# Grand Theft Internet

A true story of Internet attack and high-stakes cybercrime

J. Timothy King

Published by J. Timothy King.
http://www.JTimothyKing.com/

First electronic edition, April 2010.
Version 1.00

# Preface

This is a true cybercrime story, which hit my friend Tom—a little too close to home—on March 27, 2010. And I realized that this is something that could happen to *me*. Indeed, it could happen to any of us who owns his own business or website domain. Tom wanted this story told, in the hopes that the knowledge will help prevent similar crimes in the future, to encourage other victims also to come forward, and to increase the chances that crimes like this will be prosecuted as a result, and I agree.

I've drawn on chat transcripts, emails, and other forensic evidence, to reconstruct the timeline of events as accurately as I can. Naturally, when I portray the villain's activities—and especially his thoughts and motivations—I'm speculating... but let's call it "informed speculation." The villain, although he may sometimes appear incompetent, never acts out of random whim. His goal is not merely to poke around inside someone else's computer and see what he can find. No. He is pursuing a goal, so he has a purpose to everything he does. And I've written his character from this perspective.

I've mentioned DreamHost, our hosting company and domain registrar, by name, in the interests of full disclosure, because I have recommended DreamHost and have published affiliate links to their service, and I no doubt will in the future. Because in the aftermath, I'm still looking for another company who would have done better, who would have prevented the break-ins that occurred here.

# Chapter 1

I expected a typical lazy weekend: read a book, get ready for the Passover holiday, watch a few seasons of Mythbusters with my new Netflix Wii streaming disc. I never expected the weekend to bring me in so close to the world of high-stakes Internet crime.

As you may know, before I wrote books, I programmed software, and before that, I studied Electrical Engineering at Northeastern University. During those days, I met Tom, now one of my oldest friends. Both of us EE students, both electronics hobbyists since we were young, both hired as co-op students by the same local company. Both of us went into developing software. In the mid-1990's, Tom registered the Internet domain VL.com for his consulting business, Venture Logic. Shortly thereafter, I started JT Software Enterprises and registered JTSE.com. You can't get 2- and 3- and 4-letter domain names anymore. But at the time, the Internet was still an open frontier, and we actually homesteaded these domains, building them from the ground up.

Fast-forward to the year 2010. JTSE.com is still just an arbitrary string of characters to most people. But VL.com could stand for almost any company name, and on the open market, it's worth hundreds of thousands of dollars. (I wonder how much Barnes and Noble paid for BN.com.)

When Tom started getting genuine offers to buy his domain, we should have realized that it was like a diamond necklace, and that high-tech cat burglars would soon set their sites on it.

---

*Saturday, March 27, 9:17 PM EDT*

A dark figure lurked in the shadows, just outside the glow of the computer monitor. No one knew him. No one even knew he was there. He had been observing his prey, quietly collecting information using false names and stolen ID's, and even trial-and-error. Over the Internet, no one could tell he wasn't who or what he said he was. And by the time they put together all the pieces—if they ever put together the pieces—he would be long gone, with his quarry, having

taken on yet another false identity.

He knew the VL.com domain he wanted was registered with DreamHost; that was a matter of public record. And he knew that DreamHost would have limited resources to deal with a low-profile Internet break-in, especially on the weekend, and that could give him more time. He had also managed to crack into a different DreamHost account. He had asked them to add a credit card to the account, then talked to a different person and used the credit card information to validate that he owned the account. Customer service was always anxious to shortcut security in order to aid a helpless user, and he played the part like a pro. Through a long series of subterfuges, he had also discovered the account under which the domain was held, had even tricked DreamHost into linking it with his current persona. And now he was ready to strike at his true target.

“How may I assist you?” asked Dan, the support technician on the other end of the online chat.

“I having trouble with updating primary email address on my account,” the dark figure replied, impersonating his last victim. He then explained to Dan how he had tried to change the email address on the VL.com account. The story was a complete fabrication, of course; he didn’t even have access to that account. But he made sure he sneaked in the name of the account and the email address he wanted to use. He then complained that his computer was acting up, said he needed to reinstall Windows. It added an air of authentic helplessness.

Dan suggested he reset his browser, or try a different browser. A common support-guy fix.

