Even More What to Look for in a Phishing Email

UGA Policy Update.

EITS <EITS@uga.edu.com>

Sent: Wed 8/6/2014 3:17PMM

To: UGA Staff

Reply to address is similar to the sender name, but it contains a red flag. Did you spot it? It's tricky: UGA email addresses do not have a .com at the end.

The recipient is generic, but could be legitimate based on the alleged sender. But, doesn't UGA use a list service for mail like this?

Dear Colleagues, **Does not address you by name, so this is a third red flag.**

Each University department/unit is responsible for implementing, reviewing and monitoring internal policies, practices, etc. to assure compliance with the UGA Policies on the Use of Computers.

Poor grammar or misspellings are expected in phishing attempts. This message has none: would it fool you ?

Violations of these policies may incur the same types of disciplinary measures and consequences as violations of other University policies, including progressive discipline up to and including termination of employment, or, in the cases where students are involved, reporting of a Student Code of Conduct violation. In some cases, violations of this policy may also be violations of state and federal laws, and consequences may include criminal prosecution.

This sounds official! It should, it was copied straight off of an official UGA EITS web page.

An update has been made to a policy that affects you.

Please log in to view this update: UGA Policy Update **If this were a live email message, you could hover your mouse over the link to highlight it so you could see where the link really goes. (DO NOT click it!) It would point to** http://policyform.uga.edu.com **a fraudulent site that looks exactly like an official UGA EITS webpage. If you signed in, you would give away your credentials.**

Thank you,

EITS

The signature matches the sender name, but is suspiciously generic. UGA rarely sends out email with a generic signature. They usually come from an actual person and include contact information.