You can search the Internet for a year to find the right job. Be aware a job is more than searching for your skills to match an employer’s needs. It is much more. In the last “Get a Job” article in the April 2012 issue we painted a broad picture and filled in a few of the blanks. In this article we’ll discuss some of the search sites you can use to start with and fill in a few more of those important things that must be considered when looking for a job. Also, we’ll reiterate the more important concepts because we need to consume this information and make it our own - as if our lives depend on it - because our next set of jobs certainly do.

If you are looking for the “one best place” to find your next job – you may be finding the search frustrating because much of what is needed will be found through word of mouth and networking and not in newspapers or radio/TV ads. No one is out there trying to bring your job to you. You must work for it. There are plenty of good hunting grounds everywhere and this article will show how the Internet might be a good starting point. The search engine tools called collectors will give you a good idea of what positions might be open as a first indication.

So you are thinking – there is a lot of competition for the jobs out there, right? Remember that there will always be plenty of people who have creativity and the right attitude. How do we match the needs of an employer to what we as job seekers have to offer? How do we recognize when there is a good match between those two things? How does a job seeker get the job they truly want and can bloom at doing?

As the job seeker, your first and most important job is to find the fit you have with the company – and there are several sites that will give you a general idea of the jobs, titles and requirements when you first start looking. Once you find those jobs - then it is up to you to make the map to show the fit so that the employers can understand how and why they should hire you. Keep in mind that you are a product. Sounds cold? Nah – it’s a fact – you are the product and you would look much more appealing if you are sparkling and stellar. What seems stellar to one company might not interest another – so do your homework. First place to start? NETWORKING.

The ISSA Colorado Springs Chapter can offer you so much more in the way of personal networking than other organizations because we share a common bond of being security professionals. We know each other, and we know the challenges we face. Generally speaking – we have a wealth of knowledge that is rarely found in other organizations.

(Continued on page 6)
Internet doomsday, explained

According to media reports, July 9 will be our online apocalypse. The better story is how this crazy rumor started.

May 16, 2012, By Mathew Gross and Mel Gilles

The apocalyptic story line was once reserved for truly apocalyptic events. Nuclear war. The return of Christ. Environmental or economic collapse. But it’s 2012, and the apocalypse has become the basis for everything from Super Bowl commercials to summer romantic comedies — and no media story is too small to have an apocalyptic moniker attached to it. (Remember Snowmageddon?) If you want to get the world’s attention, simply proclaim that the world will soon end — or the Internet. Just read coverage of the so-called Internet Doomsday virus, which will supposedly strike and shut down the Web on July 9.

Here’s how the story got started. Back in October, the FBI announced that it had broken up an international crime ring when it arrested six Estonians in what was then heralded as “the biggest cyber criminal takedown in history.” The Estonians had, over the course of four years, hijacked more than 4 million computers in 100 countries through the use of malware known as DNSChanger. By redirecting the infected browsers of unwitting users, DNSChanger was able to send high volumes of traffic to the criminal ring’s rogue websites and servers, collecting more than $14 million in fraudulent advertising revenue and exposing their victims to information theft in the process.

“Operation Ghost Click” (as the FBI dubbed its sting operation) put an end to the Estonian scheme, but a problem remained. If the feds simply shut down the Estonian servers, the 4 million infected machines — nearly 1 million of which were in the United States — would be unable to reach the Internet. To give the cyber-crime victims time to clean up their machines, the FBI contracted the Internet Systems Consortium (ISC) to maintain valid servers in place of the criminal servers. The new servers would remain online until March 8, 2012.

And so it came to pass that the FBI tried to warn the people, but the people were not listening. The people were too busy swatting the pop-up ads that buzzed like flies around TMZ.

As things turned out, a cabal of Estonian thieves in an international crime ring wasn’t enough to get the public’s attention. By early February, nearly half of all Fortune 500 companies and half of all major federal agencies still had computers infected with the virus — along with 400,000 other computers around the world. If the government shut down its proxy servers on March 8, as was planned, all of these computers would be unable to access the Internet. (The FBI, frankly, hadn’t done the best job in getting the word out about DNSChanger: It slapped up a PDF on the Web and assumed people would find it.)

And then it happened. Somebody put two and two together. There was a larger, more familiar narrative at work here. The tale of Operation Ghost Click and DNSChanger held all the elements of a familiar story. A set date. The need for the wayward computer users to repent before the date came. The smug satisfaction that when the date finally came, the non-believers would be cast into a disconnected hell, with nary a Google Map to lead them out of it. Have you not accepted Norton AntiVirus as your savior? IT nerds across the nation waved their MacBooks in contemptuous indignation.

This wasn’t just any old computer virus. For those who did not repent — or at least scan their computers for the virus — March 8 would be INTERNET DOOMSDAY.

