Credit card scammers are using this tactic to bury bank fraud alerts

Michelle Singletary

Scammers have found a way to hide their credit card fraud that is as frustratingly effective as it is diabolical.

“I don’t know if you have reported on this twist on credit card fraud, but I thought I would tell you my story in case it can help others,” a reader emailed.

This reader, who asked not to be identified to protect her privacy and avoid being targeted again, shared a tactic I had not heard of before.

Here’s what happened to her.

She received a text from her bank asking whether she had made an online purchase of a $1,200 laptop. The charge was put on hold, awaiting her response. The message appeared legitimate because it came from a number that had previously sent valid fraud alerts. She replied, “No.”

The bank texted back that because the purchase was unauthorized, her card was frozen and she was instructed to call its fraud department.

Let me stop here.

If you haven’t done this already, sign up to receive text messages, emails and even phone calls from your financial institution so they can reach you in various ways about suspicious activity. I’ve authorized all three forms of communications for every one of my bank accounts, credit cards and investment accounts.

But I’ve told you to trust nothing. So, when you get that text, email or phone call, double-check it’s truly your financial institution trying to reach you.

Although the reader was confident the text message was legit, she didn’t call the number she was given.

“I looked up the phone number on my bank’s website and called,” she said.

This was the right move!

If you search online, you have to be careful you don’t land on a fake site. Look for a contact number on your statements, through the credit union or bank app, or on the back of your debit or credit card.

Now for the twist.

While waiting to speak with a bank representative, the reader checked her email for additional notifications about the compromised card. She was not prepared for what she found.

“I discovered the scammers had simultaneously signed me up to hundreds of websites and online

newsletters, all of which then simultaneously sent me either welcome emails or 'confirm your email' messages," she wrote.

She had received more than 600 emails, including many that ended up in her spam folder. Hundreds more continued to arrive over the next 24 hours. Because many came from legitimate organizations — university newsletters, charitable organizations and real small businesses — they landed directly in her main inbox rather than her spam folder.

Here's the evil genius behind the blitz: Buried in that mountain of noise was an email from her bank about the suspicious $1,200 transaction.

"Clearly the scammers wanted to spam my inbox so I wouldn't notice the fraud alert," she suspected.

She was right.

The ordeal she experienced is called "email bombing," also known as subscription or spam bombing.

Rather than hacking your phone or spoofing your bank's number, fraudsters use automated bots to submit your email address to hundreds of online sign-up forms simultaneously.

The objective is to flood your email inbox so you overlook real-time alerts from your bank. This buys the thief or criminal syndicate time to complete unauthorized transactions, hide account change notices or access other compromised accounts.

In other cases, the goal isn't credit card fraud. Scammers create chaos in your inbox so that when someone impersonating a "tech support agent" calls offering to stop the spam, you are stressed enough to pay for their fake cleanup service.

The relentless wave of data breaches leaves everyone vulnerable. Fraudsters can easily purchase credit card details on the dark web. The information often includes your name, address, phone number and email address.

Had the Virginia resident not received the text from her bank, she might have missed the alert her credit card issuer had also sent to her email address regarding the fraudulent $1,200 laptop transaction.

"I almost certainly would have missed it," she said. "I would probably have just assumed someone was trying to hack my email."

While federal law protects cardholders from unauthorized purchases, getting coverage hinges on reporting the issue quickly.

Related Articles

Under the federal Fair Credit Billing Act, you can avoid being held responsible for unauthorized charges, provided you notify your card issuer within 60 days from the date it sends out your credit card statement.

Although email bombing isn't a new scam strategy, its frequency has exploded in the past couple of years. Cybersecurity firm eSentire reported that email-bombing and impersonation attacks surged 1,450 percent in 2025 compared to the year before, with fraudsters using the inbox flood to distract their targets.

The eSentire report focuses on business attacks, in which fraudsters use email bombing as a smoke screen to breach a company's systems. They can then extort the organization into paying a hefty ransom to avoid the release of sensitive private data.

But criminals have adopted that corporate strategy and are now using it against consumers, according to Spence Hutchinson, senior manager with eSentire's intelligence research team.

Related Articles

"Good ideas move fast," Hutchinson said.

James E. Lee, president of the Identity Theft Resource Center, pointed out that many corporations have tech teams to manage digital attacks, but individual consumers are often blindsided by them.

"And it's a lot scarier," Lee said. "When they see this massive amount of email or pop-ups or text or whatever it may be, it overwhelms them, which is exactly what the bad guys want to have happen."

Artificial intelligence, Lee added, is helping make it easier to bombard consumers.

"With the kind of AI tools that are now available to your garden-variety identity criminal, they can automate these attacks," he said. "You can have an AI do this stuff at scale in the middle of the night. They can run tens of thousands of routines, and it only takes one person to write that code."

Here is how to protect yourself if this happens to you:

- **Treat a flood of messages as a warning sign.** If you get swamped with an unusually large amount of email, assume a financial account or credit card has just been breached and respond to any real-time alerts right away.
- **Check your accounts immediately.** Log into your banking and credit card apps to check for pending charges you haven't authorized.
- **Do a search before you purge.** Look for terms such as "password," "order confirmation," or the names of your financial institutions to preserve key alerts.
- **Then, do a deep dive into your email.** Look for authentic alerts hidden in the noise. After making sure that no financial notifications were buried in the pile, the reader said, "I did bulk deletions for most of the items."
- **An offer of help is part of the con.** If someone calls or sends a pop-up offering to clean up your inbox, ignore it. It is not Microsoft, Apple or Google calling. It's most certainly the scammer reaching out.
- **Resist the urge to respond to the messages.** Except for contacting your financial institution, don't do anything else. "Let it ride," Lee advised. He warned that cybercriminals often link email bombing with bogus help desk impersonation scams. They want to trick you into granting them remote access to your computer so they can steal data or charge you fraudulent fees, or both. "For goodness sake, don't click on anything," he said. If you're not sure what to do, you can get free help by contacting the Identity Theft Resource Center at 888-400-5530 or visit idtheftcenter.org.

Help spread the word to your family and friends. The reader who brought this to my attention did so because she suspected that many people had never heard of email bombing. Tell folks that if they see an explosion of sign-up confirmations, they shouldn't dismiss those emails as harmless, albeit annoying spam. It's a clever cover for a very diabolical crime.