

Online auction fraud gains popularity; FBI, USPS get serious

It's a petty thief's dream world: Millions of people, all interested in those absolutely irresistible rarities on eBay or Yahoo! Auctions, bid fanatically online in hopes of obtaining objects for a fraction of their book values. All a person has to do is "list" something, wait a week, then snag the money and disappear.

Everyone seems to collect something nowadays, from Beanie Babies (yes, still) and baseball cards to Stickley furniture and oil paintings. And there's almost nothing that can't be purchased from one of the large online auctions. *The Wall Street Journal* earlier this year estimated that online auction spending increased from May 2000 to May 2001 by as much as 150% -- nearly \$600 million in May 2001. With that kind of money changing hands, the emergence of skullduggery is not surprising.

While most auction transactions are between individuals, many businesses are discovering the advantages of shopping the

See *Auction*, page 3

No, thanks, just browsing (through your company's files)

The Web isn't the small town where you can leave the door unlocked

Somewhere out there on the World Wide Web, someone has decided that it would be really fun to break into your company.

That person could be a current or former employee, a competitor, a disgruntled vendor, a master computer criminal, or even a pimple-faced 13-year-old at a middle school in Linton, Indiana, who calls himself "HackDaddy J."

In a matter of keystrokes, everything your company maintains in digital format -- financials, strategies, contracts, payroll, confidential health records, etc. -- could be accessed, stolen or edited by someone in the next office or on the other side of the planet.

By the way, this kind of thing happens on a daily basis, not just when you hear about it on the news.

But there's nothing to steal

Depending on several factors, you just might not be concerned at all about Web security. After all, if there is no e-commerce on your site, no transaction or client information, and no company secrets available, then your company can't really be compromised, right?

Well ... wrong.

The risks involved include more than just what a malicious party can *take* from your Web site, but what they can *add* to it, as well.

If your customers pull up your Web site one morning and find profanity or offensive pictures on the home page (or, perhaps worse yet, on a few pages deep in your site where the objectionable material isn't found for several days), this could do considerable damage to your company's image.

In a way, this could be a more attractive activity for novice hackers, who probably realize that stealing information carries stiffer penalties than mere vandalism.

Of course, you could explain in a press release (or to that pesky reporter) that this atrocity was perpetrated by hackers or by former employees, but the damage would still be done, and customers will begin to wonder what other electronic leaks might exist within your company.

It's a good thing to be a little paranoid about electronic security. And it's not just about the Web, either. If your internal data resides on a server that shares resources with a Web server, your internal data is at risk, too. Think of it this way: No matter how many "degrees of separation" there are between your internal data and your Web site, as long as there is some connection, your internal data is most likely accessible from the outside.

Ignorance is risk

The worst possible security solution is, of course, not implementing one at all. But implementing an inadequate or poor solution is almost as bad. With inadequate security, a company is more likely to *feel* secure, even though its security is full of holes. When a hacker visits a site that has security holes, he will realize first that this company doesn't really know what it's doing with regard to security. The hacker can then install his own "backdoors" to the site, so that even when the initial security

See *Security*, page 2

advertisement

So when *did* your company get into the Web business?

Focus. Keep your eye on the ball.
Do what you do best, delegate the rest.

You believe this. You teach this.

But then you decide to try building your Web site in-house.

That just doesn't make sense, does it?

You have a business to run.
Leave your Web site to DataGlyphics.

DataGlyphics 

www.datag.com

449 Central Avenue
St. Petersburg, FL 33701
727. 827. 3939

"...while technology has revolutionized the way we interact ... it has unfortunately increased opportunities for criminals." - Florida Governor Jeb Bush

holes are plugged, the hacker's own secret entrances still exist.

Seek professional help

If your company can justify hiring a six-figure electronic security professional, then good for you. If not, then you shouldn't rely on someone who "uses the Web a lot" to secure your network, any more than you'd rely on a filing clerk to handle your company's taxes because he is good at filing things.

Ideally, your company should outsource Web hosting and management, so that there is no connection between your internal network and your Web site. Furthermore, you should be comfortable with the company you deal with. Make them answer the following questions:

1. Does your company proactively monitor all of your hosted sites?
2. How do you deal with intrusion attempts when they happen? (And they do happen.)
3. How do you physically protect client data? What physical intrusion-prevention systems do you have in place? What kind of security protects your data storage?
4. Who has access to your servers? Who is responsible for making sure that all bug fixes and software patches are installed?

