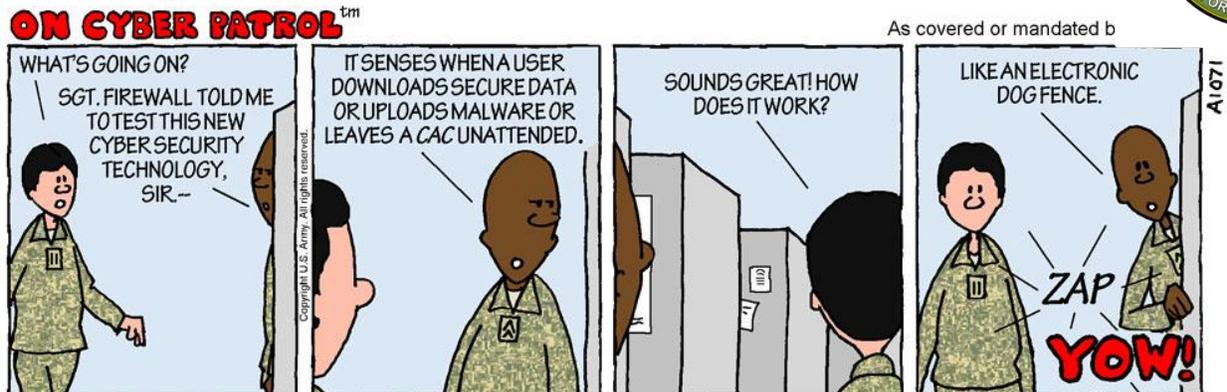


2011 New Year's Resolutions (Theirs, Not Ours)

January 2011



In an intelligence coup, G2 operatives were able to secure the New Year's Resolutions of the infamous International Cyber Criminal (ICC). Normally such information would not be released to the public in order to keep military intelligence gathering techniques and operations secure. However, as this information was taken from an unsecured social networking page of one of the ICC's top lieutenants, the decision was made to release it for its educational value. Fortunately, no American military member, government employee, government contractor or any of their family members would ever do anything like this. We have rules and regulations that are scrupulously followed to protect our secure data and personal identifications.

1. Take advantage of the fact that because most soldiers won't follow their New Year resolutions to be better at cyber security, that we won't follow ours to dramatically increase our efforts to steal their data and IDs.
2. Infect more computers belonging to military families with spyware and malware through simple fake web sites and disguised links in emails.
3. Obtain more U.S. and Coalition operational data from war zones simply by monitoring what is posted on social networking sites.
4. Aggressively promote the idea that taking secure data from government websites and posting it on the Internet is the ultimate expression of freedom and the duty for right thinking Americans (right thinking for us bad guys that is).
5. Have internal agents increase their scouring government and military offices and installations for unattended CACs, written copies of passwords and Personal Identification Numbers and unsecured mobile computers and storage devices.
6. Promote the activities of disgruntled military and government personnel to steal data or sabotage secure networks.
7. Continue to take advantage of people's gullibility, fear and greed through well targeted and sophisticated phishing schemes that will enable us to access personal and work data and steal Personally Identifying Information.
8. Promote the idea that we bad guys are uneducated third-world thugs who have no way of understanding or defeating the technological might and cyber security expertise of the United States and its allies.
9. Use every waking hour, every human and technological resource, every available financial backing and every creative way possible to defeat U.S. cyber security efforts.
10. Never give up until we have broken the technological backs of the Americans though simple deception and data theft.

Fortunately for U.S. military and government personnel, all of the ICC Resolutions can be defeated through sound cyber security and information assurance practices if used by everyone that has access to secure data. We've got that covered! Right?