

GROW YOUR ONLINE BUSINESS
20% IN 20 DAYS

GUARANTEED

**What You Should Know About
Internet Security
Before It's Too Late**

Dear Student,

I'm Michael Senoff, founder and CEO of HardToFindSeminars.com.

For the last five years, I've interviewed the world's best business and marketing minds.

And along the way, I've created a successful home-based publishing business all from my two-car garage.

When my first child was born, he was very sick, and it was then that I knew I had to have a business that I could operate from home.

Now, my challenge is to build the world's largest free resource for online, downloadable audio business interviews.

I knew that I needed a site that contained strategies, solutions, and inside information to help you operate more efficiently

I've learned a lot in the last five years, and today I'm going to show you the skills that you need to survive.

It is my mission, to assist those that are very busy with their careers

And to really make my site different from every other audio content site on the web, I have decided to give you access to this information in a downloadable format.

Now, let's get going.

Michael Senoff

Michael Senoff

Founder & CEO: www.hardtfindseminars.com

Copyright Notices

Copyright © MMVII - © MMVIII by JS&M Sales & Marketing Inc

No part of this publication may be reproduced or transmitted in any form or by any means, mechanical or electronic, including photocopying and recording, or by any information storage and retrieval system, without permission in writing from the Publisher. Requests for permission or further information should be addressed to the Publishers.

Published by:

Michael Senoff
JS&M Sales & Marketing Inc.
4735 Claremont Sq. #361
San Diego, CA 92117
858-274-7851 Office
858-274-2579 Fax
Michael@michaelsenoff.com
<http://www.hardtfindseminars.com>

Legal Notices: While all attempts have been made to verify information provided in this publication, neither the Author nor the Publisher assumes any responsibility for errors, omissions, or contrary interpretation of the subject matter herein.

This publication is not intended for use as a source of legal or accounting advice. The Publisher wants to stress that the information contained herein may be subject to varying state and/or local laws or regulations. All users are advised to retain competent counsel to determine what state and/or local laws or regulations may apply to the user's particular situation or application of this information.

The purchaser or reader of this publication assumes complete and total responsibility for the use of these materials and information. The Author and Publisher assume no responsibility or liability whatsoever on the behalf of any purchaser or reader of these materials, or the application or non-application of the information contained herein. We do not guarantee any results you may or may not experience as a result of following the recommendations or suggestions contained herein. You must test everything for yourself.

Any perceived slights of specific people or organizations is unintentional.

What You Should Know About Internet Security Before It's Too Late

I was recently a victim of Internet identity theft. The perpetrator found a weakness in my URL and attacked my website. Within 24 hours, my URL was reported by several people to be a "phishing" website. That means the perpetrator was essentially able to take over my site and use it to try to steal people's personal information.

Even after I cleaned up the problem, it was still a hassle. I had to file reports with Microsoft, eBay, the government and even the Internet Crimes Division of my local police department to let them all know I was a victim of fraud.

So in this audio, you'll hear how you can avoid common Internet security problems, like the one I just described, to make your site as secure as possible. And you'll hear it straight from the guy who got me out of that mess. Internet security expert Nick Gilbert is the owner of a popular web hosting company and is also the developer of the Guerilla Internet Marketing Course.

Important Security Issues Discussed In This Audio

- How to make sure you're not opening the door for hackers with third party scripts on your site
- How to make your HTML codes and directories safe and untouchable
- Ways to keep hackers from seeing your usernames and passwords – believe it or not, your passwords are probably vulnerable right now
- What you'll want to do before you get rid of your old computer to prevent "deleted" personal information from being retrieved by hackers
- How to make sure your "secure" wireless router really is secure
- What a "man in the middle" attack is and how to avoid one
- Ways to research a web hosting company to find out if they're really making security their highest priority

When it comes to the Internet, most people don't want to bother with dry, technical security stuff and would rather just believe they're

“probably safe enough.” But according to Nick, only about 25% of at-home users really are safe enough from hackers while on the net.

So listen to this audio, see where you stand on these security issues. Some of them are easy to fix while others might open your eyes to some potentially devastating problems. And if you decide to order Nick’s Internet Course through my site, you’ll also get a 30-minute consultation with Nick. So you can personally ask him as many specific Internet questions as you can think of. And believe me, he’s just the guy to answer them. Enjoy.

Hi, it’s Michael Senoff with Michael Senoff’s [HardToFindSeminars.com](http://www.HardToFindSeminars.com). In the next forty minutes, you’re going to hear myself and Nick field questions from my students at [HardToFindSeminars.com](http://www.HardToFindSeminars.com) about internet marketing and we’re also going to cover the security mistakes you’re making with your website and how to avoid them. This interview is packed with information, so let’s get going.

Michael: All right, I’m here with Nick Gilbert the developer of the Guerilla Internet Marketing course. So, Nick, are you with us?

Nick: Yes, Michael, just a warning, we’re talking about some real sensitive data here. If the wrong people got a hold of some of these software tools or the URLs, they could really devastate a lot of sites on the internet. So, for security reasons, we’re going to block out those URLs and names of the software except for the people who are members of the Internet Guerilla Marketing course.

Michael: I asked you to put together common security mistakes that people are making with their websites and how to avoid them. I want to interject just a little story that made me rethink the value that I have for you by you hosting all my websites, and this story kind of goes like this.

