5 Common Consumer Credit Card Scams

+ 10 Tips for Protecting Yourself From Credit Card Fraud

Credit card scams are all too common today. Are you wondering why your bank is calling you? It's probably not really your bank. Does the deal sound too good to be true? Then it probably is. Protecting yourself as a consumer means being aware of the scams that exist. Below are 5 common schemes seen in the market today.

Scam No. 1: 'Hi, This is Your Bank Calling'

Fraud rings will often make calls that sound a lot like this. “Hi this message is for [Cardholder]. I’m calling from [a bank’s lending service] in regards to a personal matter. Please give us a call back at [800 number] to speak to one of our representatives. Our hours of operations are Monday through Friday from 8 a.m. to 10 p.m, Eastern Standard time. Thank you.”

The problem? This isn’t your bank, but they’ll offer to “transfer” you to your bank. They know critical details, like cell phone number and what type of card you have, but they rely on the consumer to fill in the blanks. Avoid this by hanging up and calling your bank back to confirm details of the call. They’ll alert you if it is part of a scam.

Scam No. 2: 'The Great Timeshare Vacation Deal'

The scammers offered 4-day/3-night trips for extremely attractive prices for those willing to attend a 2-hour timeshare presentation. The fraudsters asked for an address, credit card information and birthday to confirm the identity of the buyer. They'll even provide an 800 number to call.

The problem? Most people will give out a credit card before they realize it's a scam. This timeshare vacation sounds very similar to the same types of calls telemarketers offer to get people to buy into vacation deals. By learning some basic information (name and cell phone numbers), the fraudsters quickly gained access to financial details.

Scam No. 3: ‘There’s Been Fraudulent Activity on Your Account’

This scam will sound a lot like this. “Hi, we’re calling for [name], about suspicious activity on your account. We’re calling from a [bank’s] fraud department in reference to claim number [will give actual claim number].” They will then tell you that they are removing the fraudulent charges — but not before asking for your address and other personal credentials. That data is then used to make fraudulent purchases.

The Problem? Like similar fraud schemes, the fraudsters will gain droves of personal information without the consumer even realizing they are vulnerable to credit card fraud, or an account take-over from a fraudster. Be aware that even the most reputable sounding callers can be part of massive fraud rings that are attempting to scam dozens of cardholders in just minutes.

Scam No. 4: 'Click Here to Update Your Netflix Information'

Bogus emails are being sent to Netflix subscribers telling them to update their information. The fraudulent link then leads them to a fake Netflix site, which then prompts them to enter personal information and credit card numbers. This common scam targets major reputable brands and uses an email phishing scam to lure users to give out credit card information without thinking twice. A friendly reminder: Subscription services like Netflix won’t ever send these types of emails so be wary of ones that do.

The Problem? Phishing scams like this are so sophisticated the user doesn't often realize it's a scam until it's too late. The email will appear to be from Netflix, and it will link to a page that looks exactly like Netflix's homepage. This makes it difficult for a consumer to spot a scam.

Scam No. 5: BBB Warns of Amazon Fake Email Scam

The Better Business Bureau has warned consumers about a credit card phishing scam that involves fake emails appearing to be from Amazon. The links in the emails, however, send the user to a site that automatically allows hackers to take over your computer. From there, programs are automatically downloaded on your computer and malware is often installed that demands the user to pay a ransom before they can get access back.

The Problem? In these types of scams, credit card details and account information are typically compromised. They are hard for consumers to spot and they cause incredible damage to your financial health. Avoid clicking on unsolicited emails asking for you to verify account details.

10 Tips for Protecting Yourself From Credit Card Fraud

In an era where credit card scams are running rampant, consumers must be more in tune with the risks that exist today. Banks and credit card companies are working diligently to protect your personal credentials and financial information, but fraudsters are still finding sophisticated and creative ways to hack into bank accounts and steal credit card numbers. This problem isn't going away anytime soon.

Below are 10 ways you can help prevent yourself from falling victim to credit card fraud.

1

Protect Your Cardnumber

Never give your credit card number on the phone unless you can confirm you are talking to your actual bank/credit card company.

2

Safeguard Your SSN

Never give your full social security number over the phone (your bank/credit card company will never ask for it).

3

Confirm the Caller is Legitimate

Don't confirm personal financial data by phone. Hang up and call the number provided on the back of your credit card.

4

Be Wary of Email Communication

Be cautious when providing personal information from email solicitations. Your bank/credit card company won't use this method.

5

Report Odd Activity ASAP

When you see something suspicious on your credit/debit card, call your credit card issuer immediately.

6

Be Careful Where You Shop Online

Ensure a website is secure. Look for lingo about security features and data protection during checkout. Sites with https tend to be more secure; Do not enter personal info or passwords on sites with only http.

7

Use Secure Passwords

Don't fall victim to credit card fraud over an easy-to-hack password. Use unique passwords that don't use your name, birthdate or other features linked to your identity.

8

Safeguard Your Personal Details

Never give out unsolicited personal information. Your bank/credit card company will never call out of the blue asking for you to confirm this information. Always confirm details on your own.

9

Be Cautious Of Links

Never click on email links about your account. Confirm with your actual bank or credit card company first. These links may lead you to fake sites, which steal your information.

10

Watch for ATM Skimmers

Be cautious when using your credit card at ATMs, particularly store ATMs as they are target for fraudsters looking to skim credit card details from these machines.

Want to receive alerts about ongoing card fraud threats and data breaches?
Visit **Rippleshot.com** to sign up for our weekly newsletter