

Welcome... This edition of *Inside Audit* is devoted to the IT side of Audit. We're so sure you'll find this information helpful, future issues will feature an IT Corner with reminders for computing safety.

Meet The Auditor



Sixteen years ago, Carol Westbrook came to George Mason University as a Senior Auditor. Today she is the Department's IT Audit Manager. When Carol is not busy auditing IT systems, she can be found enjoying theatrical productions starring her son Dan, who is a junior at James Madison University.

Risky Things People Do to Compromise Their Computer Security

Use a password that is easy to guess by basing it on a dictionary or real word:

Examples: "Password," your name, your cat's name, any name at all, any word that can be found in a dictionary.

Why it is dangerous: Hackers routinely use so-called 'dictionary attacks.' They simply run an entire dictionary against your password, so a password consisting of an English word will be cracked in seconds, if not faster. Hackers also know that when people are asked to create stronger passwords, using numbers, symbols, and upper and lower case letters, many will go for the easiest way, keeping a dictionary word and capitalizing the first letter of their real word and ending it with a 1 or symbol. Cracking algorithms are created to look for these "easy" combinations. Dictionary attacks can also include common substitutions of numbers for letters such as 3 for e and 1 or ! for I or l.

Remember to always use at least eight characters, and the more random and varied the characters are in your password, the better.

Open emails from strangers and run the attachment.

In addition to helping people to share information cheaply and almost instantaneously, email has become an ideal medium for disseminating computer viruses and other malicious software. Hackers quickly learned to use email attachments to send their destructive payloads. They also learned particularly well how to use social engineering to construct titles and messages that a large number of people would still fall prey to.

To protect yourself, make sure that you open only email that doesn't look suspicious. Be ten times more careful with messages that include attachments, even if they appear to be from your friends. Numerous programs exist that fight email viruses and spam, but nothing can replace simple common sense.

Fail to install updates for Windows and your anti-virus software.

Even though updating Windows can be cumbersome, people who fail to update have only themselves to blame in case they become victims of an exploit already fixed by Microsoft. Your anti-virus solution is only as good as the definitions it uses to detect malicious code. Outdated definitions can't protect you against the latest threats. Set your computer to automatically run "live-Updates" for both your operating system and your anti-virus solutions.

Click Yes on "Installing free plug-ins" popup while surfing the Internet.

Everybody who spends a few hours a day surfing the Internet has seen those "friendly" offers of free software appearing seemingly out of nowhere. Free self-adjusting atomic clock, etc. The trouble with this free software is that it doesn't come alone. It will usually install some other things on your computer that you won't necessarily like. Namely, programs tracking your every move on the Internet, redirecting you to the website that you never wanted to see, feeding you with deceptive ads and so on.

So before clicking "yes," think!

New University Policies

General Policies

- [Policy 1126](#) Participation in Political Activities

Admin Policies

- [Policy 2224](#) Recruitment and Hiring of University Employees

Research Policies

- [Policy 4014](#) Policies for Effort Certificate Reporting

REMINDER:

[University Policy Number 1301](#), Responsible Use of Computing, applies to all University faculty, staff, students, visitors and contractors. The University provides and maintains computing and telecommunications technologies to support the education, research, and work of its faculty, staff, and students. To preserve the security, availability, and integrity of the University's computing resources, and to protect all users' rights to an open exchange of ideas and information, this policy sets forth the responsibilities of each member of the Mason community in the use of these resources.

To view this and other university policies go to: <http://universitypolicy.gmu.edu/>

The Lighter Side of Audit

A guy in a bar leans over to the guy next to him and says, "Want to hear an auditor joke?" The guy next to him replies, "Well, before you tell that joke, you should know that I'm 6 feet tall, 200 pounds, and I'm an auditor. And the guy sitting next to me is 6'2" tall, 225 pounds, and he's an auditor. Now, do you still want to tell that joke?" The first guy says, "No, I don't want to have to explain it two times."

