

# KNOW WHAT YOU'RE SEEING – A STRAIGHT-TALK GUIDE FOR THE **DIGITAL** **BATTLESPACE**



**Beale AFB, 9 RW Public Affairs**

**2026**



## A note from the commander

Teammates, the information environment is a **battlespace**. With the rise of Artificial Intelligence, the nature of the threats we face has changed. We are confronting next-level threats powered by AI, designed specifically to deceive our Airmen and disrupt our mission.

This guide is a foundational tool created to give you the knowledge to navigate this digital environment safely and effectively. Inside, you will find concrete steps you can take to protect yourself, your family, and our critical mission.

Use this guide to mitigate operational and personal security risks. Be responsible digital citizens, be vigilant defenders, and be the ambassadors for the U.S. Air Force that I know you are.

The mission depends on it.

Col Typolt, Deputy Commander, 9th Reconnaissance Wing



## The 3 Types of Information Threats

Threat	What It Is	Intent	Real World Example
<b>MIS</b> information	An honest mistake. It's just wrong information.	<b>Accidental.</b> Someone shares it thinking they're being helpful.	Your friend texts you "Gate X is closed," but the date is wrong. He wasn't trying to mislead you, he was just mistaken.
<b>DIS</b> information	A deliberate lie. It's weaponized information.	<b>Malicious.</b> The enemy creates it to deceive you and disrupt our mission.	An adversary creates a fake news site claiming a major cyberattack on Beale to cause panic and erode trust in leadership.
<b>MAL</b> information	The truth, used as a weapon.	<b>Malicious.</b> Someone uses real, often private, info to hurt you or the mission. (Think OPSEC violations).	Someone with a grudge posts your real deployment dates and home station details online, putting you and your family at risk.

## How AI is the New Threat Accelerator

AI is being used to make these attacks faster, cheaper, and more believable. Here's how:

- **Fake News on Autopilot:** AI writes fake articles and posts that look and sound real.
- **Digital "Ghosts":** AI generates realistic profile pictures for fake accounts used in espionage or to spread lies.
- **Targeting Your Feed:** AI analyzes what you like and share to feed you personalized disinformation designed to trigger a reaction.
- **Armies of Bots:** AI powers thousands of automated accounts to amplify a false narrative and make it seem like everyone believes it.



**Bottom Line:** Think before you share. Verify what you see. Protect your wingmen.

<b>Actionable Steps: Media Literacy</b>	<b>How to do it</b>
<b>PAUSE</b> Before You Share.	That shocking video or post is designed to trigger an emotional reaction. <b>Stop.</b> Take a breath. The most effective weapon against disinformation is a 3-second pause.
Check the <b>Source.</b>	Is this from an official source like the Beale AFB official website or a .gov domain? Or is it from a random "military news" page you've never heard of? If you can't verify the source, don't share the info.
Look for <b>Glitches.</b>	With deepfake videos, look for unnatural eye movements, weird blurring, or mismatched audio sync. With AI text, look for repetitive phrases or a strange, non-human tone.
<b>Question Everything.</b>	If a message (even if it seems to be from a leader) announces something totally unexpected or out of character via an unofficial channel, be skeptical. Verify it through the official chain of command.



## Protecting Your Family: Hardening the Home Front

Your family is your "first line of defense" but they are also a primary target for adversaries seeking information. They may not have had the same OPSEC or threat briefings you have. It's your job to get them up to speed.

**Your Mission: Equip your family with the knowledge to protect themselves.**



<b>Actionable Steps: Family Protection</b>	<b>How to do it</b>
Hold a "Digital OPSEC" Family Meeting	Talk to your spouse, parents, and even older kids. Explain <i>why</i> they shouldn't post specific details about your job, your schedule, or when you're deployed. Use the examples: Malinformation is real info used to cause harm.
Review Their Social Media Privacy Settings.	Sit down with them and make sure their profiles are private, not public. Show them how to check who their "friends" are and to be wary of random friend requests..
Teach Them About Phishing & Scams.	Explain that adversaries will target them with fake emails or messages (phishing) to get information. A classic tactic is a message like, "I'm a friend of your spouse in the Air Force, and I need this info..." or a fake "emergency." Teach them to never give out personal info and to call you directly if something seems off.
Create a "Code Word."	Establish a simple family code word. If they get a strange message or call asking for sensitive information, they can ask for the code word. No code word, no information. It's a simple but effective security check

**DID YOU KNOW ABOUT THE HATCH ACT?** : Rules governing political activities by government civilians are found in a federal law known as the Hatch Act. [Hatch Act Guidance on Social Media](#)

## POLICY

### YOUR ORGANIZATION'S POLICIES

The 9 RW Public Affairs office is the primary office of responsibility for guidance and wing policy changes regarding social media and its use by Airmen within our organization.

We want our Airmen to understand the power of social media and its leverage in connecting others to the importance of our missions and its risks as a choice communication tool. There can be no misconception between where your responsibilities as an Airman end and where your personal life begins.



