Recommended Consumer Message Points on Denial of Service Attacks

What's happening?

- The websites at some banks are being intentionally flooded with an extremely high volume of electronic traffic from thousands of locations around the world. This flood of traffic, called "a distributed denial of service (or DDoS) attack" crowds out legitimate customers trying to use the bank's websites.
- Customers of those banks may experience a slower than usual connection or delayed connection when logging into Web site or making transactions online.
- The slowdowns do NOT involve a data breach or hacking
- The flood of electronic traffic is intended to slow down or disable the bank's Web site.
- The traffic is not designed – and has not resulted in – hacking which involves penetration of the banks' internal systems or exposure of sensitive personal information.

What You Should Know

- The attacks have not resulted in unauthorized access to customer information.
- Bank employees are working hard to ensure you have access to normal, safe and consistent online financial services. In addition, you can access your accounts through alternative means, including your bank's branch offices, mobile applications and call centers.
- Banks use sophisticated online security strategies to protect customer accounts.
- While you may experience difficulty in accessing accounts through the online channel, mobile, ATM, telephone, and branch banking will be available.
- Banks are working with telecommunications providers to increase capacity and invest in technology to defend attacks. There are limits to the capacity and services available from telecommunications providers. Banks continue to invest in technology to defend against potential attacks.
- Banks are collaborating with other banks, federal regulators, law enforcement officials, other government agencies, Internet Service Providers, and Internet security experts to fully analyze and deflect online attacks and deliver safe and consistent online service.
- Banks collaborate with the Financial Services Information Sharing and Analysis Center (FS-ISAC) which is an industry forum for collaboration on critical security threats facing the financial services sector.

What You Can Do

- Install on your computer—and keep updated—anti-virus software, firewall and anti-spyware software.
- Set your computer's operating system and browser to "automatic download" to ensure your operating system and browser include the latest security updates.
- Don't get hooked by phishing. Do not respond to unsolicited emails requesting personal information and do not download attachments on unsolicited emails.
- Use strong passwords and change them regularly. The best passwords are long and complex, using a minimum of 8 characters and incorporating a combination of. numbers, symbols and letters. Avoid birthdays, pet names and simple passwords like 12345. Change passwords at least three times a year.