

Marshfield Mail  
Marshfield, MO  
Circ. 5800  
From Page:  
14  
3/12/2008  
14840



## Hackers now target Web site addresses

In today's digital age, a Web site is often one of the most valuable assets to any organization. A change to a Web site address would result in several inconveniences and, for many businesses, a devastating blow to branding efforts.

Most savvy Internet users are aware of spam e-mails and phishing scams targeting American consumers. Unfortunately, hackers have also begun to target the business sector, specifically with schemes that attack company Web site addresses, also known as domains. Many use programs to automatically look for and snatch up

recently expired domains. They can then capitalize on Web traffic and redirect visitors to another site, often pornographic in nature.

Nelson Hicks serves as Web administrator for Socket, a Missouri-based telephone and Internet company that provides Web hosting and domain registration services to its customers. He warns businesses could suffer devastating consequences by not exercising caution with their domains.

"Regaining control of an expired or hijacked domain can be extremely difficult and costly," Hicks said. "It is much simpler and less

expensive to take proactive steps to reduce the likelihood of domain expiration or

hijacking."

Hicks says that although Socket automatically renews domain registrations for its customers, many registrars require confirmation of renewal notices sent via mail or e-mail. This means if the notices are sent to an old address or inactive e-mail account, the domain could inadvertently expire. He therefore suggests keeping detailed records of all Web addresses and when they expire, as well as keeping contact information up-to-date with the domain registrar.

"For something as important as a Web site domain, it's really vital to keep good records and not depend on another individual or company to remind you to renew," said Hicks. "Some businesses even choose to register their domains for up to 10 years at a time to reduce the likelihood of an unintentional expiration."

Even if the domain is registered and the contact information is current, a business can still fall victim to domain hijacking scams. Hackers and disreputable registrars send e-mails or faxes that appear to come from a legitimate registrar seeking information required for renewal. Once the domain owner provides the information, the hacker can transfer ownership and take control. Legal battles are usually required

to restore the domain to its original owner.

Hicks suggests verifying all requests for domain information with the registrar, who can also place a lock on the account against unauthorized transfers. Businesses can also pay an extra fee to keep their e-mail address and other contact information hidden in public domain directories, reducing the likelihood of receiving hijacking e-mails and faxes.

As with most other Web and e-mail scams, preventing the loss or theft of a Web site domain comes down to common sense and attentiveness. Businesses that stay aware of the important details of their domains and are on the lookout for possible scams can usually avoid problems.

"By staying alert and cautious, business owners can protect themselves from most instances of domain theft or loss," Hicks said. "Then they can fully enjoy all the benefits their company Web site has to offer."

Do you have a technology-related question you'd like to see featured in Socket Tech Talk? Let us know by visiting [www.socket.net/techtalk-feedback](http://www.socket.net/techtalk-feedback) or by calling us at 1-800-762-5383.

Socket Tech Talk is provided as a service to distribute general information concerning technology-related topics. Please consult your local computer expert for information specific to your situation.