

**SPECIAL
POINTS OF
INTEREST:**

Car Hacking :
Researchers discover that just like PC's, cars can be hacked.

Internet Explorer 6 past its expiration date. Microsoft urges people to update.

The Laser turned 50 on May 16th

DNA robots. U.S. scientists develop microscopic robots composed of DNA

**INSIDE
THIS ISSUE:**

How to 2

How come I 3
keep getting
this virus?

Give away 4

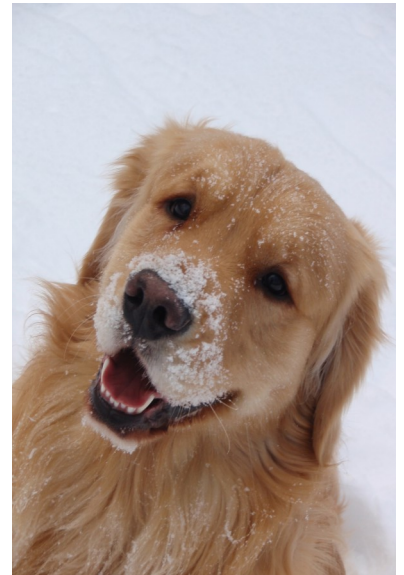
What's New ?

We would like to announce April and May's contest winners!

Last Month's winner was Ed Palmese from Cohen-Greve & Co. Congratulations Ed, your \$20 Dunkin Donuts gift card is on its way.

This Month's winner is Sam. Eileen Aliani's (also from Cohen Greve) grand-dog. Your \$30 gift certificate to Jeffers Pets is on its way.

The crew at Cohen Greve are very competitive, so don't delay when sending in your quiz answers.



**Sam is this month's
"Cutest Pet"
contest winner**



Welcome Aboard



We are excited to welcome our newest IT Freedom member :

D.R. Brown

I want to sincerely thank them for their trust and confidence!

4 tips for safely conducting research on the Web

Surprisingly, basic safety is often ignored by people using the Web to research information quickly and efficiently. If you use the Internet for research of any kind, you could be exposing yourself and your company to hidden dangers such as the unauthorized transfer of confidential information. And no one wants to be the person responsible for a companywide computer network shutdown.

1. Update, update, update!

Microsoft continually provides enhancements and security updates to all its products, including Internet Explorer. No program is completely safe from harm but as threats are discovered, Microsoft makes fixes, upgrades, and service packs for its products available. To maintain the highest level of security on your computer, you or your IT department must make sure to apply all service packs. (SSCS does this for you)

2. Get into the zone

By setting up Internet zones to meet your personal needs, your computer can help protect you as you surf the Web. A zone is a logical region or grouping of Web sites, based on where they are physically located and how well you trust the source. These default zones are available in Internet Explorer 8.

Local Intranet — Web sites located on your local network. These sites do not have to communicate over the Internet to be accessed.

Trusted Sites — A list of Web sites that you trust not to harm your computer, such as sites you have identified as properly encrypted.

Restricted Sites — A list of Web sites that are known or suspected to be harmful to your computer.

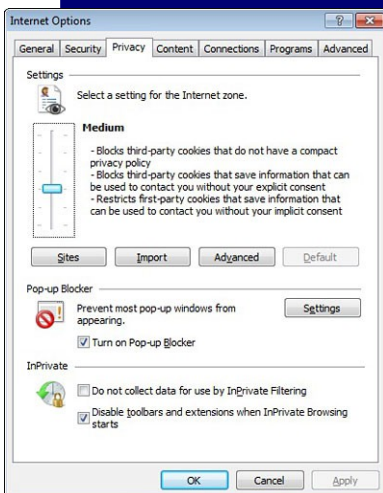
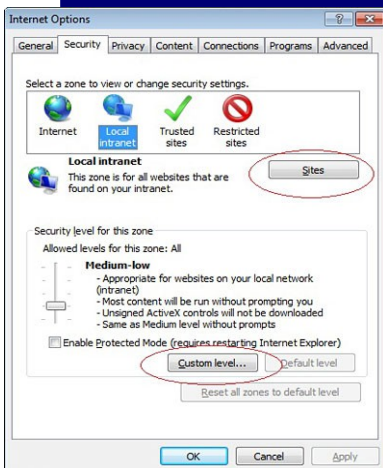
Internet — All other sites that don't fall under the other three categories.

