(Credit: U.S. Army/Spc. Hubert D. Delany III)

By Megan Jantos

Two years ago during an Army-led focus group, an older private first class made an astute observation that I'll never forget. "The Army does a great job telling me what I can't do, but I'm often left wondering what I *can* do." I suspect that this same sentiment prevents some leaders from engaging in digital leadership. For many Soldiers, it seems easier to reduce risk to your personal reputation and professional operations by avoiding social media altogether.

On the contrary, the Army actually encourages Soldiers and their families to use social media to stay connected and tell the Army's story. Engaged Soldiers are needed online more than ever before. Can you imagine a digital Army that reflects our organizational might in the physical world?

Entering the digital sphere is a double-edged sword, though. Numerous benefits of online participation also come with an equal number of pitfalls. However, given the right resources and training, anyone can become a digital pro. Here are several steps you *can* take to become an online warrior.

You Can Join the Digital Discussion But Do So Smartly.

Whether online or offline, folks should communicate with a purpose. Managing your digital presence effectively requires some research and reflection. Start by asking your nearest public affairs office for your unit's standard public affairs guidance.

The topics outlined in this document will give you an idea of your organization's communication expectations. If you notice a gap between what your organization says it does and what you think it does then you should communicate those concerns to your chain of command before taking them to social media.

Public affairs guidance will also help you identify areas where your experiences support your commander's communication objectives. These are topics you should feel free to talk about online. Staying in your sphere of experience will ensure you stay out of hot water.

To clarify, I'm not suggesting that you copy and paste government talking points to your personal social media accounts. Now is when you should reflect on the information you gathered during your digital audit. Ask yourself if your digital presence actually reflects who you are and what you stand for, and how you want others to perceive you. Thinking before you press send reduces risk to your reputation.

Finally, before publishing content to any platforms, conduct a SAPP review. SAPP stands for security, accuracy, propriety, and policy. Ask yourself the following questions:

- Does this post contain classified information?
- Is this information accurate?
- Is this post appropriate?
- Does this information violate Army or DOD policy?

You Can Gain Awareness.

The first step in gaining awareness is to "look in the digital mirror." You do this by conducting a digital audit, or study of your online presence. This can be as simple as googling your name. However, I recommend the following tips to get a better look at yourself.

First, you should use your browser's incognito mode to receive the best outside-looking-in view of yourself as well as fewer bias results. A query from your normal browser will skew your Google results based on your previous search data.

If you have a common name, the results may feature information about other people. It is still important to know what type of information pops up. Others searching for you will likely see the same information and may unwittingly associate it with you. On the contrary, if you have a unique name, or are already a publicly recognizable figure, it might behoove you to secure your username on popular platforms to prevent impersonation.

Once you conduct the search, inventory the results that appear. Almost every online experience starts with a search engine. Of those searches, 95% of users click the first result and 75% never scroll past the first page. Look for themes in the results and annotate these as well. Ask yourself if this is the information you want others to know about you.

Finally, make a list of the social media sites you maintain regularly whether they showed up in the search results or not. Review each platform for themes. You may notice that your themes vary from platform to platform. This is ok and even necessary based on the platforms as long as the portrayal remains true.

You Can Protect Your Identity.

Corporations that offer online services, mobile apps, and consumer devices say they care about protecting your identity, and I'm sure they do because they like your business. However, I prefer to apply the same advice that I was given as a young officer about career management–no one cares about you the way you care about yourself. So, get out there and check your security settings.

You may have set strict security parameters when you signed up for an online service, mobile app, or consumer device, but platforms change often. These changes can negatively impact your settings. Use the Department of Defense's Identity Awareness, Protection, and Management Guide to double-check the privacy settings on the most popular platforms. This

document also provides a wealth of knowledge that empowers you and your family to stay safe online.

By now I'm sure most of you have watched enough information assurance training modules to know that you should use strong passwords and *never* write them down. This is easier said than done in an age when the average person downloads 60-90 apps to their phone. Many experts recommend using a password manager to utilize strong, unique passwords that protect your digital presence. However, we suggest reading about the pros and cons before deciding how to leverage this tool.

Just because engaging online is a double-edged sword doesn't mean we shouldn't prepare to fight using it–probably all the more reason. At the very least, you should understand how to wield this new-aged weapon on the most basic level. Isn't security always the number one priority of work? That means doing what you can to secure your digital presence as much as your physical one.
For more information about OPSEC and protecting yourself in the information environment, visit the 1st Information Operations Command booth in the room immediately preceding the *Risky Business: Leadership in the Information Age panel*on Monday, October 14, 2019, from 1:30pm to 3:00pm at the 2019 AUSA National Meeting and Exposition.

Megan Jantos is a communication advisor to military leaders and working women. She believes effective communication–a firm handshake or well-aimed bullet–can solve any problem. You can find her on Twitter @MeganJantos, crushing weights at the gym, or helping the nearest person unleash their potential.

This article represents her own opinions, which are not necessarily those of the Army, the Department of Defense, or the federal government.

Share this:

- Email
- Tweet
- Pin it
- Print
- WhatsApp