Application deadline is Feb. 28 for the AARP Purpose Prize, which honors people 50 and older who tap into life experience to build a better future. Find out more. ›

SCAMS & FRAUD

Chip Card Scam Turns Security Feature Into Security Risk

Your bank will never ask to 'secure your account' by taking the protective chip on your bank card

By Matt Alderton, AARP Comments

Published October 11, 2024

PHOTO ILLUSTRATION: MATT CHASE

Whether you use it to buy groceries, gas or clothing, you probably swipe your credit or debit card multiple times a day at payment terminals. These EMV cards, as they're known, have a small computer chip in the corner that you insert or "dip" into payment terminals. That chip is meant to make your transactions more secure than they were in the days when we used to swipe our card's magnetic stripe through payment terminals. The chip, for one, makes it far more difficult for criminals to produce counterfeit cards.

But after nearly a decade of watching consumers dip rather than swipe (chip cards were introduced in 2015), scammers have realized that they don't have to duplicate EMV cards in order to hack them. They just need to steal the chips — and, unfortunately, they've figured out a way to convince people to hand them over.

Subscribe to the Sisters Newsletter From AARP newsletter
A free email newsletter celebrating Black women—we hope to inspire and uplift you.

How the chip card scam works

The FBI explained in a recent alert what the scam typically looks like:

It starts when a scammer calls you claiming to work for your bank. They may have even spoofed your bank's phone number, in which case the caller ID will look authentic. In a ruse to make you concerned about suspicious activity on your account, they'll likely ask about recent transactions you've made, which they might be able to see by logging into your account with your username and password. They probably have other personal information, too, like your address and account number. Although the FBI says it's unclear how scammers are getting this sort of personal data, it's likely that they're harvesting it from the dark web.

At this point, the call probably seems legit. Naturally, you become alarmed. While you're in a state of heightened anxiety, the scammer says the bank needs to send a courier to pick up the card so they can immediately secure it. Minutes later, possibly while you're still on the phone, the supposed courier arrives to collect the card. They cut your card in half on the spot, but keep intact the embedded chip, which they take with them. If they don't already have it from the dark web, scammers might also persuade you to volunteer your PIN.

With your chip and PIN in hand, the criminals can promptly use it to steal money from your account or ring up thousands of dollars in charges. Sometimes, however, the theft occurs much later, says Paige Schaffer, CEO at Iris Powered by General, an identity and cyber protection company owned by multinational insurance company Generali. "So, you might hand over your chip, and then it will be six months or a year — once you've let your guard down — before they start using it," she says.

Joshua Lee, a sergeant for the Mesa Police Department in Mesa, Arizona, has seen a variation of the same scam, where "victims were instructed to mail their cut credit cards to a fictitious processing center, which was a forwarding post office box," Lee says. "Once the criminals receive the cut cards, they simply just use the portion containing the EMV chip to make purchases."

A scam perpetrated both online and in person

What makes chip card scams especially alarming is their physical component. "Most bank-fraud scams are done entirely online. This scam uses both online and in-person criminals," says Lee, who adds that chip card scams are "highly targeted."

The criminal often knows the victim's name, address, phone number and the issuing bank of the bank card, he says. They might have purchased that information from the dark web, or they might have hacked the victim's accounts. Unwittingly, you might have even volunteered the information yourself through prior fraudulent contacts, like text messages that appeared to be from a trusted person or business.

ENTERTAINMENT
AARP Theater
Free plays, concerts, musicals, dance performances and more

Scott Anchin, vice president of senior operational risk and payments policy for the Independent Community Bankers of America, echoes Lee's concern. "When someone comes in person, I think it leads you to trust the scammer more," he says, "because you assume that if someone's coming to your house from the bank, it must be serious."

Another issue, Anchin adds, is personal safety: "When you're dealing with scammers over the phone or via digital channels, they can take your money but they can't hurt you. When someone is coming to your home and initiating personal contact, it raises a whole new level of alarm."

There's no way to track how many people have been victims of chip card scams, but experts say they don't seem to be very common — for now. "My sense is that this is not especially widespread, and I think that's because it requires a certain level of boldness for the scammers," Anchin says. "It's a huge risk for the criminal. But I think as we go forward, these types of sophisticated, personal-contact scams will start to become more and more common."

Are chips still safe?

Chip cards are "absolutely" safe to use, according to Anchin. "A chip is fundamentally more secure than a magstripe," he says. "Account information cannot be stolen from the card because it's all encrypted on the chip."

"It's the best form of security that we have right now," says Craig Kirkland, executive vice president and director of retail banking at Nevada State Bank, which operates branches and offices in 20 communities across the state. "But you have to be wise and prudent in protecting it."

How to protect yourself from chip card scams

Be proactive. Chip card scams typically begin with a call from your "bank" notifying you about fraudulent transactions. If you proactively monitor your bank accounts for suspicious activity, you'll therefore be one step ahead of scammers, says Schaffer, who recommends setting up bank alerts and notifications to keep tabs on charges to your account. That way, you can contact the bank if something's off instead of waiting for them to contact you. If a scammer does call, you'll be less susceptible to the attack, knowing that your bank is already on alert.

