VANCOUVER BUSINESS JOURNAL
The Key to Southwest Washington Business
LOCALLY OWNED & OPERATED | AUGUST 20, 2010 | VOL. 17. ISSUE 35 | $2.50

INNOVATION AND TECHNOLOGY

Coming to a computer near you

How businesses can counteract the growing hacker threat

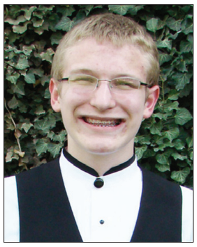
Last year, I took over management of my company's website. Being something of a programmer from a previous life, I had always wanted to run a website. Bravely, I began to convert an old Windows machine to Linux, configuring it as a server and getting it online.

It only took me about five complete installation attempts of formatting, installing and reformatting. A short time later, upon finding a rogue script I realized I had exposed my server to the Internet before it was fully secure.

For over a month, everyday at 4 p.m., a remote computer with an IP address in northeast China attempted to get information to hack my server. The hacker(s) did this by attempting to cause a "page fault," asking for a page that did not exist in order to get a reply from the server about what system it was running.

Hackers, based in places like Eastern Europe, China or right here in the U.S., are constantly on the look-out for ways to compromise computer systems, from the occasional web-browsing individual user to the small business owner installing new online accounting software.

BILL ROLLER
BR Capital


CHRISTOPHER ROLLER
Mountain View High School

No matter how big or small the target, the threat posed by hackers will only increase, according to information security analysts. There is even some speculation that the Chinese government itself may have hand in attacks on government, military and commercial interests around the globe.

So we are trapped in a virtual arms race, struggling to secure valuable information from the intruding eyes of an increasingly sophisticated hacking community.

And as computing power becomes more widely available, an increasing number of "zombie" computers, called "botnets," are being harnessed to attack even the most robust security systems.

This means constant vigilance on the part of IT staff and small business owners to constantly upgrade their information infrastructure to keep ahead of the threat. If you have not upgraded your routers, firewalls and virus protection software for several years – now might be the time.

Basic precautions for any business should include:

- Anti virus/firewall protection on every computer and router.
- Upgrading of routers to the latest level of protection.
- Closing of unused Internet ports, computers and routers.
- Daily virus scans
- Regular backups of data
- Use strong passwords that include lower case and capital letters, numbers and special characters
- Consider keeping valuable intellectual property on computers that are not connected to the Internet
- Management policies built into routers that prevent access to high risk sites by employees

Bill Roller, CFA, CFP is the president of BR Capital, a registered investment advisory firm. Christopher Roller will be a senior at Mountain View High School in the fall.