Read the rest here: http://www.salon.com/2012/05/16/internet_doomsday_explained/singleton/
Most IT and Security Professionals See Anonymous as Serious Threat to Their Companies

By Lucian Constantin, IDG-News-Service:Romania-Bureau

The majority of IT and security professionals believe that Anonymous and hacktivists are among the groups that are most likely to attack their organizations during the next six months, according to the results of a survey sponsored by security vendor Bit9.

Sixty-four percent of the nearly 2,000 IT professionals who participated in Bit9's 2012 Cyber Security Survey believe that their companies will suffer a cyberattack during the next six months and sixty-one percent of them chose hacktivists as the likely attackers.

Respondents had the option to select up to three groups of attackers who they believe are most likely to target their organizations. The choices were Anonymous/hacktivists, cybercriminals, nation states, corporate competitors and disgruntled employees.

Anonymous was chosen by the largest number of IT professionals overall, but there were some differences based on the type of organization. For example, nation states was the top choice for people working in the government sector, while those working in retail selected cybercriminals as the top threat.

Anonymous was chosen by the largest number of IT professionals overall, but there were some differences based on the type of organization. For example, nation states was the top choice for people working in the government sector, while those working in retail selected cybercriminals as the top threat.

According to Verizon's 2012 Data Breach Investigations Report, hacktivists stole the largest quantity of data in 2011, but they were responsible for only 3 percent of the total number of breaches.

Respondents choosing hacktivists as a more likely source of cyberattacks than cybercriminals is similar to how most people fear flying more than driving, even though, statistically speaking, it's far more likely for someone to be involved in a car accident than in a plane crash, said Bit9 chief technology officer Harry Sverdlove.

The truth is that you are less likely to be attacked by Anonymous or hacktivists -- depending on what public statements you make -- than to be attacked by a cybercriminal enterprise or a nation state, he said.

Despite considering Anonymous the top threat, when selecting the method of attack they are most worried about, 45 percent of respondents chose malware, which is generally associated with cybercrime rather than hacktivism.

Read more here:
http://www.pcworld.com/businesscenter/article/254270/most_it_and_security_professionalsSeeAnonymousAsSeriousThreatToTheirCompanies.html

Analysis of the Jericho Botnet - A Modern Malware Case Study

By Wade Williamson on May 07, 2012

We've talked a lot about modern malware as a concept, but I'd like to use this week's column to call out one particular sample of malware that I've had my eye on for the last several weeks -- a new banking botnet that has been referred to as the Jericho Botnet.

This botnet also illustrates the importance of the malware trends for 2012 that I called out in an earlier column -- the increasing sophistication of malware writers' coding techniques, the need to more tightly control applications that malware will use to communicate with the outside world and the advantages of sandbox analysis when applied to anti-malware network security.

We'll also analyze how this botnet typified a piece of "modern malware" by focusing on three of the stages of the malware lifecycle we outlined in an earlier post, The Evolution of Malware: Infection, Persistence and Malicious Functions.

Infection: How is the malware delivered?

In early April we began to detect samples of a new banking botnet that was hitting enterprise networks, and showing very low coverage rates by traditional antivirus signatures. We detected these samples using sandbox analysis techniques discussed earlier to scan unknown files for behavior consistent with that of modern malware. On closer inspection, these malicious files appeared to be based on a variant of the well-known, stealthy Jorik Trojan, and we noticed that all 42 variants were originating from Israeli Internet space.

These files were delivered to victims via .php pages during browsing sessions. Despite originating from domains located in Israel, analysis of the malware package itself showed that the vast majority of the URLs used to deliver the malware ended in ierihon(dot)com. Ierihon is the word for Jericho in Romania (hence the name), and reverse engineering of the sample revealed several other Romanian words buried in the sample. All of this suggests a Romanian origin for the malware package.

Read more here:
May 1, Government Computer News – (International) **Targeted attacks, mobile vulnerabilities on the rise, report states.** The findings of the latest “Internet Security Threat Report” from Symantec can be summed up as: “Attacks are rising, but the number of new vulnerabilities is decreasing.” This describes the threat landscape in 2011 in which hackers continued to exploit known vulnerabilities through new vectors as enterprises and end users failed to keep up with the flood of security updates from vendors patching their software. “The old vulnerabilities still work,” said the manager of Symantec’s security technology and response product group and a contributor to the report. Malware variants are being packaged in attack toolkits that effectively circumvent signature-based defenses. The data in the report is gathered from the company’s Global Intelligence Network monitoring activity in more than 200 countries. The total number of vulnerabilities reported in 2011 dropped 20 percent, from a high of 6,253 in 2010 to fewer than 5,000. Over the same time, the number of unique variants of malware identified in the wild increased 41 percent and the number of attacks blocked by Symantec tools jumped 81 percent to 5.5 Billion in 2011. The vectors for delivering the malware are shifting, with Web attacks and social engineering through social networks replacing e-mail as the method of choice. This is due in part to successful law enforcement campaigns against command-and-control systems for spam-speding botnets in 2011, and also because the Web offers a good alternative. Targeted attacks, which have proven to be effective in breaching high-value organizations through carefully crafted social engineering, increased during 2011, from 26 such attacks identified in January of that year to 154 in December. At the same time, the attacks are now targeting smaller organizations and lower-level employees. Source: [http://gcn.com/articles/2012/05/01/internet-threat-report-targeted-attacks-mobile-vectors.aspx](http://gcn.com/articles/2012/05/01/internet-threat-report-targeted-attacks-mobile-vectors.aspx)

