From time to time, SHAZAM is made aware of situations that may pose a risk to our clients. This information can come from various sources. *When we're made aware, we'll in turn make you aware*

THE SCAM

A scam has come to our attention. It's not a new technique, rather it's the phishing email fraudsters often use.

This particular scam involves a fraudster posing as a nationally known antivirus software company representative to socially engineer their victims. Traditionally done through a pop-up message on the victim's computer, the fraudster either gets the victim to think:

- They have a virus on their computer, or
- Their antivirus software needs to be upgraded

WHAT'S NEW

1. Fraudsters are now sending victims an email appearing to be from a nationally known antivirus software company and advising that the victim has recently upgraded their antivirus software. The email is a receipt for the upgrade, typically ranging from $200 to $1,000.
2. The fraudulent email gives a number to contact the company if the victim wants to discuss or dispute this upgrade charge. However, the number isn't to the real company; it's to the fraudster.
3. When the victim calls the fraudster to dispute the charge, the fraudster convinces the victim to let the fraudster have remote access to the victim's computer to verify that no viruses are on the victims computer.
4. Once the victim allows this to happen, the fraudster finds a bogus virus and subsequently convinces the victim to provide the victim's online banking credentials to the fraudster so they can do a "test run" to make sure the virus didn't infect the victim's bank account.
5. The "test run" will be the fraudster depositing a remote deposit capture check in the amount of around $5,000 into the victim's account.
6. The fraudster will verify with the victim that the victim's account shows a pending deposit of $5,000.
7. The victim is then instructed to proceed to their financial institution the same day and withdraw $4,000 or more from their account and mail it via UPS or FedEx to the fraudster for reimbursement of the "test run."
8. The fraudster advises the victim their antivirus software has been upgraded free of charge and the victim can keep the remaining balance for the misunderstanding of the antivirus software update email.

SPOT THE SCAM

The fraudster typically remains on the phone with the victim as they proceed to their financial institution to withdraw the money.

SHAZAM

800-537-5427 / shazam.net

[Privacy Policy]