Make sure the company you're talking with has managed some serious corporate sites, too. Don't let your site be a training ground for your Web host.

Electronic security is a hairy subject for the layperson. There's much more to it than virus protection and data backup. Your best defense is to find a vendor who can effectively secure your network before, rather than after, a hacker attack.

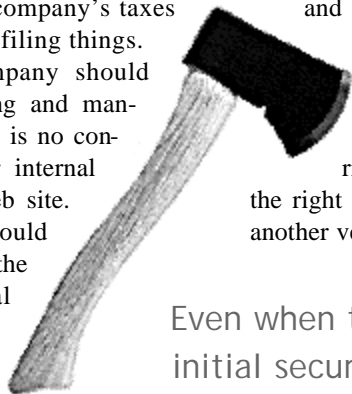
Is hiring a hosting company the best solution? Well, frankly, no. The most complete solution is hiring a competent Web developer to build your site, host it, and manage it. Security holes exist not only in the network, but also in poorly designed Web sites. A full-service Web company can build a site with security in mind from the start. And the right firm will never pass you off to another vendor if there's a problem.

Keep in mind that Web firms with the experience to implement adequate electronic security measures are rare. Yet every one of them you contact will likely declare their expertise in Web security. You should definitely look for one that has proven experience and solid policies and procedures. Ask them hard questions, and expect clear answers. Ask them to let you contact their current clients. If they balk at this request, you'd best keep looking.

Yes, you are questioning their reputation. And well you should. After all, it's your data that's at risk.

So what happens if the issue of Internet security at your company is left unaddressed? Maybe nothing.

Then again, don't be surprised by an unpleasant visit from HackDaddy J. ☞



Even when the initial security holes are plugged, the hacker's secret entrances still exist.

Why do hackers hack?

One might just as well ask why people scratch letters off bathroom hand dryers so that "Push Button" spells "Push Butt."

Here's a sampling of a few comments made by real-life hackers in anonymous newsgroups and other sources. Some comments have been edited, i.e., some words have been "bleeped" out.

Attempting to justify their actions, they explain their reasons for hacking. None of them sound convincing.

"Yeah, hackers have a bad name, they go out and do 'evil things' ... however, for them to do these things **there has to be a weakness to take advantage of in the first place** ... Think of hackers like a vaccine: get hit in small doses and grow immune to the bigger bug."

"**Most of us break into systems just to see if it can be done.** Few of us hack a system to cause it to function improperly. I can break into most personal computers with ease. **I can make most websites impossible to visit with the greatest of ease.** I can write a virus that has the potential to be mentioned on the television. Why does this scare you (the public)? Cause I have the ability to do it? Many people own firearms. A firearm can end a life in less than a second. Why don't people who own firearms scare you?"

"Some top managers [tell me] that they don't see any need to worry about network security because their servers don't handle important data. They don't seem to realize that **[hackers] use unprotected servers as launch pads for attacks on other servers**, thereby shifting the blame to others and avoiding detection. I personally know a company that was sued and paid a large amount of damages because **its server was used to attack other companies' servers.**" (former hacker Hideharu Ishikawa, in an interview with NikkeiNet)

"Whenever I found a new [security] hole, I'd say to myself, **'These guys can't get any stupider,'** until I found another new hole, and **I realized they could** ... We didn't do anything destructive, but just having the power to [destroy] was a rush."

"When [the hackers' target company] was small, they didn't need much security. But when they got bigger, they should have patched those security holes up. **They ignored it till me and some other guys started hacking it.**" ☞

30-SECOND WEB TIP: When it's time to part ways

One common security oversight that makes a company particularly vulnerable is that of a former employee's access to file servers and Web sites. When a staffer is laid off, whether or not the severance is cordial, any passwords by which that person has access to computers should be changed. It may be wise to change all passwords, in fact, as that person might have learned other staffers' usernames and passwords. If at all possible, deny an employee any access to your company's computers or Web site prior to terminating that employee.

Notifying your network administrator or Web development firm should be a high priority when a staff change is imminent.

Web to find bargains on office equipment and other company necessities. Significant savings on computers, software, and even paper and envelopes can be had through online auctions.

But one might well think of the Internet as the ultimate *Caveat Emptorium*.