May 18, Help Net Security - (International) **Spam with malicious attachments rising.** While the volume of spam messages is falling, the number of messages containing malicious attachments increased, meaning spam is growing more dangerous even as it becomes less prevalent, according to a Bitdefender study. The number of malicious attachments in January 2012 rose 4 percent from the same period in 2011, even as the overall number of spam messages sent dropped by more than 16 percent in the first quarter of 2012 from the last quarter of 2011, Bitdefender research shows. Of the 264.6 billion spam messages sent daily, 1.14 percent carry attachments - about 300 million of which are malicious. After increasing in January, the growth of malicious attachments leveled-off amid an apparent pause in spam campaigns even though spam continued to fall overall. Attachments may come in the form of phishing forms that trick users into typing in credit card credentials for scammers to use whenever they want. Or, they may pack malware such as trojans, worms, and viruses that can eventually cause trouble for users. Source: [http://www.net-security.org/malware_news.php?id=2113&utm](http://www.net-security.org/malware_news.php?id=2113&utm)

May 10, IDG News Service – (International) **APT attackers are increasingly using booby-trapped RTF documents.** Booby-trapped Rich Text Format (RTF) documents are one of the most common types of malicious Microsoft Office files that are used to infect computers with advanced persistent threats, according to security researchers from Trend Micro. The company’s statistics show that 63 percent of the malicious Microsoft Office documents intercepted in April exploited vulnerabilities in Microsoft Word. Out of those vulnerabilities, the most commonly targeted ones were CVE-2010-3333 and CVE-2012-0158, which stem from bugs in Microsoft Word’s code for parsing RTF content. This is troublesome because Microsoft just patched a new Microsoft Word RTF parsing vulnerability May 8 that could allow remote code execution. Source: [http://www.infoworld.com/d/security/apt-attackers-are-increasingly-using-booby-trapped-rtf-documents-192891](http://www.infoworld.com/d/security/apt-attackers-are-increasingly-using-booby-trapped-rtf-documents-192891)

May 15, IDG News Service – (International) **Wikipedia warns users about malware injecting ads into its pages.** Visitors to Wikipedia who see advertisements on the site have most likely fallen victim to a browser-based malware infection, Wikimedia Foundation, the organization operating the Web site, said May 14. “We never run ads on Wikipedia,” said the director of community advocacy for the Wikimedia Foundation. “If you’re seeing advertisements for a for-profit industry ... or anything but our fundraiser, then your Web browser has likely been infected with malware.” One example of such malware is a rogue Google Chrome extension called “I want this,” the director said. However, similar malicious add-ons might also exist for Mozilla Firefox, Internet Explorer, and other browsers, he said. This type of malicious software is known as click fraud malware and can target multiple Web sites at once. Source: [http://www.computerworld.com/s/article/9227179/Wikipedia_warns_users_about_malware_injecting_ads_into_its_pages](http://www.computerworld.com/s/article/9227179/Wikipedia_warns_users_about_malware_injecting_ads_into_its_pages)
Interpol to Crack Down on Cyber Crime

May 10, 2012

Interpol said it is making the war against cyber crime a main priority this year as online fraud crosses borders and increases in scope.

Khoo Boon Hui, president of the global police network, told a conference of 49 European member states that cyber crime is becoming more transnational. He pointed to a study published in March by the London Metropolitan Univ. that found 80 percent of online crime is connected to cross-border organized gangs.

"Organized crime is now able to recruit members from countries without diplomatic ties to commit crimes overseas operating from temporary safe bases in third countries equipped with the latest technology," he said.

Hui said Malaysian police last month arrested more than 200 cyber criminals from China and Taiwan who operated online scams through two syndicates under the instructions of a common Taiwanese boss.

By using temporary safe bases around the far East, the online scammers netted billions of dollars via soccer and gambling websites along with credit card and bank fraud schemes, he said. He said hackers even penetrated the Interpol website this year.

Hui said cyber crime costs Europe about 750 billion euros, or more than $977 billion, a year. Israel alone deals with more than 1,000 Web attacks a minute, he said.

To help train police worldwide in online law enforcement, Hui said Interpol will open a cyber crime and digital security complex in Singapore in 2014.