Don't answer the phone. "The most important thing is: Don't trust anybody that calls you," Schaffer says. Better yet, don't pick up the phone if they caller isn't in your contact list.

How chip cards work

The magnetic stripes on conventional payment cards contain personal information like your name, address and credit card number, which they transmit directly to the payment terminal every time you make a transaction. The chips in EMV cards — EMV stands for "Europay, Visa and Mastercard," the credit card companies that created and promoted chip technology — work differently. During transactions, they don't transmit your information to the payment terminal. Instead, they generate and transmit a one-time, tokenized account number. Because the merchant never receives your actual card number, hackers can't steal it during a data breach.

Call your bank directly. In case you do answer a call that you believe to be from your bank, it's important to know what banks will and will not do by phone. "In legitimate fraud cases, the bank will text message the consumer directly," Lee says. "They may even call the consumer to alert them to a fraudulent charge. But if a real bank calls anyone, they will instruct that person to hang up and call the bank's fraud hotline. They won't try to get any personal information."

Kirkland adds that a bank is never going to send someone to your home to pick up anything. If your bank calls you for any reason, he says, hang up and call them back directly at the customer service number that's printed on the back of your card or at the top of your bank statement.

Protect your card — and dispose of it properly. Store your card in a safe place and never entrust it to a stranger. And dispose of it properly when you no longer need it. "If you have a chip in a chip card that you want to dispose of — maybe it's expired or something like that — you need to make sure that you destroy the chip itself," Anchin says. "A shredder will do this. A pair of scissors will do this. And some banks even have opportunities to go into the branch and return your card for recycling."

Safeguard your PIN. To be successful, chip card scams typically require not only the chip from your bank card, but also your PIN. With both, scammers can make debit card transactions at stores and also withdraw cash from ATMs. For that reason, it's important to practice good PIN hygiene, Kirkland says. "Use sequences that are unusual and not tied to personal information, like your birth date or phone number," he says. "Changing your PIN from time to time is another good way to protect yourself."

Report fraud. If you've been victimized by a chip card scam, report it to your bank, the FBI at IC3.gov, and your state's attorney general. Even if you can't recoup your losses, the information could help government agencies, law enforcement officers and financial institutions identify trends and maybe even catch scammers to prosecute them.

Matt Alderton is a contributing writer who specializes in health and wellness, travel and technology. His work has also appeared in USA Today, *Forbes and* The Washington Post.

HAVE YOU SEEN THIS SCAM?
- Call the AARP Fraud Watch Network Helpline at **877-908-3360** or report it with the **AARP Scam Tracking Map**.
- Get **Watchdog Alerts** for tips on avoiding tech scams.

Report a Scam
Sign Up for Watchdog Alerts

TWO MORE YEARS OF MEMBERSHIP ONLY $25 WHEN YOU SWITCH TO AUTOMATIC RENEWAL
Plus, receive a gift. Expires 3/18.
Update to Auto Renew

AARP NEWSLETTERS
Get expert money tips with Money Matters
Manage your money confidently with expert tips on spending, saving, and budgeting!
Subscribe
See All Newsletters
Privacy Hub

More From AARP

Avoid Airline Scams When Booking Your Next Flight
Common schemes involve fake booking sites and bogus customer service reps

Fraud Victims Hit Again by Scammers Promising to Recover Stolen Cash
Be aware of criminals' touting recovery scams when you're feeling desperate to be made whole again

What to Do If You've Just Been Scammed
How one woman worked quickly — with help — to avoid being charged through PayPal
MEMBERS ONLY

Recommended For You

POLITICS SOCIETY
AARP Fights to Protect Medicaid Amid Threat of Funding Cuts
We've joined a coalition of organizations advocating to safeguard this essential health coverage

ENTERTAINMENT
The 12 Best Things Coming to Netflix in February 2025
See Robert De Niro's 'Zero Day,' Amy Schumer's 'Kinda Pregnant,' the 'Kobra Kai' finale and more

HEALTH
6 Ways to Lower Your Blood Pressure Without Medication
Try these tactics to help fight hypertension and bring your numbers down

HEALTH
How Older Adults Can Survive the Quad-emic
Lower your risk of illness amid the convergence of COVID, flu, RSV and norovirus

ADVERTISEMENT

Benefits Recommended For You

See All ›

ENTERTAINMENT
AARP Streams App
Watch Movies for Grownups and AARP Theater for free on the app

ENTERTAINMENT
AARP Theater
Free plays, concerts, musicals, dance performances and more

MEMBERS ONLY
TRAVEL
AARP Travel Center Powered by Expedia: Vacation Packages
$50 gift card of your choice when booking any flight package

HEALTH & WELLNESS
AARP® Prescription Discounts provided by Optum Rx®
Free Rx discount card for use at over 66,000 pharmacies nationwide

Captured by FirstShot Pro: 25 February 2025, 17:25:21
https://getfirstshot.com