This was last Thursday, I received a call from a lady in San Diego and she told me that she had gotten an email that had asked for her eBay user name and password. The funny thing was she didn’t have an eBay account. Now, I knew exactly what was going on right away. That was what we call a phishing email or a spoof email.

It’s when criminals will hack into a website or find a weakness in a website or a server, and upload pages into a website folder and

proceed to send out either bulk email or targeted traffic to people on the internet to try and phish, to try and get people to fall for this spoof email by clicking on a link and entering a user name and password, therefore, they could break into that person's eBay account or their PayPal account or their bank account and they could steal information or steal money or buy things using the person's credit card information and all of the above.

It's a serious crime, and this happened to me last Thursday. Someone was able to find a weakness in one of my URLs, one of my websites, and the real value in having you host my site is that I had your cell phone. I knew exactly what was happening. I called you immediately, and you were able to identify what was going on.

I got on the phone with my webmaster, and we were able to disable and secure the page within probably about thirty minutes. Then, after we took that page down, the perpetrator instantly put a new page in a new folder, and this happened two times. Between you and my webmaster, we were able to at least 99% sure identify where the weaknesses were and close all these wholes, these security measures.

So, I want to tell any of the listeners out there, if you own websites, it could happen to you, and this was a pretty eye opening experience. Because of this, I'll tell you exactly what happened.

Within about 24 hours, the URL website that was broken into was reported from several people that my URL was being used as a phishing website and it was reported as a phishing website through Microsoft. I had to go to Microsoft and I had to fill out forms. I had to fill out a form with the government. I had to call my local police and then they recommended I call their internet crimes division.

I had to file a report there. I had to file a report with eBay. I had to file a report with the government internet fraud division to cover my butt, to let them know that I was a victim of basically identity fraud.

It's real painful and eye awakening, but I'll tell you. I want to thank you, Nick, for taking care of this and that's the real value in having you handle all my websites. I can assure you if I had my sites listed with one of the big, huge website hosting companies like Go Daddy, this situation could've gone on for weeks, if not months. So, thank you for doing that.

So, Nick, with your hosting company, how often are you seeing situations like with what happened with me, with the spoofing emails?

Nick: With spoofing phishing scam, I get about ten of those per month and about fifty people with other exploits a month, either people who have scripts that are spamming or doing other things.

Michael: So, do these people call you up frantic?

Nick: Yes, they call me up asking what's going on and stuff, and then I'll do an audit of all their scripts for them and tell them how the hackers are getting in.

Michael: With your proprietary software, you're able to identify exactly what's going on within seconds.

Nick: Right, I'm able to figure it out pretty fast.

Michael: Are other webhosting companies available to react that quickly?

Nick: It's mostly done based on experience. There's a few commands I use, but there's not really software to do it automatically. So, you really do need a lot of experience there.

Michael: Tell me two of the other situations you get calls for.

Nick: A lot of times, the hacker has replaced the home page, but sometimes it will be like hacked by so and so, and they'll replace that for all your index pages so it will look really bad for business. The next problem is spamming. Someone will get into your account and then run the script there that will spam all their people.

Michael: Have you ever been contacted by law enforcement or government officials for any of these situations?

Nick: Yep, I've been contacted by a police department and also the FBI.

Michael: Are they able to deal with that efficiently, or do they just back off this stuff?

Nick: Unless there's like a great deal of money lost, there's not really too much that can be done, and a lot of times these people are overseas, too, so the US is limited on what they can do.

What I've done for you Michael is put together the top ten security mistakes people are making and how to avoid them, and your listeners are going to be able to hear those at the end of this interview.

Michael: Let's say, Nick, that I was with one of these larger companies and I was reported to Go Daddy, what could've happened to my internet website based on your experience?

Nick: A lot of the larger companies have a shut down first, ask questions later policy which means if they see a phishing scam or spam or any kind of illegal activity or anything against their terms of use coming from your account, they're going to turn your site off. A lot of times, it's really hard to get back on.

The big companies don't want to deal with it. If you call them up, they'll say there's no one in that department you could talk to. You have to send an email to them. They may or may not respond, and if you're lucky they may turn the site back on for you. Often, there's an extra charge for it, or they may even delete every file you have on there. That's the easiest way for them to secure the issue is gone, and then you lose all your data and stuff. If you didn't have a copy of it, some of it will be lost.

Michael: A lot of these securities mistakes may be over the head of a lot of new internet marketers, and it may sound a little daunting, but I know in your consulting practice that you cover and help alleviate any of these problems.

Let's go through the list for anyone who is interested in this. What's the first common mistake, and how can we avoid it?

Nick: The first one is if you use a third part script like if you have a shopping cart or content management system or a blog on your site, you want to check for updates for it at least once a month. The third party scripts are great and they'll save you a lot of time and money, but since the actual source code of that script is available to everyone, hackers and security experts will spend time studying that code, and looking for ways to get in. This is called an exploit.

Once the developers of that script learn of the exploit, they'll make changes to their script and release a new version on their website, but it's up to you to check for that and download it and install onto your website and run the script to update it. Out of date scripts with the known exploit can lead to spammer getting into your account or a

hacker getting in and uploading his own content or doing a phishing scam.