This week's conference also addressed other issues including international terrorism, the drug trade and human trafficking.


Anonymous claims access to classified US databases

May 14, 2012 by Trent Nouveau

Christopher Doyon, aka Commander X, faces 15 years in prison for assaulting the county website of Santa Cruz, California to protest the forcible removal of a homeless encampment on the courthouse steps.

Doyon is currently hiding out in Canada to avoid prosecution, courtesy of what he describes as a new "underground railroad," or a network of safe houses across the country.

"I think the general public is beginning to learn the value of information. To give an example, for a very long time nobody in the US or the world was allowed to know the number of civilian casualties in Afghanistan or Iraq," Doyon told Canada's National Post.

"There were wild guesses and they were all over the ballpark figures, until a young army private named Bradley Manning had the courage to steal that information from the US government and release it. Now we know that despite their smart munitions and all their high-tech technology they have somehow managed to accidentally kill 150,000 civilians in two countries."

Doyon - who participated in a number of other high-profile Anonymous campaigns - also claimed the collective has access to "every classified database" in the US government. According to Doyon, the digital keys were handed to Anon operatives by the very same "people who run the systems."

"It's the pimply-faced kid in the basement who controls the whole game, and Bradley Manning proved that. The fact he had the 250,000 cables that were released effectively cut the power of the US State Department in half," he said.

"The Afghan war diaries and the Iran war diaries effectively cut the political clout of the US Department of Defense in half. All because of one guy who had enough balls to slip a CD in an envelope and mail it to somebody."

Read more here:
http://news.nationalpost.com/2012/05/12/insider-tells-why-anonymous-might-well-be-the-most-powerful-organization-on-earth/
Get a Job II

So, get out on the Internet and start looking on your own – then – go to the next ISSA Chapter meeting and talk with your peers about what they are seeing and hearing. Share the information and ask questions. Find out what companies are hiring locally or nationally and what needs those companies have. Ask around and listen to the answers. You will find a lot of folks here in the Chapter have been where you are and are willing to help you.

What do you do if you don’t know where to start? First, think about what kind of job title might suit you. Where do you see yourself going? Where would you like to work? Some of the titles you might look for include: Security Architect, Security Engineer, IA Engineer, Network Engineer, Project Manager, Program Manager, Senior Engineer, Principal Engineer, Analyst and so forth.

Next, consider starting your job search by looking at some of these major job web sites:

**6FigureJobs** - 6FigureJobs.com is primarily for executives and senior-level professionals making $100k+ and includes C-level, VP, Director and Senior Manager Jobs.

**CareerBuilder** - CareerBuilder.com is the largest online job search site in the U.S. They work with over 300,000 employers including 92% of the Fortune 1000.

**Indeed** – Indeed.com is a collector site. This means that Indeed.com takes input from lots of other sites and puts it in one easy to use format. As of the end of April 2012 Indeed shows 623,585 new jobs posted in the last 7 days. Indeed allows you to search job sites, newspapers and associates as well as company career pages.

**Simply Hired** – Is another collector site and as of 29 April showed 4,708,678 open jobs from job boards, company web sites and across the web. There is no lack of work.

**Glassdoor** – Have you wanted to know what it might be like to work with a company before you got there? Glassdoor.com is a collector site that allows you to search through millions of job listings and see salaries, reviews, and any possible inside connections that you might have at the company.

**Jobs2Careers** - Jobs2Careers is a collector site that gets job listings from all over the web and allows you to search them from their site.

**Beyond** - Beyond.com is another collector site that holds 70 unique career channels and over 3,000 industry and region specific job boards.

**Snagajob** - Snagajob.com is more focused on the hourly, local, full and part-time jobs but also has a reasonable sized listing of other types of jobs.

I’m sure that someone reading will likely say – “what about DICE.COM or MONSTER.COM?” … Well the intent of the above list is not to provide the reader with the one single comprehensive list of all job sites but to give the reader a starting point to discuss with colleagues. Everyone will have their favorites and not all of them will be exactly what you want. Ask your fellow ISSA Colorado Springs Chapter members about what has worked for them. The process will likely be iterative and take time to walk through but will be rewarding in the end.

In fact, if you head over to about.com and look for the top 8 job search engines you will find: monster.com, indeed.com, usa.gov, careerbuilder.com, dice.com, simplyhired.com, linkedin.com, and craigslist.com – some are the same as we’ve listed and these others are a good starting point as well.

Next, once you have done your research, find open jobs to apply to, and send out resumes then you wait, right? Wrong – keep networking. Sooner or later you will get that call for an interview – your big number one goal changes to become the most prepared for that interview, right?

**NEWSFLASH**: The biggest mistake typically made when going to interviews is not being fully prepared. No need to be arrogant but any lack of confidence is seen by a potential employer as not knowing your stuff. In a market where you compete for the shrinking number of available jobs – you MUST KNOW YOUR STUFF. You must sparkle and shine above others.

