U.S. Department of Justice
Federal Bureau of Investigation

THREAT INTIMIDATION 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 is 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 about the person who made the threat: name, race, gender, height, weight, hair and eye color, voice, clothing, or any other distinguishing features.
- Report the threat to law enforcement.

PHONED THREAT

A PHONED THREAT 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 via the internet 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.

U.S. Department of Justice
Federal Bureau of Investigation

THREAT INTIMIDATION GUIDE

Who should I contact if I experience threats or Intimidation: local police or the FBI?

- If you or others are in immediate physical danger, call the local police by dialing 911.
- If you experience a threat associated with a federal crime, contact your local FBI field office (listings at www.fbi.gov) by calling 1-800-CALLFBI (or 1-800-225-5324) or via www.fbi.gov/tips. Examples include threats from an agent of a foreign government, organized crime, or a government official. Your report can be anonymous.
- Not all incidents meet the FBI's investigative threshold. If you are the victim of an incident that does not meet the threshold of a federal crime, you may need to report it to your local police department. Local and state jurisdictions have different thresholds for investigating suspected crimes.

What can I expect if I am interviewed by the FBI?

- An FBI agent can meet with you at an FBI field office or at another location.
- The FBI will ask you to provide as much information as possible about the perpetrator and details of the threat you have experienced.
- The FBI will ask for your contact information to follow-up with you if needed.
- The FBI will attempt to protect your identity and confidentiality.
- If appropriate, an FBI Victim Specialist may be present during the interview to provide information and support, or they may contact you after your interview by phone or mail.

What is the threshold for the FBI to investigate a complete and/or initiate an investigation?

- The FBI is able to investigate threats that violate US federal law and imply harm or danger to the recipient.
- The ability of US law enforcement to prosecute individuals for threat-related charges is contingent upon several factors, such as: the quality of the evidence, the ability to identify the individuals who perpetrated the action, the identification of a conspiracy, and/or the ability to arrest the offending individuals.

What can I expect if the FBI initiates an investigation?

- If the FBI believes a federal crime may have been committed, one or more FBI special agents will conduct an investigation. As part of the investigation, the special agents will gather evidence, which may include an interview with you and other victims.
- You may also be asked to describe your experience before a federal grand jury.
- A thorough investigation will be completed. The investigation may take a long time to finish, and you will not be updated on day-to-day case developments. Every effort will be made to tell you about major events in an investigation, such as an arrest or indictment. The FBI is committed to providing such information to you before it is released to the public, when possible. However, the FBI must always be careful not to reveal sensitive information that could hurt the investigation or increase danger to law enforcement.
- An FBI Victim Specialist will be available to provide identified victims with support, information, and referrals for any local resources that may be needed.

Even if reporting the details of how you were threatened or cyber attacked does not result in an investigation, it will likely assist other victims by helping the FBI track threats and identify trends.

FBI FIELD OFFICE CONTACT INFORMATION LISTED BY CITY AND STATE IS AVAILABLE AT WWW.FBI.GOV. IF YOU ARE IN IMMINENT DANGER, CALL 911.