**There is no discerning between your personal and military life. YOU ARE AN AIRMAN 24 hours a day. Service members and employees must understand that they may be held accountable for their online activity if they violate any standards outlined within the policy. It is not otherwise dependent on the method of communication used. The following Air Force standards must always be observed on and off duty regardless of the process of transmission.**

#### FREEDOM OF EXPRESSION:

**DO NOT:** Post offensive and/or inappropriate online behavior that could discredit the military or you as a member. Use contemptuous words against elected officials, including the President, the Vice President, Congress, the Secretary of War, the Secretary of a military department, the Secretary of Homeland Security, or the Governor or legislature of any State/Commonwealth, in an official capacity

**DO:** Use disclaimers that clearly define that the views you express are yours alone and do not reflect the views of the Air Force or our organization. (If it can be derived that you are a military member and a part of our organization, then you should use this practice). EXAMPLE: "The postings on this site are my own and don't necessarily represent Air Force positions, strategies, or opinions." Here's the bottom line: USE COMMON SENSE! If you don't want to read about it, see it in the news, or be asked about it by people you respect — don't say it, don't do it, don't post it. Don't go viral for the wrong reasons.

#### HARMFUL OR OFFENSIVE CONDUCT:

**DO NOT:** Post content in violation of federal or state laws, Air Force regulations and policies through inappropriate personal online activity, or any other form of communication. This includes posting **defamatory, libelous, obscene, threatening, racially or ethnically hateful or otherwise offensive/illegal information or material and any other form of communication, including online bullying, hazing, harassment, stalking, discrimination, retaliation, or any other type of behavior that undermines dignity and respect.**

**DO:** Report experiences of witnessing incidents of improper behavior. Reports can be made to your chain of command. Additional avenues you can report incidents or content that contains obscene, threatening, hateful, harassing, stalking, or discrimination include Equal Employment Opportunity offices, the Inspector General, Sexual Assault Prevention and Response offices, and the Office of Air Force Special Investigations.

<p><b>OPSEC</b></p> <p><b>DO NOT:</b> Post Classified, FOUO, CUI, or other official DoW information and documents on social media or any other non-DoW e-mail accounts. Don't post details about your unit's mission or security procedures or announce locations and times of deployments.</p> <p><b>DO:</b> Closely review content before posting to ensure sensitive or personal information is not accidentally released (e.g. troop locations, equipment, tactical unit details, and numbers of personnel. Familiarize yourself with OPSEC training and avoid posting content containing OPSEC hazards in them.</p> <p><b>PERSONAL SOCIAL MEDIA ACCOUNTS:</b></p> <p><b>DO NOT:</b> Use your Air Force affiliation, official title, or position to promote, endorse or benefit any profit-making group or agency, or non-profit groups based solely on religious or political affiliations, IAW DODD 5500.07, and AFI 1-1, Air Force Standards. This includes appearing in, or preparing statements for inclusion in, advertisements designed for use by electronic or print media. Don't promote yourself for personal or financial gain.</p> <p><b>DO:</b> Differentiate between opinion and official information. Stay in your lane when talking about the Air Force or the DoW. Discussion of issues related to your career field or personal experiences are acceptable and encouraged, but you shouldn't discuss areas of expertise where you have no firsthand, direct experience or knowledge.</p>	<p><b>PERSONAL GAIN SINCERELY HELD BELIEFS:</b></p> <p><b>DO NOT:</b> Use the Air Force name or your title to endorse or promote products, political positions or religious ideologies.</p> <p><b>DO:</b> Clarify all individual expressions of sincerely held beliefs (conscience, moral principles, or religious beliefs) as your own.</p> <p><b>POLITICAL ACTIVITY:</b></p> <p><b>DO NOT:</b> Solicit votes for or against a party, candidate or cause in an official capacity. Do not participate in any interview or discussion as an advocate for or against a party, candidate, or cause. This includes attending a rally in uniform. Members may, however, express their personal opinions on political candidates and issues, make monetary contributions to a political campaign or organization and attend political events, in their personal capacity as a spectator when not in uniform. Commissioned officers may not make contemptuous words against the President, Vice President, Secretary of Defense, Deputy Secretary of Defense, Secretary of DAF or governor and legislature of any state in which he or she is located, or performing duty in. Don't express or imply Air Force endorsement of any opinions, products or causes.</p> <p><b>DO:</b> Express your political views on public issues/political candidates online outside of organized communication campaigns. Clearly present your views as your own and review participation guides found in AFI 51- 508, Political Activities, Free Speech and Freedom of Assembly of Air Force Personnel.</p>
<p><b>POLITICS &amp; SOCIAL MEDIA CONTINUED:</b> You may generally express your personal views on public issues or political candidates via personal accounts on social media platforms, such as Facebook, Twitter, or personal blogs. However, suppose personnel can be identified by a social media site as a DoW employee when expressing a personal opinion? In that case, the posting must clearly and prominently state that the views expressed are those of the individual only and not of the Department of War. While Airmen and DoW civilians may "follow," "friend," or "like" a political party or candidate running for partisan office, they should avoid posting links to "share" or "re-tweet" comments or tweets from the Facebook page or Twitter account of a political party or candidate running for partisan office. Such activity could be deemed as participation in political activities. For more social media guidance for military members on social media and political activities, please review the Hatch Act</p>	

