Air Force Print News Today

Air Force news from around the world

What's the most popular computer password?

Commentary by Master Sgt. Russell Petcoff
Secretary of the Air Force Public Affairs

10/16/2009 - **WASHINGTON (AFNS)** -- Do you know what the most popular computer password is?

My guess would have been "password" or the ever sneaky "p@ssword." Turns out, the most common password is "123456." Wow, that will surely baffle cyber crooks.

Believe it or not, some folks have looked into that. They researched passwords stolen from a popular e-mail service by phishers. Another popular password is "111111." My guess is security is not on the mind of anyone choosing that password.

I bring this up because October is Cyber Security Month. It's time for everyone to think about their efforts to protect their computer systems and identity while online.

Secretary of the Air Force Michael B. Donley and Chief of Staff Gen. Norton Schwartz wrote about the importance of cyber security in a memorandum dated Aug. 20.

"Cyberspace is a contested domain, and the fight is on, today," they wrote. "Every Airman holds the key to success, and every Airman must become a cyber defender, whether acting as part of a team or individually on Air Force networks. We must all conduct ourselves as 'Cyber Wingmen,' recognizing that our actions and activities on the network affect every other Airman and impact our ability to execute the broader Air Force mission. We will, in short, deliver on our promise to *fly, fight* and *win* ... in air, space and cyberspace."

No doubt, everyone has read cyber security tips. It's always a good idea to review them if you've read them before. And if these tips are new to you, hope you will take them to heart. Air Force cyber security officials recommend the following tips for your home computer:
-- Use Anti-virus programs. Servicemembers and government employees can download free antivirus programs at **https://www.jtfgno.mil/antivirus/antivirus_homeuse.htm**.
-- Keep firewalls turned on. Firewalls keep out hackers and prevent any malware from sending out your personal data over the Internet. Both Windows and Mac OS X have basic firewalls installed.
-- Install a spyware/malware removal tool. Not all antivirus software removes spyware and adware. Look for spyware/malware removal tools.
-- Don't use an administrative account. Administrator accounts on your computer should only be used when you want to make big changes to your system, or install new software. At all other times you should be using "standard user" accounts.
-- Choose a strong password. This is one of the most important security steps anyone can take. Use a password with a minimum of 12 characters; however, more is even better. Your password should include capital letters, lowercase letters, punctuation, numbers and special characters. According to National Cyber Security Alliance (**http://www.staysafeonline.info/**) one way to choose a strong password is to choose an easy-to-remember phrase and convert initial letters into a password. "For example, 'Only you can prevent forest fires' could become: oYcp4estF,'" according to NCSA officials.
-- Keep the operating system up to date. Be sure to install the updates to ensure your computer has the latest protection. The best solution is to have the computer set for daily automatic updates.
-- Be careful what you download. Carelessly downloading e-mail attachments can circumvent even the most vigilant anti-virus software. Never open an e-mail attachment from someone you don't know and be wary of forwarded attachments from people you do know.

Many people like to surf the Internet while enjoying a "cup of joe" at the local coffeehouse. NCSA officials warn users of WiFi hotspots.

"The most convenient wireless services -- free hotspots offered by coffee shops, schools, libraries, etc. -- carry the greatest risks," according to NCSA officials. They warn criminals can use the public network to intercept your online activities.

If you use a laptop, there are additional security considerations, according to NCSA officials:
-- Treat your laptop like cash.
-- Keep it locked with a security cable.

-- Keep it off the floor.
-- Use a non-descript carrying case.
-- Keep your passwords elsewhere.
-- Password protect your system.
-- Backup important data before traveling.
-- Write down serial numbers to your laptop and keep it safe.
-- Mark or engrave your name and telephone number on it.
-- Report theft to local authorities immediately. Also, go to Consumer Information section of the Federal Trade Commission (**www.ftc.gov**) to learn about data breaches and identity theft.

So remember, you are the key to your cyber security either at home or at work. It should be a way people lead their lives.