THE LATEST PHONE SCAM Targets Your Bank Account

June 21, 2010

Justice News - Press releases and Speeches

WASHINGTON (RPRN) 06/21/10 — Imagine getting hundreds or thousands of calls on your home, business, or cell phone, tying up the lines. And when you answer, you hear anything from dead air to recorded messages, advertisements, or even phone sex menus.

It's annoying, no doubt. But it could be more than that—it could be a sign that you're being victimized by the latest scam making the rounds. This "telephone denial-of-service attack" could be the precursor to a crime targeting your bank accounts.

Denial-of-service attacks, by themselves, are nothing new—computer hackers use them to take down websites by flooding them with large amounts of traffic.

In a recent twist, criminals have transferred this activity to telephones, using automated dialing programs and multiple accounts to overwhelm the phone lines of unsuspecting citizens.

Why are they doing it? Turns out the calls are simply a diversionary tactic: while the lines are tied up, the criminals—masquerading as the victims themselves—are raiding the victims' bank accounts and online trading or other money management accounts.

Here, in a nutshell, is how the whole thing works:

*Weeks or months before the phone calls start, a criminal uses social engineering tactics or malware to elicit personal information from a victim that this person's bank or financial institution would have—like account numbers and passwords. Perhaps the victim responded to a bogus e-mail phishing for information, inadvertently gave out sensitive information during a phone call, or put too much personal information on social networking sites that are trolled by criminals.

*Using technology, the criminal ties up the victim's various phone lines.

*Then, the criminal either contacts the financial institution pretending to be the victim…or pilfers the victim's online bank accounts using fraudulent transactions. Normally, the institution calls to verify the transactions, but of course they can't get through to the victim over the phone.

*If the transactions

aren't made, the criminals sometimes re-contact the financial institution as the victim and ask for it to be done. Or they add their own phone number to victims' accounts and just wait for the bank to call.

By the time the victim or the financial institution realizes what happens, it's too late.

Law enforcement and industry response

While the lines are tied up, the criminals are raiding victims' accounts.

The FBI first learned about this emerging scheme through one of its private industry partners, which told us how a Florida dentist lost $400,000 from his retirement account after a denial-of-service attack on his phones.

And as of April of this year, there has definitely been a noticeable surge in telephone denial-of-service attacks, with numerous incidents having been reported in several Eastern states.

To help fight these schemes, the FBI has teamed up with the Communication Fraud Control Association—comprised of security professionals from communication providers—to analyze the patterns and trends of telephone denial-of-service attacks, educate the public, and identify the perpetrators and bring them to justice.

Ultimately, though, it's individual consumers and small- and medium-sized businesses on the front line of this battle. So take precautions: never give out personal information to an unsolicited phone caller or via e-mail; change online banking and automated telephone system passwords frequently; check your account balances often; and protect your computers with the latest virus protection and security software.

And if you think you may have been targeted by a telephone denial-of-service attack, contact your financial institution and your telephone provider, and file a complaint with the FBI's Internet Crime Complaint Center.

Main image credits: http://www.justice.gov/opa/pr/2009/Month/index.jsp

---

Filed Under: BREAKING NEWS, COURT NEWS, Crime, PRESS RELEASE, U.S.A. Government

RUSH PR NEWS newswire and press release services at rushprnews.com / Anne Howard annehowardpublicist.com

Content- Legal Responsibility - All material is copyrighted - You may repost but you MUST link back to the original post on your page and acknowledge Rush PR News as the news source. Rush PR News is not legally and/or morally responsible for content of press releases, opinions expressed or fact-checking.

Rush PR News cannot be held legally responsible for material published and distributed through its newswire service or published in its press-room and therefore cannot be sued for published material. Third-party must be contacted directly to dispute content.

Rush PR News is not the contact for material published.