He explained that he had already done that, and had tried Internet Explorer, Firefox, and Safari. It wasn’t important that Windows users almost never even knew about Safari; it was more important that he hit all the magic keywords, and fast, before Dan began to suspect anything.

Dan asked him to answer his security question. “What city were you born in?”

It took a minute for the dark figure to look up the correct answer, but he did find it, and answered correctly.

But Dan did not respond.

“Are you still there?” the dark figure asked.

“Changing, hold on,” Dan wrote. And finally, “Done.”

“I can see that it’s updated,” the dark figure wrote. Another fiction: he did not yet have access

to the account, so he could not actually see anything. But it was important for Dan to believe that he *could* see it, that everything was on the up and up. It was important that no one raise an alarm, not yet.

---

Neither Tom nor I use such weak security questions. Anyone can find out where you were born, or what school you went to, or your mother's maiden name, or whatever. This became painfully clear to me after I wrote my romantic memoir (*Love through the Eyes of an Idiot*). I looked to contact the people from my past that I wrote about, to inform them about the book. In the process of searching for them, I ran across all manner of personal information about them. I wasn't even looking for it.

How that security question got set at DreamHost is still a mystery, lost in the memories of time. Maybe it was an old security question, set when Tom first created his account. (Be assured that we've both verified and tightened up security on all our accounts, and no one will be pulling a similar stunt on either of us.)

Over the following hour, Tom would receive a dozen emails from DreamHost's computer, telling him someone was trying to reset his password. Each email included the standard calming notice:

> If you didn't request this email, don't fret, the security of your account has not been compromised. Somebody else must have requested your password. That's exactly why we email it to you instead of just giving it out!

If Tom had been looking at his email inbox just then, he might have been able to cut off the cracker before he did any real damage. Unfortunately Tom wasn't reading his email just then.

# Chapter 2

*Saturday, March 27, 10:23 PM EDT*

The dark figure waited for DreamHost support to respond to his chat request. He had requested the password be reset, eight times since 9:35, since he had tricked them into adding his email address to the account. But he hadn't been receiving the password-reset messages in his email.

Brian answered the chat. "Hi there, how can I help you."

Now impersonating Tom, the legitimate owner of the account, he explained his problem as best he could. "I'm trying to get login info in my new email address, but not receiving email from DreamHost." He gave Brian the account ID and email address.

"You're already logged into the panel, if you're talking to me," Brian said.

"Yes," the dark figure replied. That was true. He was logged into the administration panel, just not into Tom's account. Not yet. But hopefully soon. He told Brian that he had recently updated the email address, and that he needed to use the new address, not the old one.

Brian replied, "Both are actually listed on your account." He explained that Tom could use the administration panel to make any changes he needed.

Yes, the dark figure said, he'd tried that many times, but it wasn't working. He kept getting an error, he said in his typical broken English.

Brian asked him to try it again.

So he did. Of course, he didn't actually try anything. His story was a complete fiction, but a believable one. He described the steps he would have gone through, had he actually had access to Tom's administration panel. Every value he would type, every checkbox he would

check, every button he would click on.

“Page still pending load,” he added after another minute.

Brian waited patiently.

“Now get the page cannot to display error,” the dark figure wrote, but he knew that wouldn’t be enough. He knew he needed to make it sound like an insurmountable, unsolvable problem. “I also tried from Firefox, Safari, and cleared caches. I think it’s Windows issue with AJAX. Need to re-install windows tomorrow. Please check it.”

This must have puzzled Brian. Maybe he thought he was dealing with a clueless user. Maybe he thought it was a strange, inexplicable problem that would take too much time to track down. Maybe he just wanted to get “Tom” off his back. The exact reason didn’t matter. What mattered was that he took the bait.

“That’s weird,” Brian said. “I just tried it, and it worked perfectly. I changed it for you.”

The dark figure said he would refresh his display and see if it worked. Another fiction, of course. He couldn’t refresh any display, because he wasn’t looking at the display. But he could determine whether it worked. He asked for another password reset. He still didn’t receive the email message, but that might just mean the computer was still processing the. So he tried again, and again, and again, in quick succession. And finally it worked.

He reported to Brian that the data had been updated.

Brian was clearly pleased to have helped.

