CIVIL AIR PATROL

THE DISPATCH

Safety | Health Services | Chaplain Corps

April 2024

The Dispatch is for informational purposes. Unit Safety Officers are encouraged to use the articles in The Dispatch as topics for their monthly safety briefings and discussions. Members may go [eServices - Learning Management System](), click on “Go to AXIS,” search for this month’s The Dispatch, take the quiz, and receive safety education credit.

In This Publication

The Theme for This Month’s Dispatch is Cybersecurity. These articles from Health Services, Safety and Chaplain Corps, provide beneficial information on protecting yourself, fellow members, friends, and family from digital attacks.

Primary Articles on Cybersecurity

Cyber Safety

By: Maj. Catherine Scantlan, RN, FL-249

Cybersecurity refers to protecting computer systems, networks and sensitive information from unauthorized access, damage, theft, and cyber threats. As technology advances, we all are exposed to more online threats, such as cybercrime, and scamming. Older adults are often preyed on by scammers, teens may experience cyberbullying, online predators, and identity theft. According to research, cyberbullying poses the most common online risk for teens, causing anxiety, depression, isolation and even suicide.

Tips for teens to stay safe online:

- Don't share personal information, (e.g., your name, address, phone number or school).
- Think twice before posting or saying anything online and don’t spread rumors.
- Respect what others are saying on social media.
- Only download from trusted sources.

- Passwords should include a mix of upper and lowercase letters, numbers, and symbols.

Tips for parents to teach their children about cybersecurity:

- Use child-friendly educational resources.
- Set up basic internet and ground rules.
- Focus on empowerment rather than fear.
- Create a trusting and respectful environment.
- Discuss upsetting and inappropriate content.
- Identify social networking sites and apps that are safe or unsafe to use.
- Monitor social media usage, turn off geo-locators on apps like Instagram, Snapchat, and Facebook, turn on "restricted mode" on apps like Tik Tok, make sure accounts are private.
- Set up parental controls and communicate the message that having a phone is a privilege.
- Know who your children are communicating with and educate them on fake profiles.
- Keep devices in communal areas and not in private bedrooms.

There are educational materials at many levels. Below is a list ranging from simple to "not so simple." The main idea is awareness, knowing where to look for resources, having them readily available, and knowing who to trust with your personal information at all times.

- Homeland Security offers this excellent course: Stop Think Connect - Kids - pdf
- The Federal Trade Commission Consumer Advice - Online Privacy and Security, this link has information that covers in detail: Are Public WIFI's safe? Creating strong passwords, protecting your phone from hackers, recognizing, and removing malware, recovering hacked social media accounts, or emails, and many more subjects. It is a page to bookmark, read and have available!

Civil Air Patrol Resources:

- Cyber Information - Cybersecurity
- Specific for Cadets - Cadet Cyber

- This link looks to expand the future of Cybersecurity through introducing cadets to major opportunities, for example, Air Force Association Cyber Camps, CyberPatriot, National Cyber Academy, a summer NCSA - CAP's Introduction to Cybersecurity - pdf.

- This series is now available: Seventh Module - Aerospace Dimensions – pdf.

Learning about Cybersecurity not only protects you and your family, but as the youth begin to determine their future careers, this can be a career choice.

Cybersecurity and Safety - The Same or Different?

By: Maj. William "Bill" Trussell, CFI, IA, MEI, SQ/CC,
FAA Safety Team Representative, Asst. Stan/ Eval Officer, DE-019

In today's world we are just beginning to understand the impact that cybersecurity can have on our daily lives. Cybersecurity issues are moving well beyond hackers trying to take over your social media accounts for fun. Financial motivations were once the main force behind attacks. While money remains a force, especially large-scale ransomware attacks with big price tags, malicious actors have engaged in attacks that are probing systems that impact our everyday lives. Shutting down power and water utilities and causing widespread airline operations disruptions are all good examples of these types of attacks.

What does this have to do with safety?

While it may not be obvious right now, there are technical advances that open aviation up to safety concerns, keeping aircraft separated is a key objective in our aviation infrastructure. While it has been possible for a long time for a malicious actor to "hack" into the system and masquerade as an air traffic controller, the impact of the simplest of these "hacks" has been relatively easy to detect. The issue is this hazard depended on the aircrew as the lone mitigation measure for the risk. Right now, across the US and elsewhere air traffic clearances are being delivered by digital data messages, not solely by voice. We have all received email and text messages from sources that are not who they claimed to be. Imagine if a malicious actor was able to impersonate an air traffic controller and send, by data message, an instruction to change altitude to an aircraft, without the receiving aircraft detecting that the message was bogus. Impossible? Not exactly. Unlikely? Not exactly. So, is cybersecurity merely an issue of economic loss or does this broad issue have safety implications? It depends on your perception of "probability."