3. Limit your intake of cookies

Cookies are small files stored on your computer that contain information needed on certain Web sites. A cookie can be used to store user ID, password, preferences, personalization, or other information that is helpful to enhance your experience on that site. For example, suppose you visit a Web site that allows you to select a preferred language. So you don't have to choose the language preference each time you enter the site, a text file on the site stores language preference directly on your computer as a file, or cookie. Cookies make it possible for unwanted information to be stored and accessed repeatedly when you visit a Web site.

4. Check for encryption before entering information on a site

While surfing the Internet is less dangerous than finding an abandoned bag in an airport, security should still be taken seriously. Encryption is a method that Web site owners use to help protect sensitive information, such as user names, passwords, addresses, phone numbers, and credit card numbers. If a Web site you visit does not use encryption, any sensitive information you place on it is easily accessible to hackers who want that information for unsavory purposes. Make sure that a Web site uses encryption when you are entering or viewing sensitive information.



Cyber crooks target web applications

Cyber crooks are increasingly targeting the growing array of Web applications -- everything from interactive maps to stock tickers -- potentially giving them access to the credit card and Social Security numbers of people using those sites.

Despite the increased security threat, experts say, some Silicon Valley companies and others that make the software enabling many of these online features aren't responding quickly to fix the flaws.

"It's a wild, wild world out there," said Mandeep Khera, chief marketing officer at Santa Clara-based Cenzic, which sells software to help ward off hackers. Despite a growing effort to beef up security on the Internet, he added, "consumers need to be aware of how vulnerable most of these websites are." Hoping to attract the public, businesses and others on the Web in recent years have added more and more applications. This includes multimedia players, document readers, auction features, reservation systems, video games, calendars, stock tickers, currency converters and e-commerce payment systems.

But to make those features work requires layers of sophisticated software. And keeping all that code free of the cracks that crooks can infiltrate isn't easy, according to Tom Cross, manager of IBM's X-Force Advanced Research unit, which monitors cyber threats, "The reality is that the more complicated this code gets, the more potential for vulnerabilities there is," he said. "We're also seeing an increased sophistication in the people committing these kinds of crimes." In March, Miami computer hacker Albert Gonzalez was sentenced to 25 years in prison for orchestrating one of the nation's largest credit- and debit-card thefts, which he and his cohorts carried out after identifying vulnerabilities in various businesses' websites.

In January, Google revealed that a series of cyber attacks originating from China had pilfered its intellectual property and targeted about 30 other Silicon Valley companies.

In July last year, Twitter acknowledged that a French hacker who broke into its site had accessed sensitive company documents and, reportedly, the accounts of President Barack Obama.

"Every 1.3 seconds a new Web page is getting infected," according to a recent report by Dasient, an Internet security firm in Palo Alto. "Users who interact on the Web "... are therefore at great risk." "It's pretty bad out there now," agreed Jeremiah Grossman, chief technology officer of Santa Clara-based WhiteHat Security, which helps website operators spot vulnerabilities. But given how fast applications are being added to the Internet, he predicted, "it's likely to get worse." **The danger is acute for consumers, experts add, because just visiting a site can leave them exposed to a cyber attack.**

Several security experts said such differences of opinion can happen because not everyone agrees on what constitutes a vulnerability. Moreover, they said, many website operators use their own customized software and often aren't aware of the weaknesses lurking in their applications.

Even when holes are identified, those responsible for sealing them may be reluctant to do so because of the cost. Some flaws can be patched for a few thousand dollars, experts said. But to design, test and widely disseminate a complicated fix for a major glitch, "you are talking in the millions of dollars," said Francis deSouza, a senior vice president at Symantec of Mountain View, which provides information security services.

Another problem, experts said, is that colleges and universities do not routinely teach software engineering students how to keep crooks from compromising their code. Plus, the wide variety of software used for Web applications makes it difficult to establish uniform protections for the public.



South Shore Computer Services Corp.

Deliver to :

South Shore Computer Services

6 Suffolk Rd
Island Park
NY 11558

Phone: 516-238-2724

Fax: 516-632-5233

E-mail:

sales@southshorecomputerservices.com

Southshorecomputerservices.com

We're Giving Away a Cruise!

Refer a Business to us.

**If they sign up for our IT Freedom Platinum Service,
you will receive a Carnival Cruise gift
certificate worth \$1000 !**

In order to qualify for the certificate:

They need to be a business owner with 5 or more pc's.

They need to sign up for a minimum of 6 months service.

We promise:

To be respectful of their time.

Not to harass them with sales calls if not interested.

Your referrals are not required to buy anything
if not interested.

Plus, we'll give them a free network audit valued at \$495.

**Call 516-238-2724 or e-mail
ed@southshorecomputerservices.com**