The dark figure had access to Tom’s account now, but there was one thing he needed to do before stealing control over the VL.com domain. He needed to cover his tracks, and for that, he needed Tom’s email passwords. He logged into Tom’s account and looked up the email box ID’s. Then he contacted support again.

Unfortunately, he got Brian again. Brian was no doubt tired with him by now, but he gave it a try anyhow. He said he was trying to see the passwords of two users under his account.

Brian replied that ”Tom” couldn’t see the passwords, but he could reset them.

Indeed, that was a security precaution that DreamHost had put in place some time ago, in order to stop people from doing what the dark figure was trying to do right now.

Brian suggested not making any more changes right now, just to keep everything working for now. Yup. He was clearly tired of dealing with “Tom.”

The email the dark figure was trying to erase was actually being sent to a Google Apps account, but maybe Tom had used the same password on both his DreamHost email accounts and on his Google account. The dark figure also had asked for the Google password to be reset, and he hoped that a password-reset message then might have appeared in one of the DreamHost mailboxes.

So the dark figure waited another half hour and tried again. This time, he got Sam, who was more than happy to help. He was able to get the passwords for the two email boxes, but they appeared to be long strings of random characters. And neither of those email boxes contained the Google reset message.

The dark figure would not be able to crack into Tom’s email. His best hope was that he could complete the thievery he came here to do, before Tom realized what was going on.

---

*Sunday, March 27, 1:16 AM EDT*

Tom instant-messaged me: “Somebody is trying to break into my Dreamhost account.”

“How can you tell?” I asked.

He had gotten a bunch of email messages telling him that his DreamHost account password had been reset. But it particularly disturbed him that the last of these messages was also sent to an anonymous email address, at HushMail, an email address Tom did not control.

What to do? DreamHost’s primary means of customer support was via the administration panel, if Tom could still login.

He couldn’t.

I acutely realized that this is one of the instances in which you really need another means of contacting DreamHost support. Since then, I’ve discovered DreamHost’s public contact form, as well as their abuse email address. Either would probably have worked at least as well as what we ended up doing.

We didn’t know how the attacker had cracked into Tom’s DreamHost account. Tom’s Google-hosted account had not been compromised, as far as we could tell. So the cracker had either found an exploit in DreamHost’s password-reset form, or else he was listening in on

DreamHost's or Google's network. In any case, it was a scary prospect.

As a fellow DreamHost customer, I contacted support on Tom's behalf and relayed his plea for help. It would be almost 13 hours before we received an initial response, and several more hours before we were taken seriously. Not fast enough to prevent the disaster that was to come.

# Chapter 3

Tom and I speculated on how the intruder broke into Tom's DreamHost account, and what damage he might be doing there. I thought he might trash Tom's account, and I was concerned that Tom be able to restore any lost data quickly. But Tom really didn't have any data in that account. All of his Internet services were served from elsewhere.

He thought the cracker was probably setting up a phishing site. That is, the guy would put up a fake web page that looked like a real company web page, maybe for a bank. Then he would send people to that fake page, maybe with fake spam emails, and then try to trick people into giving him their bank logins and passwords. Tom even feared the guy might charge up fake domain names on his credit card.

Fortunately, there was no way for the attacker to obtain Tom's credit card number, except for the last 4 digits. Nor could he charge up services or domain registrations on the card, because DreamHost's system always asks for new credit card information when you make new purchases. So that was good.

Our bigger concern was how he had managed to break in. The email box Tom had been using as a contact email for DreamHost, that account was still secure. Tom was also certain that his Linux desktop computer was secure, and he had found no breaches on his office LAN. He even had been using secure protocols he used to transfer email into the office LAN. That is, even if someone were able to listen in on his Internet connection, the cracker wouldn't be able to decode Tom's encrypted communications. The only alternative was that someone had cracked into a mail server at DreamHost, or maybe even the DreamHost control panel itself.

I joked that at least I would have something to blog about the following week.

I sent a message to DreamHost support, on Tom's behalf, marked urgent. I explained that his control panel account had been cracked into, and that he had been locked out of it, so he could not contact support thereby. I gave them his phone number and told them he wanted them to call him immediately. By then it was almost 2 o'clock Sunday morning.

