Why You Can Trust CNET

Advertiser Disclosure

Our expert, award-winning staff selects the products we cover and rigorously researches and tests so you can buy with confidence. If you buy through our links, we may get a commission. Reviews Process

Editorial Standards

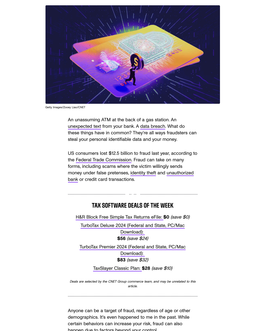
Home

Want to Keep Your Money Safe From Fraudsters? Stop Making These Mistakes

Your online information isn't as safe as you think. Here are the most common ways fraudsters steal it, along with your money.

Rahna Ito
April 1, 2025 5:00 a.m. PT

5 min read



Getty Images/Sanna Lien/CNET

An unassuming ATM at the back of a gas station. An unexpected text from your bank. A data breach. What do these things have in common? They're all ways fraudsters can steal your personal identifiable data and your money.

US consumers lost $12.5 billion to fraud last year, according to the Federal Trade Commission. Fraud can take on many forms, including scams where the victim willingly sends money under false pretenses, identity theft and unauthorized bank or credit card transactions.

TAX SOFTWARE DEALS OF THE WEEK

H&R Block Free Simple Tax Returns of Sc $0 (save $0)

TurboTax Deluxe 2024 (Federal and State, PC/Mac Download): $58 (save $24)

TurboTax Premier 2024 (Federal and State, PC/Mac Download): $83 (save $32)

TaxSlayer Classic Plan $26 (save $10)

Deals are selected by the CNET shopping commerce team, and may be unrelated to this article.

Anyone can be a target of fraud, regardless of age or other demographics. It's even happened to me in the past. While certain behaviors can increase your risk, fraud can also happen due to factors beyond your control.

How fraudsters steal your information and money

A lot of fraud occurs when thieves gain access to a victim's bank account or credit card information and make unauthorized purchases or transfers. But how do they get that information in the first place?

Here's a rundown of the biggest threats to your financial accounts and how to protect yourself.

Database breaches

When your data is stored with a third-party service — such as your utility company, internet provider or a retailer — and that service is hacked, your information can be handed into the bad actors. Take the latest Ticketmaster breach, which compromised some 560 million users' information, including names, emails and some card numbers.

Advertisement

NAVIGATING A WORLD OF ACCELERATING CHANGE CNET

"Database breaches and other compromises of third-party services are far and away the most common cause of financial fraud," said Aaron Walton, senior threat intel analyst at cybersecurity firm Expel.

How to protect yourself: While you can't prevent third-party service breaches, you can minimize the impact of a data breach on you. For starters, don't store data with third-party services beyond what's necessary. Walton recommends using single-use virtual credit cards for online purchases so that even if the card number is leaked, a criminal can't make additional purchases with the card.

Bad password security

"If you reuse passwords, you are just asking for your accounts to be taken over," said Truman Kain, senior product researcher at cybersecurity firm Huntress. "This is the number one worst thing you can do if you want your accounts to be protected."

After a data breach, attackers will try to use stolen credentials at major online accounts like banks, retailers and email providers. The process is called credential stuffing. Using weak, guessable or common passwords also makes it easy for hackers to get into your accounts, Kain added.

How to protect yourself: Use strong, unique passwords across all your accounts and change them regularly. Your passwords should be long (experts suggest 16 characters) and contain a combination of lowercase and capital letters, numbers and symbols. If that sounds like too much, consider getting a password manager. Kain also recommends enabling multifactor authentication on your accounts wherever possible.

Credit card skimmers

Skimmers are devices attached to the mouth of a card reader that steal your credit card data when you swipe your card. The skimmers then send that information directly to a card thief or save it for retrieval later.

Skimmer setups might also include a hidden camera or fake keypad to capture your PIN. Skimming can even happen online. If an attacker can compromise a website, they can "skim" information from any new transactions taking place.

Advertisement

NAVIGATING A WORLD OF ACCELERATING CHANGE CNET

How to protect yourself: Before using an ATM or payment terminal, check it for a loose card reader or any signs of tampering. Don't insert your card if you notice anything suspicious. Criminals tend to install skimmers in low-traffic areas to minimize the chances of being caught, so stick to payment terminals and ATMs in high-traffic or well-monitored areas.

