

Protect Yourself from Fraudulent Emails

Information Technology Services (ITS) at Augusta State University is committed to protecting your on-line privacy, therefore it is important that you understand our security practices. We recognize your need for appropriate protection and management of your personal identifiable information. The following information is designed to help you protect yourself from fraudulent email and password capture scams.

ITS will not send you an email asking for your user name, password or other personal/account information, nor will we ask you to re-verify or to change personal information which is already on file without first displaying the existing information. We will not send emails with "active" content such as Java, JavaScript, and ActiveX based attachments, or pop-ups.

What to Watch Out For:

Fake or spoofed emails will often look legitimate. They may include references to the university, other trademarks, logos and links to realistic looking web pages. Never rely on the name in the "From" field as this is easily altered.

Spoofed emails often invite you to re-verify account or personal information and are often initiated by the spoofing party without any action on your part. Ask yourself the following questions:

- Does the email I just received seem out of place, or is it a response to a question I posed to a legitimate person I do business with?
- Does the email create a sense of urgency or have time limits which I did not expect?
- Does it contain spelling or grammar errors?
- Does it contain offers for prizes or awards not expected?
- Does it contain links to strange web sites, or web sites whose name and URL as displayed don't match or contain misspellings?
- Does it contain active content such as Java, JavaScript, ActiveX or any other type of plug in, or ask you to download a special plug in or viewer?

If the answer to one or more of these questions is "Yes", then the email may be suspicious. Think of a stranger approaching you on the street and asking for your username and password. Treat these potentially fraudulent emails with the same caution.

If you are ever suspicious of any email or communication you receive, contact the ITS Help Desk at 706-737-1482 to get assistance on verifying the legitimacy of the email. If the email is found to be a fraud, the Help Desk will advise you appropriately.

These attempts at compromising your personal identifiable information will not just be on your work-related emails. You may get these at home as well. Treat them with the same level of caution and if you are unsure of why some entity, for example PayPal or your

bank, is asking for you to reply to an email with your information, contact the entity in your customary manner to seek verification. Do not use the reply feature of the suspicious email.

The Federal Trade Commission (FTC) is an invaluable resource for answers to questions related to email fraud (phishing) or identity theft.

For details on phishing: <http://www.ftc.gov/bcp/edu/pubs/consumer/alerts/alt127.shtm>

For details on ID Theft: <http://www.ftc.gov/bcp/edu/microsites/idtheft/>

Great resource on information security: <http://onguardonline.gov/index.html>