“Sure, self-hosted stuff is more likely to be poorly maintained and easier to breach,” Tom commented to me, “but if a problem happens, I can always hit the big red button and halt it.”

And this was certainly one of those situations. You’ve just discovered that someone has cracked into your account and locked you out. You want to be ableto scream that your account has been compromised, and before anything else happens, you want your service provider to freeze the account. You can sort it all out later, when the experts can dig up the forensic details. But for now, you just want to stop the attacker from whatever damage he’s trying to do.

Still no response from DreamHost support. No way I knew of to escalate the request. No way to phone DreamHost. (And as we discovered later, DreamHost’s policy is not to discuss security breaches over the phone, only via email, because they want a written record of the conversation.) At one point, we also discovered DreamHost’s chat-support feature, and I tried contacting someone thereby, but no one responded to my chat request at 3:00 in the morning.

In the past, I’ve defended DreamHost’s control-panel-based support system, because it’s more than effective for normal, “my website’s not working” support requests. But this was not that kind of support request. We urgently needed DreamHost to freeze the account, at least temporarily, to keep the attacker from doing any more damage than he’d already done. Then the normal support mechanism would have been sufficient to pick up the pieces.

“I’m not sure it’d be worth the savings,” Tom noted, “to host anything critical at an organization that is effectively unreachable. I get that phone support would be abused, but you have to have a ’break glass when on fire’ option somewhere.”

At 3:01 AM Sunday morning, Tom realized that there was indeed some real damage the cracker could do. “vl.com is worth $100K+. So I need to escalate this somehow.”

We gave up on the non-responsive chat and on the support ticket shortly before 4 AM. We went to bed, long overdue for sleep.

---

*Sunday, March 28, 11:05 AM EDT*

“Hello. Welcome to DreamHost Live Chat. My name is Javier. How can I help you?”

“I’m sent transfer request from new domain registrar for my domain,” the dark figure posing as Tom typed into his computer. “Can you see transfer request on your admin end and verify if received request from other registrar? VL.com.”

He had already unlocked the VL.com domain, worth hundreds of thousands of dollars, and had

transferred it to a registrar in the Bahamas. He had done this before, with other domains. Once the domain was out of the US, it would be harder for Tom to get it back, and much more difficult for anyone to prosecute the dark figure or his friends for stealing the domain. International law is a bitch, and that worked to the dark figure's favor. At the very least, Tom would have to spend thousands of dollars to arbitrate the case, possibly with nothing to show for it. Some domains may be worth massive amounts of money, but they were not considered "property" by most governments. And that too worked in the dark figure's favor.

But while the Bahamas were ready to receive VL.com, the dark figure still needed to approve the transfer away from DreamHost, and DreamHost's interface didn't appear to be cooperating. Indeed, Javier confirmed that DreamHost had not received the transfer request. The dark figure would have to contact the registrar in the Bahamas and have them resend it. Too much time wasted now, but there still was probably time to steal the domain away. Hopefully, no one would know what was happening until Monday morning.

# Chapter 4

*Sunday, March 28, 2:40 PM EDT*

Glen, from DreamHost's abuse-response team, replied to our support request, saying that Tom should provide certain billing details, in order to verify that he owned the account. That's DreamHost's standard procedure. But we believed that someone might be listening in on DreamHost's email. How to convince Glen that this issue needs looking into? Tom emailed him back, explaining that he believed that DreamHost's email servers had been compromised, asking to talk via phone or to send the data via fax.

Tom said to me, "I'm sure they've chalked this up to some customer with sloppy security getting their email compromised."

Shortly thereafter, Glen confirmed that suspicion. He said that while he was open to evidence that DreamHost's network had been compromised, there hadn't been break-ins on any other accounts. He suggested that Tom scan his computer for viruses, to make sure there wasn't something installed on it that was listening in on his email.

Tom shot back, "It's a Linux machine with a secure password behind a firewall. I have a clue about security. The *only* place I am seeing any evidence of a breach is with DreamHost. The attacker attempted, and failed, to reset the password on my Google-hosted account. If he had compromised my machine here, he would have been able to intercept that email."

