U.S. Department of Justice
Federal Bureau of Investigation

THREAT and INTIMIDATION RESPONSE GUIDE

IN-PERSON THREAT

A physical IN-PERSON THREAT is when you are in imminent danger because of the close proximity of the person making the threat. You have three options:

1. **Run:** Identify an escape route. Drop any belongings that may slow you down. If possible, help others escape. Call 911.
2. **Hide:** Hide away from view of the threat. Lock doors or block entries. Silence your cell phone (including vibrate mode) and remain silent until the threat is over.
3. **Fight:** Fighting should be a last resort and only when your life is in imminent danger. Attempt to incapacitate the threat. Act with as much physical aggression as possible.

A verbal IN-PERSON THREAT one that does not place the recipient in immediate danger or is intended to be carried out later.

- Write down or otherwise record the threat exactly as it was communicated.
- Record as many descriptive details as possible about the person who made the threat: name, appearance, skin color, sex, height, weight, hair and eye color, voice, clothing, or any other distinguishing features.
- Report the threat to law enforcement.

PHONED THREAT

A PHONED THREAT is a threat received by telephone. You should try to get as much information on the caller and the threat as possible, unless the threat is nearby or may imminently harm you or others.

- Remain calm and do not hang up.
- Keep the caller on as long as possible and try soliciting information to determine whether the threat is specific, realistic, or poses immediate danger to you or others.
- If possible, signal others nearby to listen and notify law enforcement.
- Copy any information from the phone's electronic display.
- Write the exact wording of the threat.
- Record the call if possible.
- Be available to discuss the details with law enforcement personnel.

ELECTRONIC MESSAGE THREAT

An ELECTRONIC MESSAGE THREAT is a threat received through direct messaging, email, or social media. It may include threats of blackmail or adverse consequences if the recipient does not comply.

- Do not open an electronic message or attachment from unknown senders.
- Do not communicate on social media with unknown or unsolicited individuals.
- Make sure your security settings are set to the highest level of protection.

If an electronic threat is received:

- Do not delete the message. Forensic examination may uncover important details.
- Leave the message open on the computer.
- Immediately notify law enforcement.
- Print, photograph, or copy the message, subject line, date, and time.
- Preserve all electronic evidence.

CYBER ATTACKS

A CYBER ATTACK can compromise your electronic device and expose personal information.

- Use strong passphrases and do not use the same passphrase for multiple websites.
- Set anti-virus and anti-malware applications to automatically update.
- Apply system and software updates as soon as they become available.
- Apply two-factor authentication.
- Backup data regularly.

If you suspect that you have been a victim of a cyber attack:

- Do not delete or alter your computer systems.
- Immediately contact your financial institutions to protect your accounts from identity theft.
- Change passphrases and monitor accounts for suspicious activity.

If you are in immediate physical danger, call 911.
If you experience a threat, please contact your local FBI field office (listings available at www.fbi.gov) or submit a tip via 1-800-CALLFBI (or 1-800-225-5324) or via www.fbi.gov/tips.

You can also make an anonymous tip to the FBI by phone or online.