The cyber security threat to businesses and data is much worse than most believe. Having recently started a business I now speak to a lot of business owners about cyber security. Unfortunately, a lot of the comments I hear are, “Oh, I have good security because I have anti-virus and a good password”; or, “I don’t click on emails from people I don’t know”; and the best, “The computer company that set up my network and installed security told me I am secure and won’t get hacked.”

Really? I think I have a bridge for sale.

So, how bad is it? Well, consider who has been hacked: Google, JP Morgan, Zappos, CIA, the Pentagon, RSA, and the list goes on and on. I recently read an article that stated banks are bleeding money. Think about this: these are companies and organizations with really, really good security; and they got hacked. They also monitor their networks very closely. So what does this say about the little guy who never looks at their audit logs? They have probably been compromised and don’t even know it. Still not convinced? Consider these facts and statistics:

Organized crime has now gotten into the hacking business because it is so profitable. A stolen credit card number used to go for about $200. You can now get 1000 credit card numbers for $100 because hackers did not anticipate being able to steal so many. Hackers are setting up an underground search engine for other hackers to find tools and support. Hackers are selling and leasing their botnets. After complaints from some buying hacker tools that the tools were not being supported and updated, some groups have begun leasing and providing tech support for tools. Sophos and McAfee claim they see 150,000 and 66,000 new malware a day, respectively. Your anti-virus software is only as effective as the last known malware for which a signature has been pushed out.

So, the bottom line is the hackers, whether teenage kids, organized crime, terrorist groups, hacktivists, or others, have upped the ante. Hacking has become big business. It is incumbent upon us to make the public aware of the true extent of the threat. Here are some quick tips: do not do banking on your smart or cell phone; when banking online make sure the bank window is the only one open and the bar to the left of the URL is green; use a proxy like Hotspot when using public WiFi like in coffee shops, airports, hotels, etc.; finally, encrypt, encrypt, encrypt.

David Willson
Attorney at Law, CISSP, Security + Vice-President ISSA-COS
The Hacker is Watching

Every online scam begins more or less the same—a random e-mail, a sketchy attachment. But every so often, a new type of hacker comes along. Someone who rewrites the rules, not just the code. He secretly burrows his way into your hard drive, then into your life. Is he following your every move?

By David Kushner

"Do you want to see something scary?"

It was a Saturday night, not much happening in her Long Beach, California, neighborhood, so high school senior Melissa Young was home messing around on her computer. Her little sister, Suzy, was doing the same thing down the hall. The house was quiet, save the keyboard tapping in the girls’ rooms, when the odd little instant message popped up on Melissa's screen—an IM from Suzy. Attached to the note was a file labeled simply SCARY.

Melissa wondered why her goof-off sister was IM'ing from the next room instead of just padding over—she wasn't usually that lazy—so she walked over to see what was up. Suzy just shrugged. She had no idea what her sister was talking about. Yeah, the IM had come from her account, but she hadn't sent it. Honest.

That night, Suzy's 20-year-old friend Nila Westwood got the same note, the same attachment. Unlike Melissa, she opened it, expecting, say, a video of some guy stapling his lip to his chin on YouTube. She waited. Nothing. When she called her friend to see what she'd missed, things actually got freaky: Suzy'd never sent a thing. She panicked.

That night, Suzy's 20-year-old friend Nila Westwood got the same note, the same attachment. Unlike Melissa, she opened it, expecting, say, a video of some guy stapling his lip to his chin on YouTube. She waited. Nothing. When she called her friend to see what she'd missed, things actually got freaky: Suzy'd never sent a thing. She panicked.

Amy decided to call the cops herself. But the instant she phoned the dispatcher, a message chimed on her screen. It was from the hacker. ‘I know you just called the police,’ he wrote.

She panicked.

Every ubiquitous camera becomes, the less we're aware they're even there. They stare out at us blankly from our phones and laptops, our Xboxes and iPads, a billion eyes and ears just waiting to be turned on. But what if they were switched on—by someone else—when you least expected it? How would you feel, how would you behave, if the devices that surround your life were suddenly turned against you?

Read the rest here: http://www.gq.com/news-politics/newsmakers/201201/luis-mijangos-hacker-webcam-virus-internet#ixzz1jfEHdyQx
Congratulations!

ISSA Fellows

Betty Pierce, Melody Wilson and Glenn York have become our newest ISSA Fellows!

ISSA Senior Members

Jason Andress, George Danny Brown, Mark D. Heinrich, Paul E. Kernan, Hummer D. Marchand, Carl W. Spray, Frank E. Swanson, Cindy Thornburg, Nigel E. Webb, and Timothy D. Westland are our newest ISSA Senior Members!

Looking Elsewhere?

Based on discussions at one of the luncheons we would like to see if there is enough interest in having a half day workshop on

"Finding Your Next Job".

It would cover resumes, interviewing, networking and negotiating an offer. Please shoot me a email if you're interested; if we have enough folks respond we will set up a date. Steve Winterfeld - winterfeldsj@gmail.com
Nobody asked me, but...

There is a curmudgeon in all of us at one time or another. This space is for you who have something that is Information Assurance (IA) related, and it really sticks in your craw. Please keep your statements IA focused. Ensure that it may be of interest to the whole ISSA-COS community if possible. If the Editor feels that an article may be in a grey area vis-à-vis these ground rules, it will be taken to the ISSA-COS board for adjudication.