That seemed to have been persuasive, as Glen looked at the situation in more detail. Although he didn't find any record that Tom's account password had been accessed, he accepted that Tom knew enough about security in order to avoid the common mistakes that people usually make. He also restored the account's original email address, which gave Tom access again.

At around this time, Tom's Google-hosted account received an email that someone was trying to transfer VL.com away to another registrar. Unfortunately, Google thought it was spam. Tom wouldn't find the notice until another day had passed.

*Sunday, March 28, 6:09 PM EDT*

The dark figure had requested that VL.com be transferred away to a registrar in the Bahamas. But by the time the request had gone through, he had been locked out of the DreamHost account. If he could crack back in, however, maybe he could still complete the transfer.

Using a tried-and-true method, he chatted with DreamHost support. “Need update current email on file, but still not successful,” he said in his trademark broken English.

He was on the line with Schroder, who tried to walk him through the process.

But that would do the dark figure no good, because he couldn’t actually log into the account. His goal was to beg, trick, or badger Schroder into making the change for him. “Can you done it for me?” he asked.

“No,” Schroder replied, “I’m sorry. I can’t change it for you.”

“I can verify ownership,” the dark figure said. He gave Schroder the answer to the security question, which he had set earlier just for this contingency. He also recited the last four digits of the account’s credit card, which he had gotten from the account’s control panel and written down.

Schroder said, “If you can’t walk me through the method you’re using to change the info, then, I’m sorry, but I can’t help you with this.”

“Ok. Thanks,” the dark figure wrote, resolving to try back later with a different support rep.

*Sunday, March 28, 6:52 PM EDT*

While Tom waited for his browser to start up, he told me that he had two different contract programming jobs to work on this weekend, and he wanted to upgrade his operating system and switch his MythTV box over to a digital tuner. I guess he wasn’t going to make any progress on any of those projects.

“Look on the bright side,” I said. “Can’t think of what that is. But I’m sure there’s one there... somewhere.”

“Metaphorical bruises are often good to motivate you to take corrective action against

repeating the mistake," Tom replied.

He finally got back into his account, changed the account's login email address, locked out the attacker, and reset the passwords. He examined his domains. They were all still there. He couldn't tell whether VL.com was still locked, but all the domain-name configuration looked correct.

By then, it was at 7:08 PM.

Meanwhile...

---

*Sunday, March 28, 7:07 PM EDT*

The dark figure tried again with DreamHost's support chat. This time, he got Jeremy. He explained, impersonating Tom, that he was trying to change the primary address on Tom's account.

Within a few minutes, Jeremy had solved his problem.

The dark figure used the automated system to reset the password on Tom's account, knowing that as soon as he could get in, he would be able to complete the theft. But before he could lock Tom out, someone had already overridden the request. Clearly, Tom was onto him, logged into the system, and actively fighting with him for control of the account.

Time to switch tactics.

---

*Sunday, March 28, 7:19 PM EDT*

Tom was on the DreamHost support chat with Jason. "Help. My DH account is actively being hacked."

"Unfortunately," Jason said, "any inquiries pertaining to hacked sites or accounts need to be taken care of via email so our abuse/security team can assist you. This isn't something I can help you with via Live Chat."

"Glen reset my password about an hour ago," Tom explained, "and the attacker is repeating the attack."

"Okay, you will need to submit a support ticket for this. Thank you!"

Meanwhile...

---

*Sunday, March 28, 7:19 PM EDT*

The dark figure contacted Seohee via the DreamHost support chat, still impersonating Tom, told him he was having trouble transferring VL.com away, and asked for help.

He was worried that Tom may have already discovered the pending transfer and may have locked down the domain. “What’s current status of ’TRANSFER AWAY’?” he asked. “It’s canceled?”

No, it wasn’t canceled. It was still pending. The dark figure told Seohee a story about trying to approve the transfer but receiving an error. “Please approve it from your admin end. Restarting transfer request taking few days.” Sadly.

“Please hold,” Seohee said.

Within a couple minutes, the dark figure was able to write: “I can see it’s approved. And in new registrar.”

“Thanks for hanging in there. sorry for the confusion,” Seohee wrote.

“Thanks again. Have great day,” replied the dark figure.

“You too!”

Finally, everyone was happy.

