

# Cybersecurity Awareness Month

October 2014



## ON CYBER PATROL

[ciog6.army.mil/OnCyberPatrol.aspx](http://ciog6.army.mil/OnCyberPatrol.aspx)



WASHINGTON (Sept. 26, 2014) -- During cybersecurity awareness month in October, the Army will be focusing on cybersecurity policies, practices and training to improve overall readiness. As part of this effort, commanders at all levels will lead cybersecurity awareness activities.

"Lethal Keystrokes," the Army's theme this year, highlights how simple mistakes made by a few can jeopardize military operations and business processes, compromise personal information and incur significant costs in time and resources.

"The Defense Department gets hit with approximately 10 million cyber attacks each and every day, and a very large number of them are aimed directly at the Army," said Essye B. Miller, cybersecurity director, Chief Information Office/G-6. "The potential for compromise of the network and the information it carries, and thereby harm to the Soldiers and leaders who rely on them, is simply enormous."

"Lethal Keystrokes" emphasizes individual responsibility for protecting the network and the Army, Miller said. Numerous incidents over the past several years have compromised sensitive information at the highest level of the Army. In addition to external threats, malicious insiders and lax cybersecurity practices pose significant risks.

Ongoing awareness training helps improve daily practices that safeguard information and communications technologies, as well as warfighting and business capabilities.

"Protecting our information and IT systems is a team effort. All Army personnel, whether Soldier, civilian or contractor, are responsible for safeguarding the network and our data," said Miller.

"Leaders must continue to enforce good cybersecurity practices and emphasize the impact of failures on unit readiness and mission capability. But, it's also incumbent upon every individual, regardless of rank or position, to get educated. That is, to stay abreast of threats and the best ways to avoid them, and to be vigilant," she added. "All users should think of themselves as part of the Army's cyber defense force."

Cybersecurity doesn't stop at the office door. Army personnel must protect their home computing environments, as well. Security experts recommend everyone follow the tips below.

Protect your system:

- Use anti-virus software.
- Protect computers with firewalls.
- Password-protect your wireless router and network.
- Encrypt your wireless signal.
- Regularly download security updates and patches.
- Disconnect from the Internet when not in use.

Protect yourself:

- Back-up your computer regularly.
- Restrict access to your computer and accounts; sharing has risks.
- Delete email from unknown sources, then empty the "trash" folder to make sure it's off your system.
- Use hard-to-guess passwords and keep them private.

Protect your family:

- Help your family check computer security on a regular basis.
- Take advantage of Army cybersecurity resources if you have a Common Access Card (CAC). Access information on protecting yourself online, get free security software for Soldiers and Army Civilians, and find cybersecurity training.

More OnCyberPatrol comics and articles can be found on the Army's OnCyberPatrol website located at: <https://ciog6.army.mil/OnCyberPatrol.aspx>

Readers with an Army AKO account can access more information regarding PII and other Cybersecurity related topics at the Army's IA One Stop Shop Website: (<https://informationassurance.us.army.mil>)