



READINESS RULES

“Knowledge Saves Lives”

<http://www.uosp.uga.edu>

University Office of Security Preparedness Bulletin

January 2005

Asa T. Boynton Retiring after 34 years in public safety



Serving as the Associate Vice President of The University Office of Security Preparedness since its inception, Mr. Boynton will retire January 1, 2005. This office was created and guided by Mr. Boynton from its beginning in the summer of 2002. With the goal of bringing awareness of dealing with the possibility of terrorist threats to the University community, Mr. Boynton has set the tone for the importance of preparedness in a time of uncertainty.

Mr. Boynton began his law enforcement career at the University of Georgia, where the biggest problems on campus were panty raids, streaking, and student demonstrations. Since 2002, his efforts have been in devising ways to protect the university against terrorism.

Starting work as a UGA police officer in 1969, Mr. Boynton became Public Safety Director in 1983. With a business degree from Fort Valley State, he took the police job while working on his M.B.A. but as he advanced in rank, he found he liked law enforcement. He switched his major to public administration and earned an M.P.A. in 1973.

He worked eight months as chief of the community relations division in the St. Petersburg, FL police department, then returned to UGA in late 1973 as Assistant Public Safety director and has been at UGA since.

The seismic shift from policing student pranks and protests to thwarting possible terrorist attacks may be the defining change in his 34 years in campus public safety, including 19 years as UGA's Public

Safety Director. As Public Safety Director, Mr. Boynton dealt with radiation and chemical hazards, campus crime, fires, disorderly football fans, visiting dignitaries, and massive crowds of campus visitors.

Career memories include the university's Bicentennial...a 15-month commemoration of UGA's 200th anniversary in 1984-85. He was on the steering committee that planned scores of events that brought thousands of visitors to campus. Another favorite memory is the 1996 Olympics. The challenge was daunting in providing throngs of visitors and soccer fans with a safe venue.

“My main goal,” he adds, “was to leave this place in better shape than I found it. I think we've done that, and there are good people here to carry on.”

We will miss him.

Security Tips during the Winter Season

With shorter days and longer nights during this time of the year, it is important to:

- Continue to be aware of your surroundings.
- Report any suspicious people on campus to the University police at (706) 542-2200.
- Have an emergency kit already prepared and readily available. (Refer to the University Office of Security Preparedness' (UOSP) website: www.uosp.uga.edu for a tutorial and brochure “**GRAB AND GO!**” that provides information on making an emergency kit.)

University Winter Weather Closing Information:

- Visit the website: www.uga.edu/news
- Listen to Athens radio stations:
A.M. dial: 960 and 1340
F.M. dial: 88.9, 90.5, 91.7, 97.9, 102.1, 103.7, 106.1

Featured Article

Cyber Security – Part II

By: Stan S. Gatewood - UGA CISO, CIFI
UGA- Office of Information Security and
Centaur Lab

[This is Part II dealing with cyber security. Part I is available from the July 2004 bulletin found on the UOSP website's homepage under Readiness Rules (bulletins) in the Awareness section.]

Your home computer is a popular target for intruders. Why? Because intruders want what you've stored there. They look for credit card numbers, bank account information, and anything else they can find. By stealing that information, intruders can use your money to buy themselves goods and services.

Five things to do to make your computer secure:

1. Use "anti-virus software" and keep it up to date. Make sure you have anti-virus software on your computer! Anti-virus software is designed to protect you and your computer against known viruses so you don't have to worry. But with new viruses emerging daily, anti-virus programs need regular updates, like annual flu shots, to recognize these new viruses. Be sure to update your anti-virus software regularly! The more often you keep it updated, say once a week, the better.

2. Don't open emails or attachments from unknown sources. Be suspicious of any unexpected email attachments even if they appear to be from someone you know. A simple rule of thumb is that if you don't know the person who is sending you an email, be very careful about opening the email and any file attached to it.

3. Protect your computer from Internet intruders - use "firewalls." Equip your computer with a firewall! Firewalls create a protective wall between your computer and the outside world. They come in two forms, software firewalls that run on your

personal computer and hardware firewalls that protect a number of computers at the same time.

They work by filtering out unauthorized or potentially dangerous types of data from the Internet, while still allowing other (good) data to reach your computer. Firewalls also ensure that unauthorized persons can't gain access to your computer while you're connected to the Internet.

4. Regularly download security updates and "patches" for operating systems and other software. Most major software companies today release updates and patches to close newly discovered vulnerabilities in their software. Sometimes bugs are discovered in a program that may allow a criminal hacker to attack your computer. Before most of these attacks occur, the software companies or vendors create free patches for you that they post on their web sites. You need to be sure you download and install the patches! Check your software vendors' web sites regularly for new security patches or use the automated patching features that some companies offer. Ensure that you are getting patches from the correct patch update site.

5. Use hard-to-guess passwords. Mix upper case, lower case, numbers, or other characters not easy to find in a dictionary, and make sure they are at least eight characters long.

As with physical security, information security depends on individual participation in the quest to protect sensitive areas from misuse and potential threats. These five tips are guides for a more secure computer. For more details on information security, go to <http://www.infosec.uga.edu>.

Bulletins are available bimonthly. The issues assist in disseminating current security preparedness information from this office and other University units. Sign up to receive issues of *Readiness Rules* by e-mail. Click on "bulletin by e-mail" located on the [home / contact us](#) bar on the UOSP website.



Upcoming Issue:

Terrorism - Student Perspective