You DO know yourself better than anyone else does. Clint Eastwood might ask you one question: “You’ve got to ask yourself one question: ‘Do I feel lucky?’ Well, do ya punk?” The interview is NOT a place to get lucky and there isn’t a gun to your head. There is no need to be anxious or nervous but in order to know the answers you must get a handle on what questions are likely to be asked.

One way to do this is to search the Internet for “behavioral interview questions” or search for the “top 100 interview questions” – then STUDY the questions and have your answers ready.

Although your resume lands you the interview, it is ultimately the interview that gets you the job. So, being well prepared for whatever any interviewer throws at you is crucial. Here are a few simple tips that you can use to effectively handle the interview process:

- **Conduct YOUR Research** – It’s important to be confident and prepared. Research the company before apply-
ing to a job and before showing up for an interview. By understanding and showing interest in the company, you can customize your pitch, demonstrate the value you will bring to the organization and confidently convince employers that you are the right candidate. Know what these companies do. Know who they do it for. Know where they are headed. The more you know the more you can prepare reasonable questions for them. Remember that the interview is the place to ask them questions and be prepared with at least three questions to ask.

- **Practice Interviewing** - Prepare for an interview by running through commonly asked interview questions. Understand that interviewing is a skill and as with any skill, practice makes perfect! We’ll put together a group of questions and help you do a phone interview if you would like. Contact your ISSA-COS Executive VP, Tim Hoffman, at: tim.hoffman@alidacollection.net - That’s right – your ISSA Chapter helps you.

- **Dress Professionally** – When you are on an interview, you are marketing yourself as the best candidate for the job, so it’s important to dress professionally. Do you know what the company considers appropriate dress? Wearing a hoodie to a meeting to ask for money from Wall Street just got Mark Zuckerberg noticed – and not in a good way. Appropriate attire and good personal hygiene demonstrates that you are not only willing to take that extra step to look your best but also to do your best on the job. You only get one chance at a first impression and it counts. You are being reviewed from the first moment you see the interviewer. Why not make this the most positive you can?

- **Make a Positive First Impression** – First impressions are critical. I’ve just stressed this again. So what can you do? Arrive early, give a firm handshake and make eye contact throughout the interview. It is important to be confident, but most importantly, be yourself! 100% integrity. Positive truthful answers. This is what helps make the interview go in your direction. Companies do not need people to inflate what they’ve done in their work history – so don’t try it during the interview.

- **Go Beyond the Canned Response** – Behavioral interviewing is an ever-growing interview technique. Rather than merely telling the interviewer what you would do in a situation, demonstrate your knowledge, skills, and abilities by giving specific examples from past work experiences. Show them you know your stuff and have used it in similar situations to save the day. Again – don’t em-bellish.

- **Ask Questions** – Express interest and willingness to learn about the company by asking questions and listening to details about the organization. Go back to step #1 and make sure you have done some homework on this company. This portion of the interview is your chance to really shine. Not having any questions for the interviewer can show that you are uninterested and unprepared. Also, it is really comforting knowing that many people who go to interviews have nothing when asked if they have any questions. You will fare much better than your competition if you have some questions lined up. Such as: “What can you tell me about the team culture here?” “How do you feel the re-organization will positively affect the team?”

- **Follow Up** - Reinforce to the employer that you bring value to their organization by developing a well-written thank you note. A thank you note is an easy and sure-fire way to show your appreciation, reiterate you are the best candidate, and demonstrate your initiative and follow-through as well as make you shine above other competitors for the position. It is also appropriate to make a follow up call, unless instructed otherwise by the employer.

Okay – as mentioned – we will re-iterate some of the more important concepts. Let’s drill into it:

**Be Prepared.** Regardless of the position, you should always dress appropriately to show the employer that you take pride in yourself and as a result you take pride in your work. You are pitching a product and that product is you. Being at the interview on time (15 minutes early) and ready; the way you dress, the way you walk, the way you shake someone’s hand, the way you make eye contact; all of these send the potential employer a signal. You either say “I am successful” or not. Be the right person for the job by showing the employer that you have value; that you are already successful.

Once you have refined your personal image; make sure that your internet appearance is just as professional. Stay tuned to a later newsletter article for information on how you can create a professional online presence. This is just an initial note to say – it is time to take down those bawdy pictures of you and 5 “good friends” sharing that keg of beer at the party in Cabo or that last New Orleans Mardi Gras trip. So your friend says to you - hey – I just got called for a job interview. What type of preparation is necessary?

1. **Update your resume.** Each job is unique and your approach needs to be tailored to the job. We talked about being the best fit in the last article. What does it say about the person who last updated their resume 2 decades or 2 jobs ago? The new potential employer wants to see relevant experience, and if the most recent job is not listed how will they know? The immediate thought that might come to mind could be: “Why isn’t this person on the ball?” or worse yet (because it is easy to think the worst) “What is this person hiding?” … so updating your resume is the first item on the list.