Michael: Okay, so when people how have all this software on their computer, like myself and when you restart your computer, you'll see there is a new update version 6.7, and you have 5.7, and like me, a lot of people just remind me in a week, remind me in a month. It's really important to keep updated with all these updated because they're closing up all these exploits, and it'll keep their software, your computer and your website more secure.

Nick: Right, and once an exploit has been publicly released, the hacker know about it, and they just go to Google and look for sites that are running that software, and then they go to hit those sites.

What your listeners have to understand is there's a lot of small hosting companies out there where someone just has one server with some pre-written management software, and they don't really understand how this stuff works or how to do security updates or anything.

With my webhosting, I've been in the business so long and have so many different servers, that I know what all these updates are and how to apply them and make sure everything is secured.

Michael: What's another mistake you see people making?

Nick: Another one is you need to use appropriate permissions for directories and for your scripts. In Unix this is called 755 permission, that's used for directories, and 644 permissions for scripts. This means that it's read access for all, and write access for the owners only.

A common mistake is to make a directory 777 permission which stands for world writable or other writable meaning that anyone with access to any account on that server can put files into your directory.

As you know, Michael, this is exactly what happened to you. A hacker gained access to one of the accounts on the server, and then was able to put back doors in these directories that have the 777 permissions.

Michael: What's another mistake, Nick?

Nick: You want to be very careful in including a variable in PHP. This is if you do your own coding or have someone that codes for you. What

this means is using the PHP include function and using a variable for the page you want to include in the URL.

This is one of the most common exploits that I come across. It allows the hacker to place their own code in your page, and your page will actually execute that code.

Michael: Can you explain that in more simplified terms for less experienced people?

Nick: Sure, in layman's terms that's for example, let's say they went to YourDomain.com/and after that you would see a question mark and then page equals, and then you would put main in there. The hacker would replace that main with the URL of it's own site. Instead of your page including main, which includes your main content, it's going to instead include the hacker's content.

For more exclusive interviews on business, marketing, advertising and copywriting, go to Michael Senoff's [HardToFindSeminars.com](http://www.HardToFindSeminars.com).

Michael: What's another mistake?

Nick: What you want to do is every so often do a once over of all your directories and files. That way you make sure that there's no unusual files or folders that you didn't put there.

A lot of times, a hacker will gain access to several accounts in a few days, and then store back door scripts on them. Then they're available for whenever he wants them. So, one of his accounts that he had hacked got shut down or the user fixed the issue, he has another one to go to, so he has a lot available.

Michael: So, when you say go check all your directories, for anyone who has never seen like the internal guts of a website, it's exactly what it looks like on your hard drive when you're looking at your folders and all your files. That's exactly what it looks for your website.

Your website contains folders and inside the folders or pages, and there may be a folder for images. It's just like you checking what's on your desktop, but you're checking it remotely on your server. These are the things that operate, host and display your webpages and your website.

So, if you've never been into the guts of your server and your website and you're working with a webmaster, you need to either instruct your

webmaster to do this for you, to look through the folders and look at all the pages. You can sort them by date, so you can get an idea if there's been anything uploaded recently that you may have not instructed to do that.

It's simple to check them, just as if you're checking your folders in your files on your hard drive. You can do the same for your website. Does that sound accurate?

Nick: Yeah, that's pretty accurate, and then you do come across files of directories that you don't recognize, if you email your host, they'll be able to tell if it's an exploit or a file that a hacker might have put there.

If you order the course through Michael, you can email your files in your directory that you're not sure of, and I'll be able to take a look at those and tell you if they're okay or not okay.

Michael: Okay, what's another mistake, Nick?

Nick: Another one you want to make sure you use secure passwords for your email accounts. Just as a hacker can get into your FTP to upload files to your website, if they get into your email account, they might start spamming from it. It could be hard to get your host to put you back up especially if you're with one of the bigger hosts.

Michael: I have to reiterate. In the past, this has happened to me as well. Nick, you can remember me calling you saying, "Hey, Nick, go check my server. It looks like someone is spamming through my URL." Do you remember that? I think that's happened a couple of times. Okay, what's another mistake?

Nick: Another one, you don't want to really provoke anyone. Common things that hackers can do is launch a detox attack against your site, and if it's a large enough attack, they're very expensive to block. I've had a few customers who have agitated competitors or rival gaming sites, and the party agitated actually launched a detox attack against their site which affected the server, and everything.

What this does it if they use all their bandwidth or it will overload the server with too many connections so their website won't load.

Michael: Is this easy to do? What are they actually doing?

Nick: They use a program that's keep calling URLs or one of your large images, or that keeps requesting your page so that no one else can get to it.

Michael: What's another mistake?

Nick: Another one, make sure your host provides updates for all the system packages. If you have a dedicated server, hosts often won't provide these updates unless requested. This includes the current version, THP Pro, and any other packages which may have been updated to fix security issues.

Michael: You have one more big mistake that website owners are making.

Nick: Yep, another thing that you want to do is subscribe to Bug Check and you can do that at SecurityFocus.com. This is a mailing list that informs you of security issues with common third party scripts and also server level packages.

So, if you're running a shopping cart, and you get a notice from Bug Check saying there's an exploit out for that shopping cart, you want to make sure you get the updated version of that so your site could be secure.

