

# The Roanoke Times

[Roanoke.com](http://www.roanoke.com)

Sunday, January 20, 2008

## Fending off digital thieves

Guarding Virginia Tech's vast computer network and users' privacy is a full-time job.

By [Anna L. Mallory \(mailto:anna.mallory@roanoke.com\)](mailto:anna.mallory@roanoke.com)

381-8627



Matt Gentry | The Roanoke Times

Randy Marchany, director of Virginia Tech's information security lab, looks at the [antivirus.vt.edu \(http://antivirus.vt.edu/\)](http://antivirus.vt.edu), which is a Web site that has information and tools for preventing computer and identity tampering. Below, he looks over a map showing computer activity on campus. The chart shows the volume of hacker probes and attacks since midnight that day.



### Think you've been attacked?

- If you're at Virginia Tech, contact [abuse@vt.edu](mailto:abuse@vt.edu) (<mailto:abuse@vt.edu>)

Within 10 hours on Jan. 9 -- midnight to 10 a.m. -- computer hackers lurking in cyberspace scanned Virginia Tech's computer networks 15,000 times, looking for a way to reach information, such as credit card or Social Security numbers, contained in some of the cabinet's drawers.

That keeps people such as Randy Marchany busy, competing a fast-paced race colleges run with hackers -- some tied to organized crime -- to safeguard information.

Many are falling behind.

As director of Tech's information security lab, Marchany spends his time monitoring the university's vast computer networks, hunting for potential break-ins, updating software, patching system holes and educating people about the best ways to protect their information online.

"Every time somebody comes up with a new hole and you find a fix for the attack, somebody comes up with a countermeasure," Marchany said. "It's always very fluid."

And some protective steps, such as cutting off the university community's access to certain Web sites or computer programs, aren't acceptable solutions.

"Because we're a university, and you're maybe doing research, I'm not going to get in the way of you doing your job," Marchany said. "In a university environment, we have to be open."

But that doesn't mean information isn't protected.

Tech -- and most schools -- use tools such as firewalls and encryption to

- If you're at Radford University, contact [helpdesk@radford.edu](mailto:helpdesk@radford.edu) (<mailto:helpdesk@radford.edu>)

#### Tips to stay safer

Computer experts says some common-sense steps can help keep your computer and your personal information safe.

- Put information on CDs or USB drives and lock in a desk drawer.
- Update systems with manufacturer patches.
- Clean out old folders.
- Lock laptops.
- Never open links from unknown e-mails.
- Use Web sites with padlock in right-hand corner.
- Keep passwords long and complex.

#### Public resources for protection

Check out these Web sites for more information about protecting your computer:

- [privacyrights.org](http://privacyrights.org) (<http://privacyrights.org/>)
- [security.vt.edu](http://security.vt.edu) (<http://security.vt.edu/>)
- [truecrypt.org](http://truecrypt.org) (<http://truecrypt.org/>)
- [microsoft.com/protect/computer/updates/bulletins/default.mspx](http://www.microsoft.com/protect/computer/updates/bulletins/default.mspx) (<http://www.microsoft.com/protect/computer/updates/bulletins/default.mspx>)

#### By the numbers

- 500: Number of computers in the Math Emporium, Tech's largest computer lab

keep unwanted people from viewing their data.

#### An appealing target

Because of the intricate web of information stored in computers across college campuses, they are increasingly becoming targets for hackers, said Walter Conway, a private consultant with Walter Conway Associates who works with colleges to help protect their payment systems.

College campuses offer multiple wireless access points and each department typically has its own information technology department that handles data differently, things that make the system as a whole vulnerable.

In 2007, the nation's schools, including Virginia Tech, put 1.2 million sensitive records at risk, according to the Identity Theft Resource Center.

Stolen, leaked or publicly accessible Social Security numbers, credit card digits and student and staff addresses are the kind of data that can lead to identify theft in the wrong hands.

The ITRC tracked 111 of 448 security breaches in 2007 to schools. In September, a dozen or more of those documents that contained students' Social Security numbers or partial numbers came from Blacksburg computer systems. But no evidence exists that anyone's identity was stolen, according to the center.

Earlier this month, the University of Georgia had to contact 4,000 current and former students when a hacker accessed one of its networks and got a list of Social Security numbers.

One reason for so many leaks is that the tools that schools use -- firewalls, anti-virus software, passwords and even Google searches -- are the same resources that would-be hackers have, Marchany said.