2. **Identify the application and collateral submittal re-

(Continued on page 8)
quirements and meet every one of them. If the job announcement clearly states that 3 letters of recommendation are REQUIRED — then provide three letters with the application. If 5 references are REQUIRED — then get 5 references. Show yourself to be competent. You are probably thinking — hey — no one is 100% all the time. Well, if everyone else is 97% then you be 100% correct and get the job. That is what employers are looking for. It is a competitive landscape out there and we need to present our best. Do more and be more — don’t settle for good enough.

3. Identify the employer expectations that go beyond the resume, application, collateral paperwork (like references) and try to learn what the employer really considers to be top-notch performance. Look at doing informational interviews with similar companies in industry. Ask your colleagues and find out what their experiences have been.

4. Identify the trends and latest shifts in the industry. If you are seeking a job in education - are you well read and are you published? Do you stay updated on the latest information in your industry? Do you know the latest inventions? Do you know about the latest trends in learning/teaching? Is the industry you are seeking employment with declining, growing, stagnating or otherwise doing poorly? Your industry knowledge will help you understand and navigate the process. ISSA Colorado Springs will certainly have someone working in that area.

5. During an interview you will be on your best behavior. That goes without saying — but I’ve said it again because you can easily make the wrong impression. Say you ask a question like this: “How many hours are you expecting a person to work in this job?” The people on the interview team could be left with the impression that you are the type of person who only wants to work as little as possible. Don’t leave things to chance and don’t ask open questions like that during the interview. Don’t ask that type of question at all! It is important to find out about the culture and the business itself. There is real value in asking another member of the ISSA Colorado Springs Chapter because you can ask well before the interview and know more about the company. Be sure to ask questions but think about the impact of those questions, and how they might be taken the wrong way. Word them so that they can’t be taken the wrong way. In short — think of the other person first and let them know you are sincerely interested in the job and the company.

The Questions To Ask At The Job Interview

During your interview — you will likely be asked “Do you have any questions for us?” Many people either draw a blank or think it is polite to say “No — everything has been covered” and this is exactly the wrong thing to say. You are given a brief window of opportunity to ask questions that will make a difference for you and the company. Do not pass up this chance to ask good questions. This is a time when you can use these questions to map your skills or to cover ground you may feel you have lost during the earlier part of the interview. You might have found out that the company is in crisis, or that there is major stress of some sort. This may be the type of environment that stimulates you. It would be a good idea to show that you understand the company’s needs and ask about how you might be effective immediately. The rule for this is simple — go ahead and ask the questions — but consider the audience first. FOCUS on the position and duties assigned. FOCUS on what you have heard while in the interview. Listen for clues throughout the interview.

BE PREPARED by bringing at least 3 questions with you. For example: ask how the challenges were met in the past, and what methods were most effective. Listen to the answer as this could be your chance to jump in with knowledge on how you have been effective at solving the same or similar problem. Remember the interview isn’t over until you have the signed offer letter in your hand. Another example might be to ask about how the culture works in the company or how steep the learning curve is for someone new.

Another approach might be more personable and direct with the interviewer. You might ask about the background of the people who are interviewing you. This should be done by asking the senior member if that would be alright to ask for since you might be working closely with the team in the future. Knowing about the background of team members is beneficial because it helps you bond and helps the other team members be comfortable with letting you know that they “know the ropes” — but be careful not to be so focused that it seems like a cross-examination. You might ask about qualities it takes to get the job done, management style, the steps involved with the hiring process and so on. Listen carefully to the answers because there will be clues about the job and associated difficulties.
Tim is a well-known consultant, trainer, former radio show host, and co-author of four technical books published by Prentice Hall PTR. He has extensive experience with security of wired and wireless networks, and computers and telecommunications that dates from 1969. He has worked with Fortune 1000 to small businesses, helped start small businesses of his own, and is currently the President and Owner of the Alida Connection, a VA Approved Veteran Owned Small Business that provides computer security consulting and technical training. Tim holds an MS, CISSP, GCIH, ISP, C|EH, Expert Rating PmP, CTT+, Security+ and Network+ and a range of other certifications. He consults, teaches and writes about computer and network security, TCP/IP, CISCO and most other vendor Back-Office technologies.

If you desire a mock interview or examples of interview questions that you should know the answer to – please contact Tim Hoffman at tim.hoffman@alidaconnection.net.

(Continued from page 8)
Real-world beaming: The risk of avatar and robot crime

Laurence Peter BBC News, 10 May 2012

A demonstration of how robot 'beaming' technology works

First it was the telephone, then web cameras and Skype, now remote "presence" is about to take another big step forward - raising some urgent legal and ethical questions.

