

## **SPECIAL REPORT: Phonies, Phishing and Pharming for Real Dollars How to Protect Yourself and Your Business Online**

Welcome to the latest edition of the Inside Edge--your monthly report on Internet trends and advancements that can turn your business into a more profitable e-Business!

This month we take a look at Phonies, Phishing and Pharming for Real Dollars: How to Protect Yourself and Your Business Online.

Thanks for reading!



Consumer acceptance and use of the Internet as a legitimate shopping outlet continues to rise beyond the seasonal tides. The average e-Commerce transaction increased by 4%, from \$144 spent in the fourth quarter of 2004 to \$150 in the first quarter of 2005. The number of e-Commerce transactions also grew by 31% according to the latest Internet Security Intelligence Briefing published by VeriSign, once again proving that e-Commerce is enjoying healthy growth.

However, against this rising star of e-Commerce, a dark shadow is also growing. Internet fraud is spreading beyond vandalizing email viruses, irritating spyware and ubiquitous spam. Two new forms—Phishing and Pharming—have already proven themselves to be more dangerous and more costly for legitimate businesses to fight, but improved awareness and understanding of the threats is an important step towards increasing security.

### **The Scams: What They Are and How They Work**

Phishing is a sophisticated and malicious form of email spam that targets individuals with the goal of extracting private information to be used for identity theft. Alarming subject lines on emails posing as important notices from reputable companies warn of accounts being frozen, funds lost, or other fraudulent activity. People are enticed not only to open these emails, but to follow a link to a phony website branded to look like

the real thing. Once on the bogus site, victims are asked to enter sensitive account, password and credit card information which is then captured by the phishing scam artists.

---

## **'Having personal information stolen out of the mail or swiped by family and friends, was still far more common.'**

---

According to IBM's monthly security report, phishing attacks in May of 2005 increased by 226% over the previous month, beating the previous record set in January.

Pharming attacks, which are similar to phishing, are carried out behind the scenes, tricking a targeted company's own identification process to recognize the scammer as a "trusted site." Once that status has been granted, all traffic to the company's real website is hijacked to a phony site where, once again, visitors are encouraged to submit the financial information that allows the scammer to steal identities as well as cash.

Phishing and pharming are both designed to steal a person's identity, allowing thieves to commit not one, but many robberies from each attack. Identity thefts hit 9.3 million people in 2004 and cost businesses and financial institutions nearly \$53 billion, according to a survey by Javelin Strategy & Research.

The same report also noted that Internet-based identity theft accounted for only 11.6 percent of the total. Having personal information stolen out of the mail or swiped by family and friends, was still far more common.

### **The Bait: How to Spot a Potential Phishing Email**

- Doesn't address you by your full name.
- Asks you to provide personal or financial information, such as your bank or credit card account number, an account password or PIN, your Social Security number or mother's maiden name.
- Warns that you have been the victim of fraud or that your account will be closed unless you respond quickly.
- Tells you that you have won a prize or vacation and just need to "confirm" certain information.
- Has spelling or grammatical errors you wouldn't expect a professional business to make.
- Links to the "company's" website are number based, (e.g. <http://123.654.789.0>) instead of <http://www.realcompany.com>.

## The Solution: How to Protect Your Customers

While emerging technologies and secure Web hosting environments can help protect data from hackers and other Internet scam artists, consumer education programs are still the best defense companies have to help protect their customers from phishing attacks. Email campaigns, ongoing features in newsletters and information on company websites can be coupled with offline marketing activities to help people identify fraudulent emails. It's a simple matter of reminding customers of company policies regarding the collection of personal information and to call the company to verify any questionable correspondence.

These programs can also be used to encourage customers to upgrade their browsers to newer versions to take advantage of stronger built-in encryption, or to keep their anti-virus and anti-spyware programs up to date. Customers should also be warned of the risks of using public computers for financial transactions and even reminding them to always look for the lock icon in the bottom corner of their browser before transmitting personal information.

The lesson to be learned from these latest Internet scams is that there are risks to doing business online, but in reality they are no worse than the many other challenges businesses face on a daily basis. Experts agree that being informed about what's going on is the key to protecting your business and your customers, so keep an open dialog with your WSI Internet Consultant and take advantage of the many positive advantages an Internet Solution offers your business.



### ABOUT WSI

*WSI, headquartered in Toronto, Canada, is ranked the #1 Internet Services Business in the world. With systems that have been developed, utilized and proven by over 1000 Internet Consultants in 87 countries worldwide, WSI delivers thousands of e-Business solutions to small and medium-sized businesses annually.*