

No deaths in Schriever cyber-terror attack

3/16/2007 — **SCHRIEVER AIR FORCE BASE, COLORADO** (AFNEWS) — A cadet stationed at the Air Force Academy was convicted of spear phishing after he circulated a suspicious email to more than 450 people on Schriever Air Force Base recently, coaxing 17 users into giving away information that could be used to send email to other users on the Frontrange Consolidated Network.

The email was part of a computer security attack that investigators with Air Force Cyberspace Command's Cyberspace Assurance Assistance and Assessment Program detected from Jan. 29 to Feb. 9.

Awareness campaigns have made most people aware of the dangers related to giving other Air Force members their personally identifiable information such as home addresses, credit card numbers, birthdates or Social Security numbers. However, information such as an individual's office symbol or email address may also pose a hazard in the wrong hands.

For example, someone on another Air Force base could obtain information from the Global Access List (GAL) to send an email to someone on Schriever, which is effectively the same as getting attacked directly. "It only takes one user to give away this information and potentially wreak havoc on a network," said Hank Gunlee, Cyberspace Assurance Office chief here.

What makes the matter worse is that several bases share the same network, Mr. Gunlee said. "If you compromise one account on the network, you've potentially compromised the entire Frontrange domain," he said.

Mr. Gunlee said his team hopes to sever all ties between the Schriever network and the rest of the Air Force.

During the attack, the NCC detected the scam within five minutes. Inspectors let the attack continue to see how it would play out. More than 450 people received the email.

The best defense is to beware emails from Air Force members stationed at other bases, Mr. Gunlee said. He also recommended protecting military email addresses, affiliation with specific units or offices and any other information that can be used by Air Force personnel at other bases to personally identify a Schriever employee.

Investigators worked with Schriever's Cyberspace Assurance office to let the attacker's email pass through Schriever's spam filters. The process took three days, said Master Sgt. Bryan Brinderson, 50th Cyberspace Communications Squadron, but they ultimately made it possible for the attacker to commit his crime.

Users who get emails from Air Force personnel at other bases should contact their client support administrators, who will in turn contact the Schriever Network Control Center at 567-3090. Users are urged to call 911 if the email contains an attachment larger than ten megabytes.

Search

[Advanced Search](#)
[Week In Photos: 11/24/06](#)

[Featured AF Links](#)

- [AF 60th Anniversary](#)
- [AF Bandstand Player](#)
- [AF Posture Statement](#)
- [AF Media Center](#)
- [AF Mission](#)
- [AF Senior Leadership](#)
- [AF Symbol](#)
- [Airman Magazine](#)
- [Biographies](#)
- [BRAC 2005](#)
- [Deployed Newspapers](#)
- [Fact Sheets](#)
- [Senior Viewpoints](#)
- [Senior Leader](#)
- [Soundbites](#)
- [Week in Photos Gallery](#)
- [Why I Serve](#)

[Specials](#)

[Blue Summit Videos](#)

[AF Cyber Command](#)
[Letter to Airmen
CSAF Vector](#)
[New Viewpoints](#)

[How We Fight Video](#)

[AF 60th Anniversary](#)
[Other Links](#)

- [AAFES](#)
- [AF Crossroads](#)
- [AF Personnel Center](#)