And these days, hackers are more brazen.

Instead of trying to tear down network walls, hackers often try to con users out of sensitive information.

A common technique is phishing. To do that, hackers pose as reputable organizations and send out e-mails with links to phony Web sites. When victims open the e-mails, they are sent to a page that looks like the reputable site -- except any information or passwords given out go to the hackers.

Another criminal act, often called social engineering, is to pose as an employee inside an organization and just ask for a password or sensitive

- \$45 million: Current budget for Tech's centralized information technology department
- 400: Number of employees in the centralized IT department

information.

"It's a lot easier if I'm a bad guy to get you to give me the information than to go storm the IT walls," Conway said. Both Tech and Radford University use third-party processing agents to complete credit card transactions for payments, such as tuition. Those systems are held to national protection standards, Conway said.

### Getting the word out

While most people think of hackers as people slaving over keyboards to break into computer networks for fun, many hackers actually use computer programs that work to guess passwords or hunt for unsecured wireless networks to steal information, Conway said.

Even if potential hackers don't ask for information, they can still find it

legitimately. Conway said often organizations don't have the time, or the money, to educate people about the best ways to store information or how to take precautions against social engineering.

In September, when Liberty Coalition, an identity-theft watchdog group, found documents listing Social Security numbers and names of Tech students published to a public file on one of the university's servers, the group contacted Tech, and the information was removed from public view -- but its presence meant no one had to hack and no one had to ask.

Marchany attributes that security breach to a "digital pack rat," someone who stockpiles information long after it's needed. He said the error was corrected and that it underscored the need for more education.

Teaching people about the dangers of storing personal information online is key. Although many tips are common sense, Marchany said people often don't listen.

Chief among the safeguards is to delete the personal information, Marchany said, or to store it on a portable device such as a USB drive. But even that can cause problems. Conway suggests that storing info on disks or drives is most dangerous because it can be easily lost.

Schools try to promote software tools that will scan for sensitive information and try to safeguard documents. Some of the resources are free and can scan individual computers for potentially dangerous information.

### Tighter security

IT employees at Radford and Tech use advanced Google searches to hunt for personal information that might be stored on their Web sites. But so do hackers.

In January 2007, Radford officials found that someone had broken into a server containing "personal information" in the Waldron College of Health and Human Services on campus. Investigators didn't find that any information had been stolen or even viewed, a spokeswoman said.

Tech tracks potential break-ins and hunts for public documents that could compromise identity, but often it has to wait for someone else to tell them about a potential breach, he said. And some schools, such as

Radford, don't have time to track the number of potential hacks on campus.

"We know there are attempted attacks, whether it's one or 30,000, we still want to have as secure a system as we can have," said Danny Kemp, chief information officer at Radford. "Is the number that important?"

State law requires that public institutions report security incidents to VITA, the Virginia Information Technology Agency. But the rules apply only if they result in a personal information breach.

Tech -- along with the University of Virginia and William and Mary -- is exempt from the state's reporting rules. The exemption is part of the state's Higher Education Restructuring Act, passed in 2005. The act gives the three schools more autonomy. Regardless, Marchany said, their IT department follows most of the same guidelines, such as reporting incidents that result in exposure of sensitive data.

In 2007, colleges across the state reported 70 security incidents to VITA. One was from Radford. Not all of the incidents were data breaches, according to a VITA spokeswoman. She did not say how many were.

VITA suggests that IT directors report incidents that disrupt daily activities, or those that cannot be explained. For the most part, schools aren't required to report threats or social engineering attempts.

Still, Conway suggests that schools should follow a higher standard because of their higher level of vulnerability.

Conway and Indiana University's Dennis Reedy performed an analysis of security breaches between 2000 and 2007 that showed that colleges do have a hacking problem, he said.

"Nearly 40 percent of higher education breaches were the result of hacks. This is twice the rate for businesses, and there is no indication that this high rate of higher ed hacking is slowing," Conway wrote in a blog on the subject.

He admits that schools will never cease all vulnerability, but he predicts a shift in the schools of thought surrounding data security.

Right now, people think, "Protect, protect, protect." He said the key element is to purge all nonvital sensitive data or "get off the bull's eye."

"You can protect, but no security comes with a guarantee," he said. "If somebody wants something, they can get it."

**THE ROANOKE TIMES**  
roanoke.com

Copyright © 2008