't pay immediately. But utility companies don't work that way. It's a scam.

Scammers ask for money after they chat you up on a dating website. Romance scammers will make up any story to trick you into buying a gift card to send them money. Slow down. Never send money or gifts to anyone you haven't met in person — even if they send you money first.

Scammers send a check for way more than you expected. They tell you to deposit the check and give them the difference on a gift card. Don't do it. It's a scam. That check will be fake and you'll be out all that money.

Buying & Using Gift Cards

Gift cards are for **gifts**. Only gifts. Not for payments. Never buy a gift card because someone tells you to buy one and give them the numbers. Whenever you buy gift cards:

Stick to stores you know and trust. Avoid buying from online auction sites because the gift cards may be fake or stolen.

Inspect the gift card before you buy it. Make sure the protective stickers are on the card and that it doesn't look like someone tampered with them. Also check that the PIN number on the back isn't showing. Pick a different gift card if you spot a problem and show the tampered card to a cashier or manager.

Always keep a copy of the gift card and store receipt. Take a picture of the gift card and store receipt with your phone. The number on the gift card and store receipt will help you file a report with the gift card company if you lose the gift card or if you need to report fraud.

Fake Barcodes

One common scam involves fraudsters applying fake barcodes to the backs of gift cards in stores — so that when you activate the card, the money is sent to the scammer's gift card instead of yours.

Fake Security Labels

Scammers may also scratch off the material covering the card's number and PIN (and cover it with a similar silver sticker).

QR Codes - Easy To Use For Scamming

- Cyber criminals posing as real companies send phishing emails with a QR code and ask users to scan it. Then, they attempt to obtain information or spread virus-infected files. Another common scam is the false QR code stuck on top of an original one, like in restaurants and street advertising.

QR Codes - Easy To Use For Scamming

Check to make sure you cannot scratch or peel the QR Codes off

They should be “Under” the laminate or printed “Directly” on.

At The Register Or For Payment

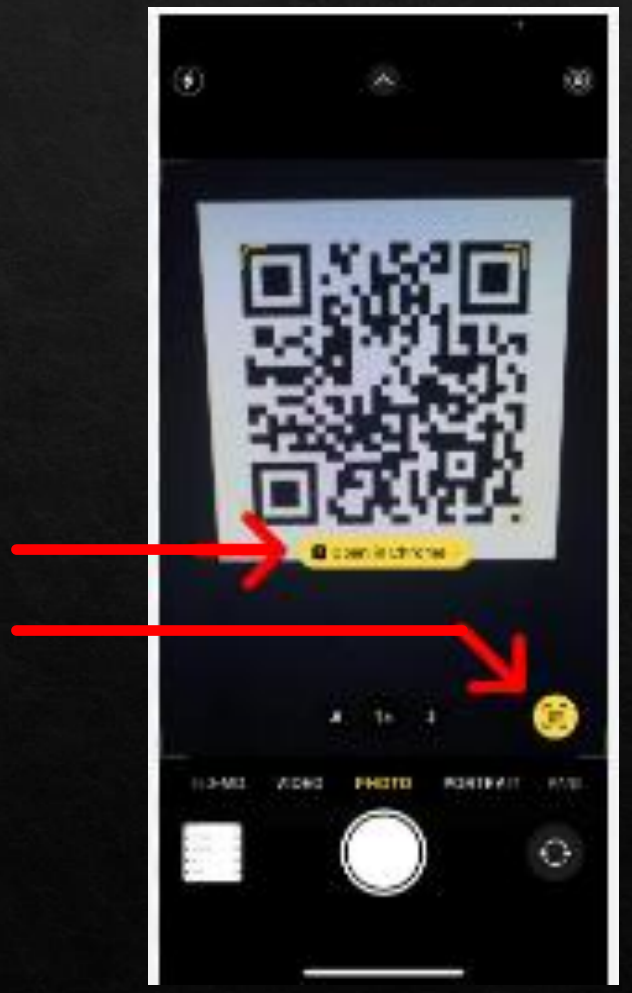
- Scams that use inv
- Scammers first cre ed payment method.
- But the code does er scanned it. Instead of paying the merc makes the merchant and the customer
- This type of scam details.

How To avoid A QR Scam

- Before scanning a QR code, like in a restaurant or some other public space, check that it hasn't been tampered with or got a sticker placed over an original code.
- Installing anti-virus software to verify original QR codes that do not contain malicious links will help you avoid having a virus or other malware downloaded onto your mobile.
- Double-check the preview of the QR code link. When you scan a QR code, a preview of the URL should appear. Make sure the website address is legitimate. Look for a padlock symbol and an address that begins with "https://". Only those URLs are secure.
- Think twice if the app or website you're being directed to asks you to provide personal details. If it does, make sure it's authentic.
- QR Codes Using iOS QR Codes Using Android

How To avoid A QR Scam

- When you scan a QR Code, you will see the translation link as well.
- Look at it.
- To open (go to the link), select the “Yellow” text or the “Yellow” box.



Validating A QR Code

??? QUESTIONS ???