Michael: Anyone who is listening to this who has a hosting company and they'd like to run these ideas by them to make sure that they're covered in all these security areas, please, you can email them the transcripts of this recording or send them directly to this page.

Nick, can we reiterate the offer and let the listeners know how they can try your Guerilla Internet Marketing course one more time?

Nick: Sure, the special offer, Michael, for your members is \$97 for the digital version. That's regularly \$597, and to get the \$97 price, they have to use the link from YourMarketingMastermind.com, and that'll take them to the page with that special deal. It does come with a sixty day money back guarantee.

Also, with that, you'll be able to email me if you have any security issues with your site or see any files you're unsure of. You also have my private line number, so you can call me if you ever have an emergency and need help right away.

Michael: That's the end of my question and answer interview with Nick and the ten biggest security mistakes you're making with your website and how

to avoid them. Remember, you get Nick's personal cell phone number when you order the course through YourMarketingMastermind.com.

You'll have Nick's personal cell phone number to handle and field any common problems related to phishing scams or any other internet related emergencies with your website, and you will also be able to email Nick any suspect pages or files that you find on your website host server. I urge you to take advantage of this offer.

Nick, let me ask you this. Everyone has heard the name hacker. Do you know where the term hacker came from and what is a hacker for people who don't know?

Nick: Technically, it was originated by just someone who likes to use the computer and does attacks on the keyboard, but over the years it's become known as someone who uses it to break into other people's computers.

Michael: Can we talk and educate the listeners a little bit about how dangerous a hacker can be? In the recording we just did previously, we talked about how a hacker was able to find a weakness into one of my websites, and to set up a phishing scam.

It got me to thinking, and I think it's really important to understand the power a hacker has in reeking havoc on one's website, their online business and on their server. So, can we educate the listeners a little bit about how a hacker can break into one's site and do some serious damage? What's another example of how they can do that?

Nick: One way is if they use a password cracking tool.

Michael: What is a password cracking tool do? What is that?

Nick: That'll run constantly and keep trying a huge list of different user name and passwords, and if it finds a match it displays it to the hacker's screen. They'll know right away what your user name and password is if their system found a match on that.

Michael: So, what they're doing is they're trying to find a site or a server, a bank account or something they want to get into, and they point the software to that area on the site, and try to crack it.

Nick: Right, it points their software to try to keep logging in or log in on a webpage somewhere or to like FTP or control panel or something. The

way it works is it goes through a word list. They can have over a million different words, and they're in many different languages.

They also have names, common pet names, and it'll do numbers added before and after words. So, doing your name and then 99, they'll still be able to guess that adding numbers is not enough to prevent them.

They also do things like replacing an I with a one or a zero with an O, and so on.

Michael: Why is this kind of software even out there available on the internet?

Nick: You could get a publicly available places like dot-org, and they are available just because system administrators use them to penetrate their own servers or if they have a server that they're locked out of and they forgot their password to it. They might want to use one of these tools to be able to get back in.

Michael: Have you been able to use it to test the security of your servers?

Nick: I have, yes.

Michael: Is that a standard practice that a lot of website hosting server operators will do to these their own security, or most people don't even mess with it?

Nick: Most people probably don't mess with it. The good people do though.

Michael: How do you keep hackers from breaking into your servers?

Nick: The way I block it is on all of my servers, I have a special detector that logs on the server and if it sees more than ten invalid log in attempts, it'll block the IP address to the hacker which is going to stop his program from trying more passwords.

Michael: How recent is this detector? Is this something that's been out for a long time or commonly known by other internet security experts?

Nick: I found out about it a couple of years ago. There's still a lot of companies out there that aren't using it, though.

Michael: What's another way hackers are able to break into people's information?

Nick: They could use a network sweep such as – and this is available at dot-net. This does a lot of things. The main thing it does is capture all network traffic. If it sees a user name and password going through in plain text, it will display it to a separate window.

I was actually really surprised when I tested this on my own network. I saw a lot of user names and passwords coming through pretty often, and they were email user names and passwords. This is because a lot of email clients are set to check their email every ten minutes, and a lot of people don't use secure connections for checking their email.

So, each time the computer would go to check the mail, it would send the user name and password across the network in plain text.

Michael: So, for instance, I want to give you this example. Let's say I'm pulling off all my email off of MichaelSenoff.com through my Outlook, and I have my Outlook designed to set and check my email every ten minutes, and my password and user name to get into the server is the same to get into the server.

Are you saying someone could set up this network sniffer and capture that user name and password trying to log in to get my emails?

Nick: Yes, in order to do that, though, they'd have to have access to your network.

Michael: So, if I don't have a network, I've just got a individual computer, I don't have to worry about it.

Nick: You still have to worry about it because you're going through other networks that goes from your computer through a bunch of different switches and routers that your ISP, and then on to our server and then back to you. So, it could be anywhere in between.

Like, if my ISP had a bad employee or they had a computer server router that was attacked by a hacker, that hacker would be able to get your data.

Michael: Do you have an idea of a better way for me to pull my email down off of the server that would be more secure?

Nick: Yes, you could use secure ports for sending and receiving email, and then you also want to make sure your website uses the HTTPS secure URLs on pages that have or receive sensitive data.