"Beam me up Scotty" - that simple phrase reminds us of Captain Kirk, whisked from alien worlds back to the Starship Enterprise via the magic of "teleporting", in the cult TV series Star Trek.

"Laws might have to adapt to the fact that certain crimes can be committed at a distance, via the use of beamed technologies"

Beaming, of a kind, is no longer pure science fiction. It is the name of an international project funded by the European Commission to investigate how a person can visit a remote location via the internet and feel fully immersed in the new environment.

The visitor may be embodied as an avatar or a robot, interacting with real people.

Motion capture technology - such as the Microsoft Kinect games console - robots, 3D glasses and special haptic suits with body sensors can all be used to create a rich, realistic experience, that reproduces that holy grail - "presence".

The kit is getting cheaper all the time and researchers expect that in the near future it will be quite easy to set up a beaming-enabled room in a typical home. Beaming may also use less bandwidth than conventional video streaming.

Project leader Mel Slater, professor of virtual environments at University College London (UCL), calls beaming augmented reality, rather than virtual reality.

In beaming - unlike the virtual worlds of computer games and the Second Life website - the robot or avatar interacts with real people in a real place.

He and his team have beamed people from Barcelona to London, embodying them either as a robot, or as an avatar in a specially equipped "cave". One avatar was able to rehearse a play with a real actor, the stage being represented by the cave's walls - screens projecting 3D images.

The technology is already good enough for "blocking" a play - working out how the actors should move around the stage - though emotion and facial expressions are not yet captured accurately enough to replace a traditional rehearsal. This may not be far off, however.

Teleconferencing would be transformed, once beaming is able to convey the non-verbal communication that people value, reducing the need for businessmen to jet around the world.

The cinema experience could also be "augmented". In Aldous Huxley's science fiction classic Brave New World characters enjoy the "feelies" - films that thrill with sensations of touch and smell as well as sound and vision. Beaming might one day deliver something comparable. And imagine what erotic movies could do with that.

There are many other areas where the technology has obvious applications.

Beaming sessions could help military morale by giving soldiers based overseas a sense of being back home with their loved ones. The same would apply to workers or businessmen posted abroad.

A virtual doctor could visit a patient at home, if that patient is unable to travel to the surgery.

Read the rest here:
http://www.bbc.co.uk/news/world-europe-17905533
Microsoft kicks Chinese company out of vulnerability sharing program

After an investigation into the embarrassing proof-of-concept leak, Microsoft said MAPP partner Hangzhou DPTech Technologies breached the strict non-disclosure agreement.

Ryan Naraine, May 3, 2012

Microsoft has kicked a Chinese security company out of its MAPP vulnerability information sharing program following a recent leak of proof-of-concept code for a serious security hole in all versions of Windows.

Microsoft identified the company as Hangzhou DPTech Technologies Co., Ltd, a Chinese outfit that describes itself as a “high-tech company integrating research and development, manufacturing and sales in the network security industry.”

After an investigation into the embarrassing proof-of-concept leak, Microsoft said Hangzhou DPTech Technologies breached the strict non-disclosure agreement that is meant to ensure that sensitive information doesn’t fall into the wrong hands.

“Microsoft takes breaches of our NDAs very seriously and has removed this partner from the MAPP Program,” according to Yunsun Wee, director, Microsoft Trustworthy Computing.

Starting this month, Wee said Microsoft will strengthen existing controls and and take actions to better protect the MAPP information.

“We believe that these enhancements will better protect our information, while furthering customer protection by aiding partners developing active protections,” she said.

Microsoft did not elaborate on the new controls. A separate blog post on Microsoft’s eco-strat blog provides a detailed overview of MAPP and outlines that the benefits of the program outweighs the occasional information leakage problem.

Ever since MAPP launched in August 2008, there have been at least three confirmed leaks that included the publication of proof-of-concept code snippets on Chinese-language web sites. Microsoft previously suspended an unidentified Chinese security vendor from the program but there remains a legitimate risk that technical details of high-risk vulnerabilities could reach cybercriminals before Windows users get a change to apply security patches.

MAPP data given to security vendors ahead of Patch Tuesday includes:

- A detailed technical write-up on the vulnerability;
- A step-by-step process that they can follow to parse an affected file format, or network protocol, that identifies which elements need to have particular values, or exceed specific boundaries, in order to trigger the security vulnerability;
- Information on how to detect the vulnerability, or exploitation thereof (e.g. event log entries, or stack traces);
- A Proof-of-Concept file that is in itself not malicious, but contains the specific condition that will trigger the vulnerability. Partners can leverage this file to test detection signatures they develop using the step-by-step process we provide.


DoD broadens cyber info-sharing with industry

The Pentagon’s pilot program for sharing cyber-threat information with its key vendors has worked so well that it’s expanding to many more companies in the defense game, according to an announcement Friday.

