

FOR IMMEDIATE RELEASE

Steve Lundin, slundin@bigfrontier.com
Jessica Secord, jsecord@bigfrontier.com
BIGfrontier for Halock Security Labs (312) 238-9308

Halock Security Labs warns companies to beware of the *fruit* cake: Holiday season is prime time for social engineers

More social activities, chaos, increased office visitors lead to business vulnerabilities

Chicago, IL, December 6, 2007: Halock Security Labs, an information security organization, warns all companies with a physical location and Internet presence to make sure security policies and procedures are strictly enforced during the holidays, because criminal social engineers are out shopping for others' confidential data. Offices are particularly vulnerable in times of increased social activity, like the holidays, because employees are accustomed to seeing new faces, new vendors, receiving many email solicitations and disclosing personal financial information online while shopping.

Halock specializes in ethical hacking and social engineering – at a client's request, to test a company's physical and Internet vulnerabilities. In one recent instance, a Halock employee was able to enter the corporate headquarters of one of the country's largest financial institutions and gain almost complete access to the company's sensitive data simply because he was carrying a cake. "When asked what he was doing, our man simply said, 'I have cake,' and nobody wants to impede the progress of a nice looking cake – right?!" observes Jeremy Simon, Halock's CTO.

"Social engineering is typically defined as the skillful exploitation of the natural human tendency to trust. This engineering can come through an actual physical interaction, through an email, as in phishing schemes or online, through falsified websites. The criminal social engineer is out to con someone into giving up credentials that can ultimately be used to generate or gain access to sensitive information," says Terry Kurzynski, CEO, Halock Security Labs. "And during the holidays companies are inundated with strange names and faces in the form of guests, delivery people, greeting cards, special offer websites -- the list is endless. Some of these guests are quite unwelcome," he adds.

What can a company do to make sure that they don't inadvertently let the Grinch spoil Christmas? Here are a few techniques that Halock Security Labs recommends:

- Stick to your policies and procedures; carefully track visitors coming and going into your facility. If you don't recognize someone or they are not displaying the

correct badge or ID, ask them their purpose and who they are working with. It will become clear if they belong within the walls of your organization.

- If your organization has a clean desk policy and/or a system lock policy for unattended systems, be sure to enforce those policies. Shred documents that contain confidential or sensitive data. This goes for home and work. Identity thieves pray off of the garbage can. Criminals that have socially engineered their way into an organization will be looking for low hanging fruit including paper documents or systems left unattended. They may try to quickly install a malware program on systems left unlocked and potentially gain administrative rights remotely to that machine.
- As for your on-line shopping this Holiday season, be sure to locate the little picture of a lock the on bottom of Web pages whenever you provide private information, including credit card numbers, name and address. Be especially careful of phishing attempts to get your password, social security number, account number, or credit card number based on an email that has arrived in your inbox. Never click on hyperlinks in emails unless the message comes from a trusted source (and even then, be careful!) And don't ever give out your password, credit card number or social security number via email.

“As an experienced social engineer, I've seen how easy it is to manipulate people and policies to gain access where it shouldn't be granted,” says Kurzynski. “Every organization and business is deficient in this particular area. We have countless accounts of our professionally-trained social engineers entering businesses or gaining access to data through phony websites or email scams. If I had one maxim of advice it would be this: develop a robust information security program for all private and sensitive data and make sure everyone sticks to it. Party punch or no party punch, someone's always got to be the designated driver when confidential data is at stake.”

#

About Halock Security Labs:

Halock Security Labs (*formerly Remington Associates*) is a professional services organization focused 100% on information security. Halock's core services include Assessments, Security Strategy, Network & Systems Security, and Web Application Security. We are in partnership with our clients to provide Purpose Driven Security to protect critical information assets as well as to meet compliance needs.

www.halock.com