A common mistake some people make is using HTTPS for the form page, but then they have their form action task going to not necessarily URL, and that actually sends the data in plain site. You need to make sure that both are HTTPs URLs.

Michael: I'm just thinking on my secure order forms where people fill in all their information, it's a secure page, but then that information goes into a database that my webmaster set up.

Nick: Right, so you'd have to make sure that anytime you access that database and stuff you're doing it over the secure URL.

Michael: The HTTPS. All right, I'll double check on that. Now, in my Outlook settings for my email, when I set up my email accounts, there is a button that says to have it secure. There's an option in there I guess to check my email when it's secure.

Nick: Right, in Outlook, if you go into the properties for email accounts and then go to the advanced tasks, it'll have a check box for this server requires a secure connection SSL, and if you check that, that's going to change the port that uses to 995, which is a secure port for incoming email and then for outgoing, if you check that, the outgoing SSL port for us is 465.

Michael: Okay, so look, I'm in my email accounts. I'm looking at my email account. It says log on using secure password authentication SPA.

Nick: That one is a little bit different. You want to look for where it has the port numbers for your email. It might be under more settings or advanced.

Michael: What would I look for in my Outlook?

Nick: Right.

Michael: Do you know what it would be under?

Nick: In advanced tasks.

Michael: Advanced? Let's see I've got email, view, tools.

Nick: View.

Michael: View, navigate, auto preview, windows toolbar, status bar.

For more information on how to grow your internet business 20% in 20 days go to <http://www.yourmarketingmastermind.com>

Nick: That might be something different. Go to tools first.

Michael: Tools, send and receive.

Nick: You should see account.

Michael: Email accounts. Email accounts, and there's a wizard. It says if you are changing existing email accounts.

Nick: Yep, do that one.

Michael: Then, I have change, add, remove, new Outlook data file.

Nick: Do change.

Michael: Okay, here more settings. There are more settings. More settings, advanced. So, server port numbers – incoming POP3. It's set at 110.

Nick: Is there a box underneath the server requires a secure?

Michael: Yes.

Nick: Check that. Does it change it to 995?

Michael: Yes, it does.

Nick: Good, and then do the same thing for outgoing.

Michael: Okay, 25.

Nick: Okay, change that. Type in 465, not the same one.

Michael: Okay 465, and then just go okay?

Nick: Yes.

Michael: Tell me the short little example what I've done to protect myself.

Nick: This is going to interrupt any data. So, when you check your email and it sends your user name and password across the ISP and stuff, it's going to send it encrypted, and this also even encrypts the emails and stuff too. So, if you send or receive sensitive data into your email, it'll be secure that way.

Michael: Now, I do have a little pop-up, the server you are connecting to is using a security certificate that could not be verified.

Nick: Just click yes on that.

Michael: And, I'm good to go, so I'm sending and receiving email the same way, but now I've secured and encrypted all my email communication. Man, that is awesome thank you.

Anyone who is emailing sensitive data and is sending any kind of email operating their business needs to do it on their Outlook. These same options are in all the major email clients.

Nick: Yes, every email client will have that.

Michael: Perfect, this is great value. How does this network sniffer suite work? What is it? Is it a piece of software the hacker downloads on their computer?

Nick: Yes, it's just a piece of software the hacker will have, and then it captures all the packets and stuff. Inside the packets, there's a bunch of data that's pretty much unreadable. You just look at it with the naked eye, but if you just network sniffer like this is actually a piece of multi-data and stuff, and show you actually the data in a very readable format.

Michael: So, packets are how data is transferred through the internet.

Nick: Right, in order to send data across the internet, it's got to be in real small packets because if you send a large file, even like a kilobyte, a lot of times, that won't go through. They break them up into small packets and send a whole bunch of little packets.

Michael: What kind of file is a packet?

Nick: It's just pretty much plain text, but it's in codes that the computer knows how to read.

Michael: So, network sniffer software will uncode that and make it readable, and when you read it you're reading it like as if someone's typed up emails, where it came from and all of that.

Nick: Yes, this is very readable and like a regular format.

Michael: So, why is this kind of stuff available on the internet? What kind of people create this software?

Nick: Employers can use that monitor their employees and stuff, if they want to monitor what employees are doing on their network. They might use one of these tools.

Michael: So, they can read the emails and stuff.

Nick: Right. The way to block this is to use the secure ports for setting and receiving emails, and Michael, that's exactly what we just did for you, and then on your website, you want to make sure you have the HTTPS on your pages that send or receive sensitive data, and make sure it's on your database too for your stuff that reads from the database. You want that to be over SSL as well.

Michael: What's another tool that hackers use to try and crack access into your sites?

Nick: A hacker can use a tool to gain access to your secure private wireless network. For example, if you have a wireless router at your home or office, there's a tool that will analyze the packets and it's able to determine the WET or WPAT.

Michael: What is that?

Nick: When you set up a wireless router, it asks you if you want to make it secure or not, and if you say yes, then it'll ask you to type in a key, and then when you're connecting your computers to the wireless network, it's going to ask for this key. It's kind of like a password to get on your network.

Then, that key is used to protect your wireless network, and then once they're able to use this program which will figure out your key or password for your wireless network. Then, they're able to connect to your network and they can use a tool like which we talked about in number two to be able to access your network and mess up some of your data.