# Chapter 5

*Sunday, March 28, 8:06 PM EDT*

“They stole vl.com!!!!!!!!!!!!!!!!!!!!!!!!”

By 7:45, Glen had discovered that the attacker had been manipulating the DreamHost support people in order to crack into Tom’s account and steal VL.com, a tactic called “social engineering.” Glen discovered this just minutes too late.

Glen immediately promised to gather forensic evidence in order to get back Tom’s domain, to insist on reforms of DreamHost’s policies and practices, and to pursue prosecution. He confirmed that there had been a security breach at DreamHost, and that the support people on chat were not supposed to be making changes on customers’ accounts. DreamHost serves as registrar for over a half-million domain names, and hosts close to a million websites, and the attacker could have gone after any of these— and still could. No doubt, the story, as he reconstructed it, stunned and panicked him and everyone else at DreamHost.

In most incidents of stolen domains, once the domain is transferred away, there’s little the rightful owner can do to get it back. File a police report: check. But aside from the blank stares, you’re likely to get little response. File a report with the FBI: check. But while the FBI is very interested in being informed, unless there’s substantial monetary loss, they can’t justify the resources needed to investigate and prosecute. Challenge the domain on trademark grounds, but that will cost thousands of dollars and take God-knows-how-long. You could even beg with the foreign registrar, but without conclusive evidence of fraud, they won’t undo the transfer. Most businesses who lose their domains to domain hijacking or domain theft, they simply give up.

The break in the case was perhaps Glen’s enthusiasm. Many companies would have clammed up in the face of these circumstances— Indeed, many have done so, whether to avoid being sued or just to avoid being bothered. And without DreamHost’s help, Tom’s situation would have been as bleak as the rain-soaked skies that week. If Tom had complained to the registrar

in the Bahamas, they probably would have dismissed him. But when an official DreamHost representative did so, they listened. They locked down the domain, which at least kept Tom's Internet services up and running. They considered the evidence that Glen had dug up, which clearly showed fraud. And they promised to return the domain, once the paperwork had been processed.

Interestingly enough, the cracker refused to give up. He opened a fake Gmail account, impersonating Tom, in an attempt to trick the registrar in the Bahamas into releasing the lock on the domain. And he hit DreamHost support again at about the same time, trying to get them to stop asking for the domain back. Then he attempted again to break in to Tom's Google-hosted domain, by trying to trick DreamHost into modifying the domain configuration— using the same MO: claim he tried to make the change himself, make up a story about encountering an error, and ask the support person to make the change for him. This would have allowed him to access all the email stored in all the accounts on that domain. But he probably only wanted to impersonate Tom, in order to call off the investigation. He may have made other attempts as well, attempts that we do not know of yet.

---

But the real question is how to proceed going forward.

This story is not about DreamHost. It's about the domain industry. Domain theft happens on the Internet, and social engineering is one of the thief's primary tactics. The most famous case is probably the theft of Sex.com, which is probably famous because of the letters S, E, and X. It took Gary Kremen years to get that domain back.

Moving my domains away from DreamHost doesn't necessarily solve the problem. Because a cracker can attack any registrar. If I have a diamond necklace worth $100,000, I can keep it in a bank safe-deposit vault. And short of a Mission-Impossible-style heist, I can feel pretty safe that it'll remain in my possession. If I have a domain name worth $100,000, there is no safe-deposit vault, and the quality of security at different registrars varies.

Additionally, the law is only beginning to see domain names as "property," even though, of all the things we call "intellectual property," domain names bear the closest similarity to real property. Until the law catches up to modern technology, we have to fend for ourselves.

As a defense, maybe there's some value in looking for a registrar who's as paranoid as I am. Maybe right now, that's still DreamHost, because they've been spooked. And maybe there's also some value in a registrar who will come clean when there's a break-in, and do their best to set things right. Maybe that, too, is DreamHost. But I find it disheartening that if I go into a crowded room full of IT gurus and ask, "Where can I register my domain to keep it safe?" the best I get is, "Well, I've been happy with such-and-such a registrar, but no one's ever tried to

rip me off before." No one cites any systematic studies of domain registrar security practices, and there's no single registrar that comes to the top as *the* name in domain security for the average business.

