

## – NEWS RELEASE –

### Top Ten Myths of Information Security: What You Don't Know Will Hurt You

**CHICAGO, IL** – No one wants to think their most sensitive personal and financial data could be lost or stolen. It is a nightmare scenario: a single compromised computer can cost an organization millions in recovery costs, not to mention its hard-earned reputation. Yet most business people are woefully unprepared for the growing threat of information theft. They assume that they are fully protected by passwords, anti-virus software and other security precautions. They might as well believe in the Easter Bunny.

In a Special Report titled **Top Ten Myths of Information Security**, Daniel H. Harris, founder and president of **en-terpret.co**, an international Information Technology consulting firm, exposes the most common fallacies associated with data protection, such as:

- **Password protection is an oxymoron.** Any hacker who knows how to read can probably break through a password barrier faster than you can remember your username.
- **E-mail is an open book.** A single e-mail message will make hundreds, maybe thousands, of stops on other public systems before it reaches its intended destination.
- **Kids are a security risk!** When your children install “shareware” programs for pictures, videos or MP3’s they open the files on your home computer to anyone who really wants to look.
- **You can’t rely on firewalls.** Firewalls are designed to protect you against threats from the outside, but the biggest threats are found within the four walls of your own office.

Phone: 773.868.4381

Fax: 773.913.6217

[www.en-terpret.com](http://www.en-terpret.com)

3642 N Magnolia, Suite 2

Chicago, Illinois 60613 USA

Associated Worldwide with JHI  
[www.jhi.com](http://www.jhi.com)



- **A bad day “phishing” beats a good day working.** Do your vendors regularly ask you to update sensitive account information using a secure e-mail link? Actually, this is probably just a scam called “phishing,” and it causes serious problems for individuals and businesses.
- **Laptops are incubators for computer viruses.** We all love the mobility of wireless computing, but every time you sign onto a WiFi network at your local coffee shop, hotel or anywhere else, you stand a good chance of picking up whatever bugs are floating around that network.
- **Don’t turn your back.** Laptops have a way of disappearing, left behind in rental cars and airplanes or simply stolen. An enterprising thief realizes your data is worth a lot more than the machine itself.

The report concludes that while no security system is foolproof, there are specific actions businesspeople can take to better protect themselves, their data and their organizations. The first, and perhaps the most important step, is to become fully aware of the grave threat posed by information theft.

For additional information or a free copy of the complete, 11-page report, contact Daniel H. Harris at [en-terpret.co](http://en-terpret.co): (773) 868-4381 or [dharris@en-terpret.com](mailto:dharris@en-terpret.com).

**About *en-terpret.co*** – Founded in 2000, [en-terpret.co](http://en-terpret.co) provides system consulting services for small to medium size business. It supplies strategic and tactical technology consulting services and designs and implements solutions for its clients. Specializing in knowledge management, it helps clients achieve business goals by creating the most effective technical applications to maximize intellectual capital.