Michael: Okay, so, let me ask you this. I just changed over to AT&T Broadband Wireless router. Now, I'm not using it. I'm using a regular desktop, but I am going to be getting a laptop and using it wirelessly. So, what can I do to make sure I'm secure using that?

Nick: With your router, there's going to be a default gateway, and when you go to that default gateway in your browser, you'll see a section there. It says set up a secure connection in that WP or WPAT.

Michael: How many people out there using their computers in offices and homes do you think are transmitting data securely, would you say out of a hundred?

Nick: Offices, maybe like fifty percent if that. Homes probably only 25% of data. A lot of people don't know how to set it up or don't want to bother with learning, or are not really sure how big of a risk it actually is.

Michael: What's another tool hackers are using?

Nick: They could use the read through data that you just deleted on your hard drive. For example, if you upgraded your computer and have an old hard drive that you're selling on eBay or selling your old computer, simply deleting the data off your hard drive isn't enough.

Once that is on the hard drive, it actually can't be deleted, and a hacker could use a tool like available from and what that'll do is go through the deleted files under your hard drive and allow a person with your hard drive now to be able to restore those.

So, if you had a file with bank account information or passwords in it that you moved to the recycling bin, and then emptied the recycling bin. The hacker who got your hard drive would be able to restore that.

For more interviews like this, go to HardToFindSeminars.com.

Michael: What about some of these free download softwares like Internet Eraser that's supposedly will erase all that?

Nick: I'm not sure exactly how those work. There's some paid ones out there that go through and make sure there's no left. One's called Secured Clean, and that's available at WhiteCanyon.com, and this will override all data on your hard drive with other data so it will add zeros to every spot on your hard drive. That's actually recommended that you override it at least three times just in case something didn't work. You go over it a couple of times to make sure.

Michael: So, if you've got a computer that's several years old, there's a real good chance you've got secure information on there. You want to get the software and clean your hard drive.

Nick: That's mainly if you're just getting rid of the computer. You don't want someone else to get the hard drive and then look at it and see what you did have on there.

Michael: What's another hacker tool?

Nick: One thing they could do on your web server and this is actually special files on there that'll hide them inside the server and hide the commands you run, like you'll never know he's there.

Michael: So, it's the ability to take over your server, and you would never even know.

Nick: Right, like if you do a DIR or an LIS directory listing, they'll make that script so it doesn't show up his files, but the scripts he uses then damage stuff that'll never show up.

Many of the scripts the hacker can use to gain access to install there are available, and these can be either local or remote attacks, remote meaning the hacker doesn't even need to have access to your server to be able to get in and get the route or the administrator level of access.

There was a big exploit out about a year ago where many hosting companies got hit with this kind of remote exploit.

Michael: Are you able to detect something like this on the servers that you host?

Nick: If you know what to look for, you can, but sometimes it's pretty hard not to experience. You can't really prevent it all the time, those remote exploits, but the companies that got the worse damage from it are the ones that didn't protect themselves from it right away, or the ones that didn't know it did until it had been some time had already passed.

For my servers, I have special software. It checks for over sixty known as well as second common files that a hacker might have changed to get that access.

Michael: That's great. What's a directory listing hack?

Nick: A directory listing hack is where a hacker will scan your website for every directory you have, and then use the directory in your browser, and if you don't have an index page on there, it's going to list every file that's in there.

I know of another hosting company who has a server hacked because he had his password in what he thought was a private directory, and the hacker was able to find and get access.

Michael: I think anyone who's surfed the net a little bit can relate to this if they're going to a website and instead of like a webpage coming up, an index page. They see this white page with the folders on it, right, and that's because that guy didn't have an index page that took him to a regular webpage.

So, with those folders, can they upload into those folders?

Nick: They can't really upload them.

Michael: But, they can download. Those are files on their server, so they can look inside those files. I got you. These hackers have software that scan the internet looking for these websites.

Nick: Or, they're targeting a specific person or something else, scan just a company and just start looking for directories that they might have created that don't have an index.

Michael: When you say directory, is that each folder on the site?

Nick: Yes, each folder.

Michael: So, each folder should have an index page?

Nick: Yes.

Michael: Each folder on the server should have an index page.

Nick: Yes, even if it's just for images or just something that's always good just to put an index page up there just in case.

Michael: How can I scan my site? What would I do to check all that?

Nick: If you have a lot of folders, it might be hard, but one way to prevent this is use that special configuration which is options minus indexes and you would put that in the HTX's file in your web root directory. If you have that, then even if you forget an index page, this will block a directory listing.

Michael: Can you do that for me?

Nick: Yeah, I can do that.

Michael: I appreciate it. This hosting business I've seen on the internet you've got a lot of hosting in a box type programs. How is the hosting industry changed with hosting companies reselling hosting packages where people can just buy into and suddenly they're an internet server host? How is this dangerous?

Nick: It's really easy to get started in this business, and a lot of companies out there, actually a lot smaller than you might think. One host that I know of just had a couple servers, and he was running them just out of a spare room and an office. He was actually in a pretty bad neighborhood and had a window air conditioner that anyone could easily have pushed in and took a couple of servers he had on there, and those websites would go down.