How likely are we to see this scenario happen? The probability is low, but not zero. Perhaps the best way to deal with the safety implications is to consider that it can and will happen, the only question is when.

Cybersecurity and You

By: Ch Maj. Michael Morison, USAF Master Resilience Trainer, PCR-001

This above all, to thine own self be true. (Shakespeare).

Cybersecurity is the protection of cyberspace from malicious attacks by spammers, hackers, and cybercriminals. Cyberspace includes the hardware, software, and data, be aware of what you can do to protect yourself. Research shows that many people present themselves one way in everyday life and have a different personality in cyberspace, to overcome this temptation, be true to the values that define you, be educated in how to be safe, listen to your intuition as it guides you, and know that you are not alone.

CAP's core value of integrity is the North Star guiding the presentation of who we are. Integrity allows me to do the right thing even when I am able to camouflage it. I will be true to who I am anywhere that I am present – including cyberspace, be the authentic you.

Not everyone has integrity, you may share information with honesty in cyberspace, others may unknowingly be groomed for any number of reasons by an anonymous person who conceals their purpose using cyberspace as camouflage, cadet and senior member should be mindful.

Cyberspace interactions do not necessarily provide a trusted and safe place to be. In times of acute stress or trauma, many turn to support by entering blogs and chatrooms, where numerous participants are unknown to the user. Studies have shown that responses may or may not be helpful, comments may help one to better cope, or can intensify the negative spiral of feelings, you should exercise caution and verify if the source is trustworthy.

In cyberspace, paralleling ordinary life, be aware of the reliability of the source of information. Research has also indicated that social media sources of information regarding significant news events are generally not edited. Traditional news media sources are often reporting for audience impact, try to limit your exposure to the reported news. Look for the facts being reported and separate this from the emotional drawstrings the story may have. To deal with traumatic incidents, it is recommended that you watch the news for a few minutes, two to three times a day. You will be able to be more present in the moment to separate fact from conjecture. In the initial stages of a critical incident, be knowledgeable of experts who are speculating, concrete information may not yet be available.

Protecting the Gift: Keeping Children and Teenagers Safe (and Parents Sane) - A book authored by Gavin De Becker and highly acclaimed by law enforcement officials. He borrows from Dr. Christiane Northrup who stated that intuition is "The direct perception of truth or fact independent of any reasoning process." Our brain takes in so much environmental and social information that it cannot cognitively process it in split seconds. Often social conditioning can cause us to override the discomfort we feel. A stranger who is insistent on willing to help, and will not take **No** for an answer, we may feel uneasy, but society enculturates us to trust polite people or people of authority, so we may give in to the pressure. The feeling of discomfort is the result of our intuition warning us. Dr. Northrup continues that "It's a part of our body that lets us know whether we are safe and whether we are being lied to."

Mr. De Becker offers a **Test of Twelve** that ideally every youth should know when in public regularly and cyberspace. Here are a few:

1. Know how to honor your feelings – be aware if someone makes you uncomfortable.
2. Defy inappropriate or unsafe online activity and know you will be supported.
3. Be assertive in maintaining your core values and withdraw from the situation.
4. Distinguish how to choose ***who*** **to ask** (Parents, chaplains, trusted individuals). You can speak to that person, trust makes it easier to tell your story, no matter how unpleasant.
5. Report information immediately that may identify a risk or threat and be specific.
6. If someone says, **"Don't tell,"** the thing to *do is* **to tell**, this is a Red Flag.
7. Always refrain from going anywhere out of public view with someone you don't know.

CAP family, we have an obligation to be wingmen to everyone. It is incumbent on us to develop a culture of trust that promotes a feeling of safety for cadets especially, and seniors. Chaplains, Health Service Officers, Safety Officers, and other trusted individuals, enjoy providing support. If someone comes to you and you are unsure of what to do, refer them to a person that you trust who can help. With situational awareness, knowledge, intuition, a culture of caring, and trust we can ensure a safer cyberspace experience for our members.

Secondary Articles/Information of Special Interest

Health Information Overload: Identifying Credible Health Information Online

By: Maj. Heather Parth, MPH, CIC, FAPIC, National Health Services Deputy, FL-001

Searching for health information has never been easier – nor more daunting. Everywhere we turn there's another headline-grabbing news story about a new drug trial, or sensational claim for a quick cure-all ("What your [fill-in-the-blank-expert] doesn't want you to know!" Click here!). But how do we sift through the clickbait to find credible health information for decision making?

Keep a questioning attitude: **Think the 5W's and H.**

- **Who** is listed under the "About Us" section?
  Is there an editorial board of health experts with clear qualifications?
- **When** was content updated or is it current?
- **Where** is this site? Does it have a .gov (official government) or .edu (educational institution) ending? Organizations (.org) may be credible but additional research may be required into the type of organization.
- **Why** does this site exist – What is the *motive*? Is it to offer balanced education?
- **How** is content vetted?
  Is there a review process with criteria to facilitate scientifically grounded material?

