2-11-2004

Unsolicited email (SPAM)

Bill Levernier
Georgia Southern University

Unsolicited email (SPAM)

Submitted by: Bill Levernier

2/11/2004

Question:

Is Information Technology Services (or some other office) attempting to do anything to stop the unreasonable amount of unsolicited e-mail we are receiving on an almost daily basis? I am constantly receiving emails, which I do NOT open, from commercial enterprises that I have never done business with. How are these enterprises getting our e-mail addresses in the first place? Also, it seems like the problem has gotten worse since we migrated to GroupWise. Has anyone attempted to determine whether migrating to GroupWise has made the e-mail problem worse?

Rationale:

Is Information Technology Services (or some other office) attempting to do anything to stop the unreasonable amount of unsolicited e-mail we are receiving on an almost daily basis? I am constantly receiving emails, which I do NOT open, from commercial enterprises that I have never done business with. How are these enterprises getting our e-mail addresses in the first place? Also, it seems like the problem has gotten worse since we migrated to GroupWise. Has anyone attempted to determine whether migrating to GroupWise has made the e-mail problem worse?

Response:

Bill Levernier (COBA) requested information regarding efforts to block SPAM email, which was referred to David Robinson (CLASS), the Senate member of Information Technology Advisory Committee.

Robinson (CLASS) reported as follows:

SPAM, or unsolicited e-mail, falls into several categories: unsolicited commercial mail from off campus sources, unsolicited quasi-commercial mail from on campus sources,

and viral mail, which is mail created by computer worms attempting to spread themselves. IT services currently filters for viruses and unsolicited commercial from off-campus sources with a software package called RAV. Suspected SPAM is passed on to recipients with special notification in the subject heading. RAV has been a limited success, and is being discontinued by its new owner, a spunky little startup named Microsoft. Georgia Southern will replace it with a new hardware-based solution called Barracuda. (A link is provided for information on Barracuda.)

Barracuda uses a range of state-of-the-art methods for detecting and filtering SPAM, none of which are very good. It has been selected by IT Services based on price and the experience of other academic institutions. More advanced content filtering will be possible, and configurations of this will be tried out during a testing period before the final purchase decision is made. ITAC will review these plans and make recommendations as necessary. The principle user concern is that whatever filtering solution we have not block mail so successfully we no longer get legitimate mail The lesser problem of unsolicited quasi-commercial mail sent over GSINFO was discussed at the March 9th meeting of ITAC. A range of possible policies will be forwarded to the Provost for action. In reference to the increase in SPAM in recent months, this is not Georgia Southern specific; it is universal. As to the question of how commercial enterprises come into possession of our e-mail addresses, the Georgia Open Records Law permits outside entities to obtain campus e-mail lists, but according to Jeff McLellan (University Counsel) this has rarely been done. In general, spammers obtain addresses by harvesting them from internet discussion lists, from web pages with programs that surf the web looking for them, by buying them from disreputable online vendors with whom you have done business, or by randomly generating likely user names. Viral mail is typically sent to addresses which the invading computer virus has stolen from a machine that is already compromised, which is another way these addresses get out there, and why you get viruses from people you think you know. With the death of our old e-mail addresses, we may see a downward spike in SPAM shortly after the end of this academic year.