A good data center is like the ones I use. You need to pass through a keycard access and it's several doors you have to pass through. My data center it's three, and they're monitored with video surveillance, and you also need a positive ID and a biometrics handscanner. So, even if you have a key card, you wouldn't pass the handscanner and not be able to get in.

Even if you do get in to my data center, all the servers are locked up in cages, once you get inside.

Michael: So, they protect this thing like protecting gold in a vault. So, what's the reason why you want a reputable company to host your site?

Nick: You need a reputable company, there's one company I know of they had some servers that were being used for illegal activity, not by them, but by some of their clients. The FBI actually raided their data center and confiscated all of their equipment, so even the customers who have legitimate websites and stuff, their equipment was still confiscated, and the websites were down and everything.

Michael: I don't know if you remember me telling you this. I had my old autoresponder service with a company called ReplyTolt.com. They were out of Canada, and I had them for years. I had my entire database on there and everything, and then all of a sudden, they were gone. The Reply To It autoresponder service wasn't working.

I finally tracked them down and got in touch with the guy, and that's exactly what happened. They were being accused of doing spam, and they came in and confiscated the servers. So, everyone who had a Reply To It account, it was gone, all their mailing lists and everything. Fortunately, I had mine backed up, but a lot of people lost their entire mailing list because of something like that.

Nick: Yeah, a lot of people can lose data that happens. To prevent that, you want to research the company you're doing business with. Ask for some references of businesses that they do host. You could ask what IPs, and you need to do some research on that IP, and you could also ask if they host any IRC or Warez sites on their network. Those are the ones that tend to cause a lot of trouble.

Michael: What is an IRC or Warez site?

Nick: IRC a lot of the hackers and stuff will get together in this IRC chat room, and the warez sites are the ones where they used to download some illegal software that they use for hacking and stuff.

Michael: So, anyone who is allowing a server to have that kind of content is suspect.

Nick: Right.

Michael: What's a man in the middle attack?

Nick: A good analogy is do you order a product online than the company ships it out to you, and while it's in the middle of transit, someone takes out your product and replaces it with a bomb. Then, when you get the package, you're going to open it since you recognize that you order something, and when you open it, the bomb explodes.

Michael: Now, when you say bomb, what do you mean a physical bomb?

Nick: Yes, just as an analogy.

Michael: So, they could replace a CD with a worm or virus that goes on your computer when you put it in your computer.

Nick: Right, online it would be like replacing with a virus or something, and then hackers online can either send you their own data online when you're downloading a file from another website, or even if you're uploading to your own website, they could replace that with their own

virus. So, if you're putting up a file on your website for download, they could replace that with their virus.

Michael: I see. If they have access into your server, if I'm uploading files to my site for someone to download or for my customers to download, they could replace that file with a virus.

Nick: Right, actually, I am applying stuff that they have access to network like one of the things the program does is it can do this man in the middle attack. So, if they see transferring files, they could stick one of their own files in there, and then it'll say upload complete, but it's really uploading their file.

Michael: I see. So, they can see my file being uploaded and they can right there intercept it and upload their own file, but they could keep the same name as the file that I was uploading.

Nick: Right, they'd have the same name, so it would be hard for you to notice.

Michael: Would they know how comes to my download page and downloads the file so they know exactly who has the download of the virus?

Nick: Yes, they'll be able to see the IP address of the person who's downloading your file.

Michael: How can we prevent this?

Nick: To prevent this, you could use an MD5 Sum check. This reads your file and assigns a code to it based on the contents, and then after you upload it, download that file, you could run that MD5 Sum command again, and make sure it returns the same code meaning it's the same file.

The code is so unique that the chance of two files having the same code is over one in one trillion.

Michael: Okay, so give me an example of how I can specifically use that. Let's say I'm uploading files up onto my server for my audio editor to do editing. How do I get this MD5 Sum check? How does it work?

Nick: That's a command in like Unix or Linux, so if you're running that on your computer, you would just type in the command MD Sum space and then the file name, and then hit enter. It would return the code, and

then after you upload it, you would go to your server. Let your server run MD5 Sum space and the file number, enter. See if that code matches.

Michael: Okay, but if I'm not running Unix, I'm just running Windows XP, I can't really use that.

Nick: There's probably a program out there that'll run it for Windows or something similar.

Michael: Okay, but as long as I'm covering my bases on all of the other areas, I really don't need to worry about that.

Nick: Yeah, then you should be okay.

Michael: Tell me how hackers use social engineering. Explain what is social engineering.

Nick: Social engineering is kind of like panning your way when you're talking to people. Hackers are going to find out a little bit of information about you, and then they could contact like your hosting provider, ISP to try to get your password or have like the email changed on your domain. There's place where if the hacker types in your domain name, it'll give your name address phone number, etc. So, they can call up your hosting provider and try pretending they're you.

If they're asked to verify their address or phone number, they have that handy so they'd be able to verify. You'd be surprised how much information companies will give out.

This is because A the smaller companies don't really have a strong verification procedure in place, or if the bigger companies have the verification procedures, but a lot of times they get employees who won't file them. Either they're poorly trained, or they're on the way out the door looking for a job somewhere else and don't really care, or they're just trying to get home for the day and just want to get the customer off the line.

Michael: Nick, so what makes your hosting company different? Can we talk about you having all these servers? They're in secure lock down cages. No one can break in. You're constantly scanning for hackers. How important are updates, and how do we know that you're updating your servers and what's important about having servers updated for people hosting their websites on their servers like myself?

