Police: He Said They Wanted to Reimburse Her. Instead, He Took $9,000

Author : David Gurliacci

Categories : Public Safety

Tagged as : Any Desk, AnyDesk, Computer Scams, Computer Scams 2017, Crime Prevention Advice 2017, Crime Prevention Tips 2017, Overpayment Scam, Overpayment Scam 2017, Overpayment/Reimbursement Scam, Phone Scam, Phone Scams 2017, Reimbursement Scam, Reimbursement Scam 2017, Telephone Scam, Telephone Scams 2017

Date : November 1, 2017

A Darien woman was scammed out of $9,000 through a more sophisticated scam than usual, involving a caller who convinced her to download a program to her computer.

Darien police described what happened this way:

On Tuesday afternoon, Oct. 24, the woman, a Long Neck Point Road resident, told police she believed she had been scammed.

She said that she had received a phone call from a male (when the call came, police didn't say). The male said he worked for a subsidiary of Microsoft and that his company owed her money as a reimbursement for computer software she had bought.

In order for her to get her money back, the caller said she should download a certain computer program called "Any Desk" (the program that allows someone else access to your computer, something that can be proper and useful in certain circumstances, such as getting technical support for problems on your laptop).

The scamming possibilities of Any Desk software were identified years ago. Here's an image of part of a Web page on the Any Desk website that discusses the problem and Any Desk's solution, involving a scam notice that was either disabled or just didn't work in the recent Darien case:

The caller instructed the victim on how to download the program, telling her that would allow him to guide her through the reimbursement process.

That, it turned out, was the equivalent to giving him access to her bank accounts.

As the male (police didn't say whether it was a man or possibly a teenage boy) was explaining to her how the money would be transferred, he was already taking money out of her accounts in a way that somehow made it look as if a deposit had been made. (Police didn't describe what that looked like or what was involved in doing that.)

The caller stated he would be over-depositing, and that she would need to refund him $9,000.

As the police announcement put it:

"The victim went to her bank and withdrew the $9000 she believed had been deposited by the caller. She then deposited the money into the account specified by the caller.

"After reviewing her account, the victim realized no deposit had ever been made to her account and she had deposited her own money into the caller's account."

The Darien police investigation is ongoing.

Overpayment/Reimbursement Schemes

The Darien police announcement gave this advice to the public about similar schemes:

- Many of the computer/phone scams that the department investigates involve some sort of overpayment/reimbursement transaction between the scammer and victim.
- The scammer "overpays" the victim (in a variety of methods) and requires the victim to reimburse them the overpayment. The money that the victim reimburses ends up being their own money.
- If someone is approached with this overpayment/reimbursement scenario, they should consider that this is not normal business practice and proceed with caution.