
IF COMPUTERS COULD MAKE NEW YEAR'S RESOLUTIONS, HERE ARE SEVEN THEY'D MAKE FOR A SAFE, SECURE 2007

Milford, CT December 15 --While artificial intelligence has come a long way, computer users are still the ones charged with security of their data, networks and computers. Human beings at the keyboards should take seven key steps to assure the maximum possible computer and network security as New Year's Eve approaches in a hacker prone era rife with data theft, historically high levels of SPAM, and increasingly innovative computer fraud.

"It doesn't take very long at all to enhance the security of a computer or its network," says Andrew Greenawalt, founder of Perimeter eSecurity, a company charged with protecting more than 4,000 computer networks nationwide. "Some of the more esoteric services we provide are more appropriate for the 1,600 plus financial institutions we protect," Greenawalt says, "but whether you have a small business network or a vast business enterprise, these seven steps are imperatives to optimize your eSecurity as the New Year approaches."

1. **Change every password you can find** before New Year's Eve: every online commerce site visited, every computer, and any other password protected device or website will be security enhanced with this simple, time efficient move. Avoid easily discovered passwords such as names or numeric series such as 98765. Resolve to change your passwords at least quarterly in 2007.
2. **Download patches and updates:** Even the least expensive computer security programs offer downloadable updates or "patches" that can detect the latest viruses, close "backdoors" that hackers have discovered, or otherwise enhance network protection. Software provider networks generally provide these downloadable patches at no charge for paid-up customers. Operating systems should be patched and upgraded at yearend—and regularly—as well. More sophisticated business security providers like Perimeter automatically patch and upgrade the computer networks they protect. Network owners with less thorough security programs should resolve to check and update patches on a monthly basis.
3. **Hire a Hacker:** Network owners should use the holiday lull to conduct a "penetration test," as it's called in the industry, to identify weaknesses in the network's security. Also known as a "vulnerability scan," these tests attack a network just as a hacker would. Instead of attacking databases and network tools, these scans report back on specific vulnerabilities and recommend ways to solve the problems they identify.
4. **Conduct Regular eSecurity Check-ups:** Keep your network safe by scheduling ongoing risk assessments. These automated, monthly remote risk assessments can be conducted for less than the cost of a single onsite review and can help assure that confidential customer and financial data are as secure as possible from external attack. Waiting a full year between risk assessments in today's Internet is no longer a viable option. ..

5. **Communicate and Review Your Data Security Policy:** Write a memo to all staff members stressing the importance of protecting such critical, confidential customer data as social security, bank account or credit card numbers. State an explicit policy on how and when, if ever, these should be included in unsecured email correspondence with customers and others. Consider implementation of a simple encrypted email system as a giant security step forward for 2007. Perimeter's "mailexchange" system for encrypted email, for example, costs less than 50 cents per user per day—far less than the cost of a single lawsuit.

6. **Keep Your Network Virus Free:** There's nothing worse than starting the New Year with a network infection. With the increasing amount of entry points for viruses to penetrate your network (email attachments, shared files, infected websites, downloads, etc), a full evaluation of your network is critical to ensure that safeguards are in place to protect all these entry points and minimize infection. Unfortunately, simply installing AV software is not enough... The AV system still needs to be monitored to ensure that the most recent definition files are updated on all devices and you are alerted when a device is not "up-to-date." But... even the monitoring will not assist in defending against new viruses that don't yet have definition files. Because most infections occur before a definition file is available, early warning signs of new outbreaks with built in defense mechanisms is critical; however, without a team of round-the-clock "malware specialists" this level of protection is difficult to achieve. In order to ensure full protection from viruses this year, evaluate a service which provides a full suite of AV services with the ability to be proactive with new outbreaks.

7. **Consider "giving up" on do-it-yourself security:** Just as few business people attempt do-it-yourself insurance or computer repair, fewer still are able to keep up with the increasingly complex, fast changing demands of computer network security. The New Year is a good time to consider "outsourcing" network security, Turn instead to thoroughly scrubbed secure internet bandwidth that is delivered by a professional outsourced network security provider like Perimeter. "We worry about all the security risks so the business network manager doesn't have to," says Greenawalt proudly. His company offers more than 50 different on demand, affordably priced, state-of-the-art network security services to small and medium sized businesses. They select the security levels and services they want so they can focus on running their businesses rather than constantly installing, integrating, upgrading and patching their IT security systems.

Founded in 1997, Perimeter eSecurity, is the only provider of complete eSecurity on demand, that offers network security "in the cloud," or directly to the network, for more than 4,000 growing companies nationwide. Headquartered in Milford, CT with seven geographically-distributed operations centers and three redundant data centers, the company is among the fastest growing network security providers. Its website, www.perimeterusa.com, offers a wealth of network security services and webinars that are available to businesses on demand.

For Further Information Contact:

Cathy Clarke
CNC Associates
617-527-2089
cathy@cncassoc.com