Better Business Bureau® Senior Awareness Initiative

72-year-old Mayfield Heights woman scammed out of $291,000

A tech support scam targeted a Mayfield Heights woman, stealing nearly $300,000 in the process. The 72-year-old victim's case is so serious, even the Department of Justice has become involved. BBB Serving Greater Cleveland is warning Northeast Ohio consumers to watch out for the red flags of this tricky scam.

The victim clicked on the pop-up window which gave her a number to call where "they would provide the help that would secure her bank accounts that had been hacked and were at risk." Once the victim called, she was shuffled between multiple different people, all of whom referred to themselves as part of the Microsoft fraud team and fake security identification numbers.

The scammers convinced the victim to go to Citizens Bank four separate times and send varying amounts to her account, which they told the victim was a more secure account for her money. The teller questioned the victim on one of her visits but continued to transfer the money when the victim said they wanted to send it.

BBB Serving Greater Cleveland offers the following tips to protect yourself from tech support scammers:

- **Look out for warning screens.** Nearly half of tech support scams begin with an alert on the victim's computer screen. This pop-up will have a phone number to call for help. Instead, disconnect from the internet and wi-fi connection by shutting off the device and restarting it with an antiviral scan.
- **Legitimate tech support companies don't make unsolicited phone calls.** A popular way for thieves to get in touch with victims is through cold calls. The callers often claim to be from a tech company. Scammers do and they can spoof official-looking phone numbers, so don't trust Caller ID.
- **Be wary of sponsored links.** When searching online for tech support, look out for sponsored ads at the top of the results list. Many of these links lead to businesses that scam consumers.
- **Avoid clicking on links in unfamiliar emails.** Scammers also use email to reach victims. These messages point consumers to scam websites that launch pop-ups with fake warnings and phone numbers.
- **Do your research**. Research tech support companies online at **BBB.org** learn more about the company, read customer reviews, and more.

Always report fraudulent activity. You can report scams, regardless of whether or not they have lost money, to BBB.org/ScamTracker. These reports can help others avoid falling victim to fraud.

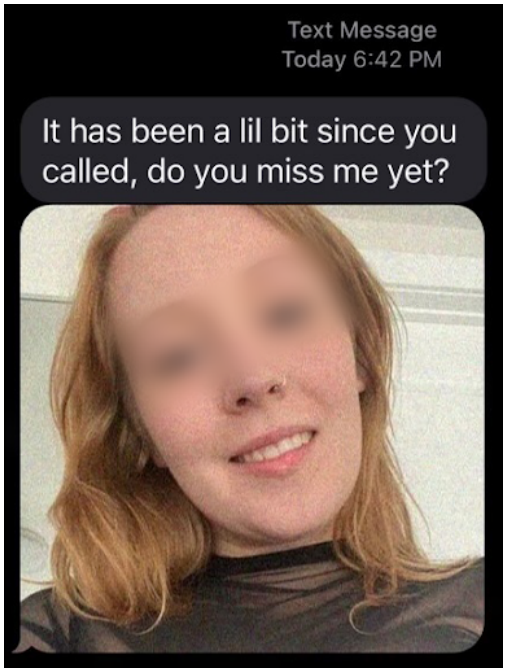
Better Business Bureau® Serving Greater Cleveland
200 Treeworth Blvd., Broadview Hts., OH 44147
info@cleveland.bbb.org I BBB.org I 216.241.7678

Better Business Bureau® Senior Awareness Initiative

A Wrong Number Can Lead to a Bad Romance Scam

Better Business Bureau Serving Greater Cleveland is advising area residents to be wary of unsolicited text messages appearing to come from wrong numbers. These communications often appear to use a photo of a young woman who is trying to text a friend. They may be a premise to a more sinister "romance scam" or a way for con artists to simply collect working cell phone numbers for future scam attempts.

