

# IN FOCUS: FREQUENTLY ASKED QUESTIONS ABOUT

---

OPERATIONAL SECURITY FORCE PROTECTION INFORMATION ASSURANCE



[What is personal information assurance?](#)

[Why is it important?](#)

[What's the real threat here?](#)

[I couldn't possibly be a target, right?](#)

[What do I need to know about Facebook and other social networking sites?](#)

[What should I know about using Twitter?](#)

[What kind of passwords should I use?](#)

[What are security questions and which ones should I use?](#)

[Where can I get free anti-virus software through the military?](#)

[What are some simple mistakes that are easy to avoid?](#)

[Wouldn't the best practice be to just not use the internet?](#)

[Where can I find other resources about information assurance?](#)

## **What is Personal Information Assurance?**

Information assurance (IA) is the practice of managing risks related to the use of computers and the information stored on them. Personal IA is about protecting *your* information on a personal level, at home and at work, and what the best practices are for fully utilizing the tools available on the web while remaining secure and lowering your risk.

### **Why is it important?**

Although it is easy to have a “That could never happen to me” attitude, we still need to be prepared to protect ourselves and lower our level of risk while using computers and the internet. Today’s reliance on computers and technology means that learning good IA practices is as important as learning to look both ways before crossing a street.

### **What is the real threat here?**

Intelligence and information are more important than manpower to today’s battlefield, and the internet makes it easier than ever to gather information.

For example, on a typical Facebook page, after becoming someone’s “friend,” you can quickly see that person’s full name; birth date; the country, city and state in which he lives; who his friends are; and view multiple photos of them. All of this -- information that would have taken much longer for someone to gather 20 years ago -- is now easily and quickly available if you aren’t careful.

Any computer connected to the internet can be “hacked,” giving people access to your stored information. Many people keep digital copies of their personnel files, receipts and other items on their computer. Information such as banking account numbers and Social Security numbers can lead to identity theft.

### **I couldn’t possibly be a target, right?**

Criminals, terrorists and hackers look for two types of targets: predetermined targets and targets of opportunity or “easy targets.”

Regardless of which category you fall into, you should maintain the same level of security. By taking steps to protect your information, you decrease the amount of information available if you *are* being targeted and you cease to become an easy target.

### **What do I need to know about Facebook and other social networking sites?**

Protect your personal information from people you don’t know. You can set your information to private and allow it only for people that are your ‘friends’. Of course, in order for this to protect you, you should be careful who you add as friends. Only add people you know personally, not people who have been recommended to you that you have never met.

## **What should I know about using Twitter?**

Twitter is a useful tool for “micro-blogging” -- sending short messages about a topic that contain links to another website or location. Most links are shortened to fit Twitter’s 140-character-per-tweet limit.

Be cautious following links from unknown sources, as they can sometimes lead to places on the internet that upload viruses or spyware onto your machine.

## **What kind of passwords should I use?**

- The Army policy for passwords requires that any password must have at least two uppercase letters, two lowercase letters, two numbers, and two special characters or symbols. This is a good practice to follow for any password you use.
- Avoid any password that is easy to break. Avoid using Social Security numbers or your “last 4,” birthdays, phone numbers, addresses or other personal information.
- Avoid simple number combinations such as 12345 or 4321.
- Use different passwords for different accounts. Army Knowledge Online, online banking, personal e-mail, and social networking passwords should all be different. That way, if one is compromised the rest of your information should be safe.

## **What are security questions and which ones should I use?**

Security questions are the questions you are asked when filling out an online “I forgot my password” form. Setting up these security questions is part of the registration process for any new account that is password protected.

You should always pick ambiguous questions that have answers that ONLY YOU would know. “What is your hometown?” or “What high school did you attend?” are bad choices because these are things people could easily find out about you. In fact, they’re probably on your Facebook page.

## **Where can I get free anti-virus software through the military?**

The Army website for free virus software is the site for the U.S. Army Computer Emergency Response Team – Computer Network Operations, which can be found at <https://www.acert.1stiocmd.army.mil>

You will need your Army Knowledge Online user name and password or your Common Access Card to log on to the site and download fully licensed versions of professional-grade antivirus software at no cost.

The site also offers other computer protection software such as anti-spyware programs.

**What are some simple mistakes that are easy to avoid?**

- Posting things like phone numbers or addresses in a public place on the internet. If someone you know asks for one of these things it's better to send it to them via email than posting it on their 'wall.'
- Using poor passwords
- Following links from unknown sources.

**Wouldn't the best practice be to just not use the internet?**

The internet is quickly becoming an integral part of day to day life for most people in the military community. Although it comes with its risks there is no reason to not use it to its fullest potential as long as we do what we can to mitigate those risks.

**What are some other resources I can use to find out more on Information Assurance?**

- <http://iase.disa.mil/eta/>