“The expansion of voluntary information sharing between the department and the defense industrial base represents an important step forward in our ability to catch up with widespread cyber threats,” said the statement from Deputy Defense Secretary Ash Carter. “Increased dependence on Internet solutions have exposed sensitive but unclassified information stored on corporate systems to malicious probes, theft, and attacks. This expanded partnership between DoD and the defense industrial base will help reduce the risk of intrusions on our systems.”

DoD’s announcement does not make clear whether there’s a limit to the number of firms that can join the cyber-info-sharing arrangement, which grew from an initial class of some 20 companies, but maybe that’s the point: Defense officials want to help as many vendors as possible protect their trade secrets, given the rampant pillaging we’re always hearing about from China and Russia.

To make it easier, the Pentagon has set up a website through which companies can apply to join the “Defense Industrial Base Cyber Security/Information Assurance” program, provided they have the right kind of systems and already handle some DoD information. From what defense officials have said in the past, the idea is that DoD and its contractors share information about the kinds of probes and attacks they’re seeing, to make it easier to defend against them. Although no one can actually say what they mean in the cyber world, the coded message in the past has been that the Pentagon mostly defends itself well, but that its vendors are getting robbed blind, which is why everyone needed to team up.

Read the rest here: http://www.dodbuzz.com/2012/05/11/dod-broadens-cyber-info-sharing-with-industry/
Chapter Meetings

<table>
<thead>
<tr>
<th>Date</th>
<th>Time</th>
<th>Location</th>
</tr>
</thead>
<tbody>
<tr>
<td>Jun 20</td>
<td>11:00 to 1:00</td>
<td>Bambino's Italian Eatery and Sports Bar, 2849 East Platte Avenue, Colorado Springs, (719) 6308121</td>
</tr>
<tr>
<td>Jul 18</td>
<td>11:00 to 1:00</td>
<td>Bambino's</td>
</tr>
<tr>
<td>Aug 15</td>
<td>5:30 to 7:30</td>
<td>Bambino's</td>
</tr>
<tr>
<td>Sep 19</td>
<td>11:00 to 1:00</td>
<td>Bambino's</td>
</tr>
<tr>
<td>Oct 17</td>
<td>5:30 to 7:30</td>
<td>Bambino's</td>
</tr>
<tr>
<td>Nov 14</td>
<td>5:30 to 7:30</td>
<td>Bambino's</td>
</tr>
<tr>
<td>Dec TBD</td>
<td>11:00 to 1:00</td>
<td>Carrabba’s North</td>
</tr>
</tbody>
</table>

Training

- **Security+**... June 9, and September 8
- **CISSP**... June 16, and 30; July 14 and 28
- **(ISC)2 Exam**... 18 August at CTU

Upcoming ISSA Events

- **Aug 1-2**, Wednesday and Thursday, Crowne Plaza Hotel (CSTC)
- **Oct 24-26**, Wednesday through Friday, Disney Hotel, Anaheim, ISSA Annual Conference
- **Nov Conference**, **Friday, Nov 16**, Crowne Plaza Hotel, 7:30 – 5:00
The Information Systems Security Association (ISSA)® is a not-for-profit, international organization of information security professionals and practitioners. It provides educational forums, publications, and peer interaction opportunities that enhance the knowledge, skill, and professional growth of its members.

The primary goal of the ISSA is to promote management practices that will ensure the confidentiality, integrity, and availability of information resources. The ISSA facilitates interaction and education to create a more successful environment for global information systems security and for the professionals involved. Members include practitioners at all levels of the security field in a broad range of industries such as communications, education, healthcare, manufacturing, financial, and government.

Article for the

Are you a budding journalist? Do you have something that the Colorado Springs ISSA community should know about? Can you interview one of the “movers and shakers”? Tell us about it!

We are always looking for articles that may be of interest to the broader Colorado Springs security community.

Send your article ideas to Don Creamer at doncreamer@q.com or william.creamer.ctr@us.af.mil

Ensure that “Newsletter” is in the subject line.

Looking forward to seeing you in print!

Are Hackers Watching You?

May 15, Wired – Popular surveillance cameras open to hackers, researcher says. Three of the most popular brands of closed-circuit surveillance cameras are sold with remote Internet access enabled by default, and with weak password security — a classic recipe for security failure that could allow hackers to remotely tap into the video feeds, according to new research. The cameras, used by banks, retailers, hotels, hospitals, and corporations, are often configured insecurely — thanks to these manufacturer default settings, said a senior security engineer at Gotham Digital Science. As a result, he says, attackers can seize control of systems to view live footage, archived footage, or control the direction and zoom of adjustable cameras. The researcher and his team were able to view footage as part of penetration tests they conducted for clients to uncover security vulnerabilities. Source:

http://www.wired.com/threatlevel/2012/05/cctv-hack/