"I did a double-take," says Pam Anson, Director of Brand Outreach for BBB Serving Greater Cleveland. "It's a different approach than most scammers take and I didn't think anything too seriously until more of my friends started to say that they also received it." A quick search on TinEye.com and Google Images reveals other users on the internet who reported receiving the screenshot. "It's obvious that the scammers are trying to elicit a response, such as sympathy, to this woman for receiving a fake number from a friend but we need to remind consumers that appearances can be deceiving."



Better Business Bureau Serving Greater Cleveland is providing these additional tips for local consumers who are looking to steer clear of text messaging scams.

•**Be skeptical.** Strangers on the internet can pretend to be anyone. Question motives behind both solicited and unsolicited messages.

•**Check for spelling and grammatical errors.** While not all scammers have poor grammar, many fraudsters are located off-shore do. Carefully check over communications and analyze them for any inconsistencies.

•**Guard personal information and photos.** Scammers may try to solicit personal information through methods such as cold calls, text messages, or emails. Be mindful of this, and always verify, when possible, the organization or individual you are speaking to through a third-party or video conferencing software. Also, remember that any photo you upload on social media can be stolen and used by a scammer.

You can report scams, regardless of whether or not they have lost money, to **BBB.org/ScamTracker.** These reports can help others avoid falling victim to fraud.

Better Business Bureau® Serving Greater Cleveland
200 Treeworth Blvd., Broadview Hts., OH 44147
info@cleveland.bbb.org I BBB.org I 216.241.7678

Better Business Bureau® Senior Awareness Initiative
Cryptocurrency Scams Increasing Bit by Bit (Coin)

More cryptocurrency scams are now aimed at consumers, and the trend is growing. The number of BBB Scam Tracker reports involving cryptocurrency doubled in 2021 and tripled from two years ago. BBB finds that there are generally two types of ways that cryptocurrency is used in scams. One type is investment schemes and the other is seeing cryptocurrency used as payment for more traditional scams. Victims most commonly find investment frauds on social media. Victims may be contacted through Messenger or Instagram by a "friend." Unbeknownst to the victim, their "friend's" account has been hacked or spoofed and it's actually a scammer that is advising them to invest or make payments to a fake company.

A senior citizen in Mansfield recently lost $5,500 to ransomware scammers posing as "Geek Squad" employees, using a Bitcoin ATM at a gas station. The consumer granted remote access to her computer after she was notified she needed to make a payment to Geek Squad. The scammer used the remote access to "accidentally" withdraw $5,000 from the consumer's bank account which he said he would refund and then advised the consumer that she needed to deposit $500.00 in a Bitcoin machine at a Marathon Gas Station in Ashland instead to make payment.

Scammers also ask for Bitcoin as a payment method for other types of scams. Most of these schemes are for online purchases, employment scams, tech support scams, and or even fake requests to pay utility bills. Scammers use the growing number of BitCoin ATMs to their advantage. With these ATMs, often found in places like gas stations, convenience stores, victims only need to insert $20 bills, scan the scammer's QR code, and then their money can be off to anywhere in the world.

Be incredibly careful when anyone asks them to pay with Bitcoin or another form of cryptocurrency. BBB is providing these tips for anyone considering using cryptocurrency:

- Cryptocurrency transactions cannot be reversed. It is like sending cash.
- Safely secure digital wallets containing cryptocurrency. Act like these are house keys.
- When in doubt, contact companies directly using the information provided on official websites and not websites sent by scammers.
- Make certain that the web address of any exchange or other site is the real one. Fake websites are widespread and may look very professional.
- Be skeptical of a romantic interest or a friend urging you to invest in cryptocurrency online. Talk to friends on the phone or in person to be sure someone has not hacked their social media account.
- Claims of a guaranteed return on any investments, especially cryptocurrency, are always false.

Better Business Bureau® Serving Greater Cleveland
200 Treeworth Blvd., Broadview Hts., OH 44147
info@cleveland.bbb.org I BBB.org I 216.241.7678