What is the actual content? There are important clues that indicate good quality information:

- Statistics indicate the groups they apply to, for example: age. These details will indicate if the numbers can be generalized. Statistics should also answer the "out of how many?" question – "100 people affected" sounds like a lot, but the picture changes if it is out of 101 versus a million people.
- *Correlation* (relationship) is different from *causation* (A → B): Grilling out and CAP Encampments both trend in the summer but grilling burgers won't cause a pop-up encampment to occur! Summer is the confounder – Encampments and grilling are common during the season, but one event doesn't cause the other event to happen.

Red flags:

- Lack of transparency: anonymous organization, no contact information, no citations.
- Advertisements disguised as health information.
- Selling a product or ideology.
- Alarmist writing style.
- Drastically different information on the same topic when compared to other sites meeting credibility criteria: All scientific breakthroughs were initially revolutionary but consider this in context with other red flags.

There is a wealth of variable quality health information, the goal of any credible source should be to promote *your* health literacy so you can make informed decisions with your healthcare provider.

Resources:

Evaluating Health Information: MedlinePlus

Evaluating Health Information | Patient Education | UCSF Health

Evaluating Online Information - Consumer Health - Research Guides at Syracuse University

Finding Reliable Health Information Online | NIH News in Health

How To Find Reliable Health Information Online | National Institute on Aging (nih.gov)

Beware of Phishing Emails

By: Joseph Hall, Jr., CISM, CAP Deputy Chief Information Officer,
Information Security Manager

Civil Air Patrol has observed a significant increase in phishing email attempts. These malicious actors are creating clever emails that manage to bypass spam and phishing filters by appearing to be related to legitimate subjects. These emails deceive individuals into visiting malicious websites or downloading malware, which can lead to data theft and computer damage.

General guidance on how to safeguard yourself and CAP against these destructive email threats:

DO NOT

- Open any suspicious email based on the Subject or Sender—delete it or use the Phish Alert Button (PAB) or follow the preferred method to report phishing emails without opening them.
- Reply to, open attachments from, or click on URLs from unknown and untrusted sources.
- Ever send personal/sensitive information via email—e.g., passwords, social security.

DO

- Check for misspellings, grammatical errors, and abnormal spacing.
- Check links by using your mouse to hover over the hyperlink to determine if the URL makes sense with the sender—e.g., matching the sender's name to the URL; and whether there's a foreign name or location in the URL.
- Report any suspicious emails received and delete them immediately to prevent yourself from accidentally opening the message in the future.
- Use common sense—if it doesn't look right, trust your judgment.

RED FLAGS

- Does the email ask for any of your or anyone else's sensitive/personal information?
- Does the hover-text link match what's in the text?
- Does the address in the 'To' field match the sender of the email?
- The email asks you to immediately act or open an attachment to avoid account closure.

Maintaining your vigilance about phishing threats is crucial in promoting CAP's Security posture!

Small Unmanned Aerial Systems (sUAS):
Safety and Risk Management for Drone Pilots

By: Maj. Jeffrey Rayden, CA-379

Small Unmanned Aerial Systems (sUAS), known as drones, are transforming various industries. In the area of Civil Air Patrol emergency services, sUAS can be valuable in search and rescue (SAR) operations locating missing persons, assisting, and assessing disaster-affected areas. Ensuring the safe and responsible operation of sUAS, drone pilots must understand and review potential risks and adopt risk management strategies. Battery safety is also a crucial element due to the need for reliable power sources and volatility of these power packs.

Education, training, adherence to regulations, and effective risk mitigation strategies are essential. By following these guidelines presented in this article, sUAS pilots can conduct essential missions safely and responsibly, contributing to the well-being of those in need.

Please read the entire article here: sUAS Safety and Risk Management for Drone Pilots - pdf

** Messages From Safety, Health Services and Chaplain Corps**

To our Flying Squadrons:

To improve our knowledge and to connect with our pilots we provide this YouTube video from the Federal Air Surgeon. Pilot Minute: What are Some Aviation Specific Reasons to Stay Fit?

Request for The Dispatch Articles

We would like to solicit your valuable input for The Dispatch articles.

For consideration, please kindly submit your article the following editors:

Safety - Health Services - Chaplain Corps

Upcoming Editions:

May - Theme: Encampment, please submit your article by **April 19th**.

June - Theme: 101 Critical Days of Summer, please submit your article by **May 15th**.

*Current and Previous Issues: **Safety Beacon / The Dispatch***
*CAP Safety Communications: **Website - Facebook - Email***