



TELEPHONY DENIAL OF SERVICE (TDoS)

Telephony based DoS attacks occur when perpetrators deliver a flood of telephone calls to your administrative or emergency telephone lines disrupting normal operations. These calls may accompany attempts to extort money, promises of lottery winnings or other economic gain or may only contain recorded music, tones, noise or dead air.

Verizon is committed to assisting our customers in identifying and mitigating the effects of TDoS attacks and we've produced this advisory to help get you the expertise and assistance you need. This advisory recommends actions you can take to report TDoS activity affecting your communications.

What you can do:

Follow the recommended best practices developed by the U.S. Department of Homeland Security in consultation with the Association of Public-Safety Communications Officials International (APCO) and the National Emergency Number Association (NENA);

1. Before an event:

- a.** Discuss how to respond to a TDoS event with your service provider. These discussions might include both your telephone service providers as well as your equipment vendors.
- b.** Ensure that your staff and their supervisors have access to the phone number and direct contact information for the service provider's personnel or division equipped to respond to a public safety TDoS.
- c.** Discuss with your telephone system vendor engineer or technician possible configuration changes to isolate critical phone lines from other lines, taking into account hunt-groups, busy or no-answer rollover to other lines, etc.
- d.** Remind employees of their obligations to protect personally identifying information, and how to protect themselves from identity theft (for example, see <http://www.consumer.ftc.gov/features/feature-0014-identity-theft>).

2. During the event:

- a.** Save the voice recording of suspects who may call before, during or after the TDoS events.
- b.** Record all phone numbers and account information
 - i. Start and stop times of the events
 - ii. Number of calls per hour or per day
 - iii. Phone numbers and other ANI/ALI information of the incoming calls
 - iv. IP addresses if applicable
 - v. Any instructions or statements made by the perpetrators for how to pay, such as account number, call-back phone number etc.
- c.** Retain all call logs and IP Logs
- d.** Attempt to separate the affected phone number from other critical lines – work with your PBX provider/maintainer.

3. **After the event:**

a. File a complaint with the Internet Crime Complaint Center www.IC3.gov - co-sponsored by the Federal Bureau of Investigation (FBI) and the National White Collar Crime Center (NW3C).

Include the keywords TDoS and Public Safety in the description of the incident

b. File a report with your local police department or sheriff's office.

i. If the investigator is unsure of how to proceed there are resources available to assist. The FBI, FCC (Federal Communications Commission) and FTC (Federal Trade Commission) are all engaged in this process, and DHS-NCC- NCCIC (Department of Homeland Security - National Coordinating Center for Communications - National Cybersecurity and Communications Integration Center) can help coordinate information.

ii. Law enforcement officials may also contact service providers with a request or subpoena to obtain additional information, if necessary.

c. Consolidate call logs and IP logs; mark for long-term retention.

How Verizon can assist:

1. Compile all the information you have from Step 2 above and contact the **Verizon Global Fraud Control Center** (available 24x7x365) at **800-309-3338** (Option 3).
2. Explain the issue you are experiencing and be prepared to share your findings with the Global Fraud Center.
3. The Global Fraud Center will conduct the necessary troubleshooting for this issue and coordinate with internal Verizon resources to research and resolve the issue.
4. Information on resolution will be shared with your POC as it becomes available.