Even so, there's some value in looking for registrars that offer increased security and services, even at slightly increased prices and with longer waiting times:

- positively identifying the domain owner before releasing a domain to another registrar, such as with two-factor authentication being offered by some registrars;
- confirming domain transfers through phone calls or cellphone text messages, as well as the standard email;
- approving domain transfers through multiple, independent means, or multiple, independent accounts, all of which must approve before the transfer goes through;
- effective crisis procedures, when a break-in does occur;
- effective forensic and recovery procedures, when a theft occurs;
- insurability—if a domain name is stolen, the insurance company will pay for recovery or losses.

Notice I did not include domain locking in the above list, even though that's the first thing most people mention when they talk about protecting your domain. Why not? Because (1) it's a standard feature, (2) usually all the cracker has to do to turn it off is to click a button on some administrative panel, and (3) it can't protect you from lax security at your registrar or a break-in of your account. However, I might add confirmed domain locking to the list, that is, require approval through an independent email address or cellphone text message before anyone can unlock the domain.

Changes to approval email addresses also should use the same approval process. So for example, no changes should be made to my account email address without affirmative approval via that email address. The current standard system, which at best sends out a "email address has changed" message, that's inadequate for domain security, because a secure system is only as strong as its weakest link.

Even registrars of high-profile domains such as Amazon.com, BarnesAndNoble.com, and Coke.com don't offer services like these. And some high profile domains (such as Comcast.net) have indeed been hijacked. Fortunately, if you're Amazon or Coke, you can probably get your domain back pretty quickly with a simple phone call. But if you're not, you need a registrar that's going to stand up for you, no matter how small you are. And you can expect it to take days at best, or weeks, or months, or years, or forever.

There are some additional safety measures you can take to slow up a thief trying to steal your domain:

- Use a secret email address for your account email.

- Always use a secure computer and encrypted connection to download email.
- Use long, random passwords for each email and domain account.
- Use secure secrets for any “secret question,” obscure facts that no one else can find out.
- If you have multiple domain names or web holdings, split them up between multiple registrars and hosting services.
- Use low-value domains for daily activities, if possible. (So if someone steals away VL.com, your email will still continue uninterrupted through VentureLogic.com.)
- Know how to get in touch with your registrar in an emergency, whether by phone, email, or web form, even if you’ve been locked out of your account by an attacker.
- Establish secure, authenticated communication channels with people you are likely to work with to resolve a crisis: obtain email certificates, exchange public keys, and set up secure IM.
- At least ask yourself, “Will that busty model come to my rescue when I have a problem with my domain?”

Unfortunately, as long as an attacker can trick the registrar to bypass security, neither strong passwords nor two-factor authentication nor double confirmation nor any other security measure will be effective.

Conceptually, you could test a domain registrar. Try to convince them to shortcut security for you, in order to make legitimate changes to your account. And if they do, bolt. I can’t comment on whether that’s legal or not. But as for me, I’d be interested in a broad-based study of how tight security really is at the Internet’s top domain registrars.

Additional resources:

Interview with Bjørn K. Andersen, who had Direction.com stolen:
http://www.vtalkradio.com/bjorn.asp

The story of the theft of P2P.com, and the first ever criminal prosecution of a domain thief:
http://www.domainnamenews.com/featured/criminal-prosecution-domain-theft-underway/5675

2005 ICANN SSAC report on domain hijacking:
http://www.icann.org/en/announcements/hijacking-report-12jul05.pdf

DynDNS on domain hijacking:
http://www.dyndns.com/support/kb/domain_hijacking.html

Moniker.com, a registrar that advertises a higher than average level of domain security:
http://www.moniker.com/

Other mentions of the theft of VL.com:

Report of the theft, on Domain News Wire:
http://domainnamewire.com/2010/04/03/vl-com-domain-name-stolen-too-heres-the-inside-story/

Boston Linux & Unix users' group discussion, as the story unfolded:
http://old.nabble.com/Dreamhost-account-hacked-td28062149s24859.html

Boston PerlMonger's discussion:
http://www.mail-archive.com/boston-pm@mail.pm.org/msg05971.html

Hacker News discussion:
http://news.ycombinator.com/item?id=1229247

If you liked this story,
you may enjoy some of the other work
of J. Timothy King.
http://www.JTimothyKing.com/