If possible, use tap to pay — which is less vulnerable to skimming — instead of swiping your card. If you're using a debit card, run it as a credit card (if you can) to avoid entering your PIN and having a thief steal that information. To be extra cautious, you might also use or limited-use virtual cards when shopping online.

Phishing and other social engineering attacks

Aside from data breaches, phishing attacks are the primary way attackers get ahold of your credentials, Kain said.

Phishing is when a scammer contacts a target, usually under the guise of a legitimate institution, to trick you into handing over sensitive information, usually via a link they want you to click. Phishing attacks can occur over phone, email or text.

How to protect yourself: A good rule of thumb is, "If you didn't request the message, you should be suspicious of it," Kain said. If you need to verify whether a message is legitimate, directly contact the institution through contact information found on its website.

You should also be skeptical if someone online says you owe them money or have an outstanding payment, Walton said. "Take it slow and approach with caution," he said. "Don't let a false sense of urgency lure you into a costly mistake."

Data stolen over unsecure Wi-Fi networks

Visiting websites that don't encrypt traffic with "https" security on public Wi-Fi allows cybercriminals to see anything you do online. Cybercriminals can also steal your data by setting up fake public Wi-Fi hotspots.

After you connect to the free Wi-Fi, "the attacker can redirect you to fake websites that closely mimic the real thing, capturing your logins, passwords and sensitive data as you enter them," Kain said.

How to protect yourself: Avoid public Wi-Fi for sensitive transactions. It's smart to protect yourself with a virtual private network. A VPN encrypts your browsing activity so even if your data is intercepted, it's unreadable.

"Using a reputable VPN is like sealing your internet traffic inside a secure envelope," Kain said.

Other proactive ways to prevent fraud

Despite the real and serious risks from fraud, 26% of bank customers and 31% of credit card customers haven't taken any recent steps to keep their accounts secure, per J.D. Power's 2024 US Financial Protection Satisfaction Study released in November.

If you want to be more proactive about protecting yourself, here are the strategies experts recommend.

Card controls

Many banks and credit unions offer card controls that let you lock and unlock your credit and debit cards online or on a mobile app. Locking cards you don't use regularly and unlocking them only when you need to make a purchase can help prevent unauthorized transactions from going through.

Freeze your credit

Freezing your credit will keep lenders from accessing your credit reports, which prevents scammers and identity thieves from opening new credit accounts in your name. If you need to apply for a new loan or credit card, you can temporarily lift the freeze and refreeze your credit after.

Use a virtual card

Both Kain and Walton recommend using virtual cards to protect your credit card information from being stolen. Virtual cards are randomly generated card numbers connected to your real card. You can set usage limits on virtual cards, such as being only good for one purchase, rendering them useless even if a scammer steals the card information.

Setup account alerts

Criminals will often put small purchases on a stolen credit card to test out the card before using it for larger purchases or selling the card information on the dark web. If you can catch the small fraudulent transactions as soon as they happen, you can lock down the card before any big ones occur. To do this, you can set up alerts for all transactions or purchases under a certain dollar amount.

How to report credit card or bank fraud

If you think you're a victim of fraud, report it to your financial institution immediately. Most banks have a designated phone number for urgent assistance. You can then place a lock on your credit or debit cards to prevent new purchases from going through. Your bank might cancel the compromised card altogether and send you a new one.

In some cases, such as if your Social Security number or other sensitive information was compromised, you might also want to implement a credit freeze or sign up for identity theft protection. The latter will help monitor your identity online and can sniff out signs of fraud. You may also want to change your password for your financial account and any online account with the same login information.

Aura

AURA

CNET's pick for the best identity theft protection service

See at Aura

Rank

Protect your personal data and get peace of mind with CNET's top pick for identity theft software.

Finally, it's always a good idea to report the fraud to the FTC at reportfraud.ftc.gov to help the federal government thwart scams.

"In many situations, some forms of help are available, be it from an employer, law enforcement or elsewhere," Walton said. "It is a mistake to believe no one can help or that one should be ashamed of being tricked."

The editorial content on this page is based solely on objective, independent assessments by our writers and is not influenced by advertising or partnerships. It has not been provided or commissioned by any third party. However, we may receive compensation when you click on links to products or services offered by our partners.

© 2025 CNET, a Ziff Davis company. All rights reserved.