



HALL COUNTY SHERIFF'S OFFICE

CRIME PREVENTION UNIT



CRIME PREVENTION TIP

DATE: October 30, 2009
SUBJECT: Computer Security

Recently a subscriber to our crime prevention notices brought to our attention a telephone / internet solicitation that poses some computer security concerns.

She was initially contacted by telephone from a purported "Windows service provider" on a Saturday, stating that they received internet confirmation of potentially harmful viruses on her computer (**red flag #1**). The caller then asked that she go into her computer's files and review the history log, where she found a number of yellow or red warning or error signs. The caller then stated that these would need to be taken care of and that he would need a supervisor. Within seconds, a "supervisor" (**red flag #2**) came on the line and said the problems needed to be fixed and requested remote access to her computer (**red flag #3**). Fortunately, our subscriber declined that request and being very diligent, asked for a call back number and the address of the company. A little research revealed that the company is based in New York and has a less-than-professional website advertising its services as described in the call. She chose not to enlist the services of the company, and there are several reasons why we think this was a good decision.

Lessons Learned

Red Flag #1: This point alludes to the possibility that this caller may have already gained access to her computer. The statement may have simply been a sales bluff because he knew whatever they were looking at would be there anyway, but we don't know this for certain.

Red Flag #2: It seems awfully strange that the person making the solicitation call doesn't even have the skills to perform the service advertised. The "supervisor" routine merely sounds like an attempt to make things sound more official than they really are.

Red Flag #3: An unsolicited caller has just requested remote access to a computer. Remote access is a completely valid tool, but be extremely cautious in granting this to anyone. Once you grant access, not only could your personal information be compromised, but your computer could be used for any number of unauthorized things without your knowledge.

** If you are in need of computer work such as this, there are always local companies that provide the same services who are easily verified. Nothing wrong with keeping business local.

** Always be wary of an unsolicited call of any sort, but especially one that requests personal or financial information. The potential for the compromise of both is great with regard to personal computer security.

** Diligence and caution pay off. If you're not familiar with a business, always research it before committing to them, especially if it involves the release of or access to your personal information. And just because a "company" has a website doesn't necessarily mean they are legitimate. Websites are as easy to establish.

If you have any questions or concerns, please contact

Deputy Stephen Wilbanks
Crime Prevention Coordinator
Hall County Sheriff's Office
610 Main St.
Gainesville, GA 30501
770-533-7674
swilbanks@hallcounty.org