Nick: A lot of hosts don't do regular updates, if they do them at all. There's five main ones you want to make sure your host does. Number one is the kernel. This is the heart of the operating system.

A lot of hosts don't do this because one, they don't know how. Two, it requires a reboot of the server, which causes some downtime, or three, if you're not good at it, a lot of times the server doesn't boot back up and you have to redo the kernel or do something else to get it to work again.

I know when I first learned how to upgrade kernels, there were a lot of times when the test servers I was working on didn't come back up, and you need to do these upgrades to enhance the performance of your server as well as for security reasons.

Michael: So, people are hosting with companies who aren't doing these updates. Their websites are a lot slower than they need to be.

Nick: Yes, they'll be slower, and it'll be possible that a hacker could get into them, too.

Michael: How important is Apache and PHP, and what are those?

Nick: Those are for the web server. A lot of companies start out with this company in a box. They're turn-key solutions to start up their company overnight. They're not going to run a lot of those updates even though you're supposed to.

The Apache upgrade could be difficult because it requires running a lot of codes via the Unix command line, and like the kernel, if you don't know exactly what you're doing, the web server is not going to come back up when you're done, or it'll be missing important libraries and stuff.

If they forget to include the code for even one library, instead of your webpage coming up, it's going to give an error message instead.

Michael: I've noticed over the years in the control panel part of my websites, I've seen you do several updates over the last several years. How important are these updates for the control panel area?

Nick: These have been really important. I know there are a couple of times where I needed to upgrade your control panel software immediately to patch an exploit that just became publicly available. The reason these

are so important is because this software is installed with what's called root access or like the super user access meaning that user could do anything on the server.

If there's a mistake in the code for part of that control panel that uses thousands of scripts and stuff, and if even one part of those scripts is wrong, a hacker could potentially gain this super user access and take over the whole server.

Michael: Now, you just emailed me today about a widespread exploit. Tell me what that was about. How did you find out about this, and what was this doing?

Nick: A customer on one of my other servers, this site was sending out a lot of spam emails, and I checked for it running the commands I usually do, and that didn't find anything. So, I had to do some more digging and stuff. It turns out these hackers are using a new method now that's this user encode thing, and they're using that just because they're trying to stay one step ahead of the good system admin and stuff, trying to get it so they're not able to get caught.

Michael: How long were you able to identify it and eradicate it?

Nick: Let's just say about an hour and a half to find out what it was, so it was pretty hard. I had to look through a whole bunch of files, and now that I know what to look for, I could find them real fast.

Michael: Now, once you found out, how did you design and secure the site to close up that whole?

Nick: Those were because the user had a third party script that they didn't upgrade, and these files are actually back doors and stuff. So, if they do upgrade, if I left those files in there, they'd still be able to get in after they upgraded their software. So, I removed those files, and then I had them upgrade their third party scripts that they had on there.

Michael: That brings me into this next one. Running up to date, what is this up to date script and why do you use it, and how do I benefit by hosting with you by you using it?

Nick: The up to date runs an update for all the little packages that your operating system is comprised of. If there's a patch released for one of those small packages, then this up to date is going to update your package and feed the performance issue or security issue.

Similar to number three, all these little packages are installed as roots, so you're looking at a potential full takeover if one of those aren't updated, and just to give you an idea of how many there are, on my servers, and I don't really have that much extra stuff installed, there's roughly 400 small packages. I regularly check for updates on those via an automated script I have.

Michael: How often do you check timewise?

Nick: Daily.

Michael: Daily, and you did a report.

Nick: Yes.

Michael: Give me one more example of ways that you protect your customers by making sure your servers aren't being hacked.

Nick: Another thing I do is check for files out of the ordinary. This is files at the user level, and also for system files. What we do here is check for certain strings that are common for files that hackers would upload. This is similar to what I searched for on your server today when I was doing the scan for you.

If I did find any of those files on your server, I would go one level up from the user level to see if a hacker got into like the root level. There wasn't anything wrong on the server at the user level, so I didn't have to do that second level check, but if I did, I would review some of the system binaries, and also check the running processes on your server to look for anything that was out of the ordinary.

Michael: Nick, if someone was hosting a site with someone else, could they approach you and have you do an audit of their website, even though you're not hosting it? Could you look at their site and kind of look at the guts of it to explore for any kind of vulnerabilities?

Nick: Yes, I could check for about 75% of the stuff. The other 25%, you need that super user access to check for. Michael, for any of your listeners, if they order the Guerilla Internet Marketing course, you could use one of the consults with me for me to go over your website to look to make sure that the hacker hasn't gone in and hasn't upload anything bad to your account. All you have to do is go to YourMarketingMastermind.com

That's the end of our security recording with Nick. I hope this has been eye-opening and educational, and I know for a lot of website owners like myself, a lot of what Nick was saying is probably over your head. I would definitely recommend you contact Nick if you want him to review your site for security loopholes. Obviously it's easy to let things slip by. I would hope that your site doesn't get hacked into like mine did. It's a real headache. You can contact Nick by getting his Guerilla Marketing Internet Secrets product by going to YourMarketingMastermind.com. Thanks for listening.