According to *E-Commerce Times*, the Internet Fraud Complaint Center, jointly operated by the FBI and the Department of Justice, reported in late August that it has received 1,000 complaints per week since it launched in May, expecting that total to increase to 1,000 complaints each day once it fully automates and links up with major portals later this year. The average complaint amounts to \$800. And one of the most "popular" items paid for and never received? Computers.

You'd think these sellers would realize that online fraud is a federal crime. The

humorous side to all of it is that these people are often really easy to track down, as few of them, if any, know how to hide their identities. Even with online auction transactions, a paper trail usually exists, as well as a clear digital trail.

The only problem is that the volume of fraudulent transactions is so high, the authorities really can't handle them all. (It's been said that this makes a strong case for vigilantism, but you didn't hear that here.) So, naturally, the largest fraud cases push the smaller -- and more abundant -- cases to the back burner.

It's a real possibility that the federal authorities will use the online fraud prevention argument to make a case for

tighter governmental controls and more intrusive monitoring of the presently private Internet. The question is *not* whether the "protections" the government decides to put into place will prevent fraud, but whether their motives for monitoring the private citizen will be for the public's good or for their own ... okay, a little less *X-Files* from now on.

For most sales gone bad on eBay (specifically), there is some recourse in the form of insurance, subject to a \$25 deductible and a \$200 maximum, as well as copious amounts of paperwork. The best thing to do is avoid getting burned in an online auction transaction in the first place. Read "Countermeasures" below. Have fun, but stay suspicious. ☞



Countermeasures: How to avoid the online auction bandits

While there's no sure-fire way of guaranteeing that you won't ever get defrauded by an online auction seller, you can minimize your risk considerably by following these simple guidelines:

- 1. Check the seller's feedback.** And even this has its caveats. Look for feedback ratings for *sales*, not purchases. Also, check dollar amounts of sales. If the seller has excellent feedback from buyers with high feedback, make sure the items sold are in the same range as the item you're looking at. What's high feedback? Over 100 is good. Over 100 with no negatives is better. Sellers aren't very likely to risk a feedback rating in the hundreds on a single transaction.
- 2. Buy with a credit card, if possible.** Your credit card is your best friend on Web purchases, especially as it limits your liability. If you use services such as PayPal -- the seller should be a "verified" seller (i.e., the card processor has taken some steps towards verifying the seller's identity) or you aren't covered as well. You can, of course, always refuse the transaction through your card company.
- 3. View seller's other auctions.** You can discover a lot about a seller from that person's other auctions. Also view the seller's *completed* auctions. If he's sold 23 Rolex Daytonas in separate auctions over the last month, and each of the watches belonged to his late grandfather, and he just hates selling, but he needs the money ... well, you get the picture. Just be on the lookout for red flags.
- 4. Three cheers for international trade, but ...** keep in mind that the FBI's jurisdiction doesn't extend beyond U.S. soil, and if you send a traveler's check or international money order to someone in China or the Ukraine -- or
- even in Canada or Latin America -- you're pretty much at the mercy of the seller. That's not to say that international sellers are any less honest than domestic sellers, it's just that sellers in the U.S. can be "reached" by the FBI, the USPS and local law enforcement, if necessary.
- 5. Contact a few of the seller's customers.** Ask directly if they had any trouble with the items they bought. Disgruntled buyers are likely to tell you anything you should worry about. Happy buyers will let you know there were no problems. Just make sure that what they bought was of comparable value to what you're considering.
- 6. Use escrow on very large purchases.** Services such as TradEnable (formerly iEscrow) allow you to pay them as the middleman, then receive your item from the seller. If you're pleased, you can let the escrow service know, and they'll forward the payment (minus their fee) to the seller. Escrow fees vary. They seem high to some people, and a bargain to others. In most cases, the buyer pays escrow fees. The seller can choose to disallow escrow, so read the descriptions carefully.
If the seller states that he or she won't accept escrow, contact that person and ask what other arrangements can be made to guarantee that you receive what you pay for. If you don't get a reply, then maybe you should just keep shopping.
- 7. A little paranoia is a good thing.** Most fraud is "successful" because warning signs weren't heeded by buyers. The old adage, "If it looks too good to be true, it probably is," is something to keep in mind when you shop online. If *anything* about an item or a seller strikes you as fishy, then don't take the bait. ☞