Jealousy is an Ugly Thing

I must admit that periodically I am jealous. It is a character fault that I am not proud of, but it’s there. There may be times when you feel the same way.

What am I jealous about? The respect that is afforded our physical security counterparts.

Most of our co-workers who are not in IA understand why there are physical security measures taken in their facility. They understand that there is a reason why money is locked up at night, why many of us are required to wear identification badges, why there may be security guards watching the facility. They understand why the Police patrol the city and the Sheriff’s Deputies patrol the County. They get that.

Many of these co-workers will also look at us as if we have just declared our birthplace is the planet Neptune if we tell them that they can’t download just any software that they like onto their work computer. They don’t get it when we tell them not to bring in software from home and load it onto their machines. They don’t get it when they are told to use relatively lengthy, somewhat complicated passwords.

And too often their managers actually support them!

Late last year after going through three rounds of interviews for an IA management position I asked that my name be taken out of consideration. There was nothing about the goals of the organization that I disliked; in fact their goals are quite admirable. Unfortunately, though, it became clear to me that if I took that position (assuming that it was going to be quite admirable. Unfortunately, though, it became clear to me that if I took that position (assuming that it was going to be offered to me) that I would spend much of my time in battles with other managers over the implementation of reasonable IA security measures.

This past summer was spent teaching Security+ at Keesler Air Force Base in Biloxi, Mississippi. My students were both Active Duty and civilian Air Force personnel. On the first day of class as part of my introduction to my students I would inform them that “I am paid to be paranoid.”

These students needed to understand that I take all of this quite seriously. Teaching it was not just a “summer job” for me. It’s my chosen career.

Is education the problem? No, I don’t believe so. Within the government world employees are required to take the IA training annually. Yes, they view it as a pain; heck, sometimes I view it as a pain! But it’s necessary, and everyone does it. But it doesn’t answer the question, “What does this mean to me?”

Many years ago I lead a vulnerability assessment (Blue Team) of a major corporation’s division under the direction of the corporate headquarters. The attitude at the facility was “We’re just one happy family.” Within 30 minutes of being given minimal privileges on their network we essentially owned all their systems.

When I paid the division’s President a courtesy visit and let him know what we had been able to accomplish, he had the attitude that there was no real problem. Well, we had managed to acquire his personal password. When I repeated that password to him, I had his attention. He knew at that point that if that password got out, he would be in serious trouble.

There is something else at work here. When was the last time you saw someone punished for violating IA rules? Last month? Last year? Ever? It is a rare event, and usually carried out quietly, discreetly, so that no one is embarrassed.

Additionally, too often IA rules are pushed aside for convenience sake. Too many times we have been viewed as the people who are “keeping us from getting our work done.” “This system would run so much better if we didn’t have to worry with this IA stuff,” etc., etc. If you have ever been associated with a vulnerability assessment or a penetration test (Red Team) you know that if anything at all happens on the system or network that may be out of the ordinary during those tests, the Test Team is immediately blamed. That generally reflects a lack of respect. Why? We have no real power!

There is a quotation that I have carried with me from office to office for many years. In the November 2006 Information Security magazine Marcus Ranum said, “We need federal IT security regulation that reads as if it were written by Napoleon Bonaparte and enforced by Vlad the Impaler, not ‘What, me worry?’ Alfred E. Newman.”

Well, that is not going to happen anytime soon. So, what do we do in the mean time? Regardless as to what your business is (national defense, a not-for-profit, etc.) you must show a business case for what you are proposing. Then and only then will you have the support of those who hand out the money, and they will ensure that what you represent includes teeth.

Now, what are your thoughts?

Don Creamer
Newsletter Editor
Latest attack against Wireless Routers

By Erik Hjelmstad, ISSA Colorado Springs

Presented at the January ISSA-COS Meeting.

Attacks against wireless access points are not new. Since wireless devices have been around, attackers have tried to gain unauthorized access to them. A new attack against wireless routers was disclosed last month, targeting routers that have WPS as a built-in option.

What is WPS?

Wifi Protected Setup (WPS) was designed to make it easier to connect wireless devices to wireless access points. WPS works by allowing the user to enter in an 8 digit PIN number that requests the WPA or WPA2 to be sent to the requesting device. This makes it easier to setup the encryption on these devices versus the alternative of having to know the exact WPA key (which could be ‘S0meTh1ng\3rYKoMPl3x’). Less security savvy users will find this method easier than having to remember that long key.

Why is this news now?

Two independent researchers discovered an attack that is better than brute force against routers that implement WPS. The flaw is in the way the router responds to incorrect PIN requests. By guessing PINs, it is possible to guess the correct pin in less than 10 hours. Lots of routers that have been sold in the last few years have this functionality including D-Link, NetGear, Linksys, Belkin, Buffalo, and ZyXel.

How does the attack work?

The attack works by guessing random 4 digit numbers, using a set pattern for digits 5-7, and computing the checksum. If the EAP-NACK is returned after the first 4 digits are sent, then the first 4 digits were incorrect. If the EAP-NACK is not returned until after all 8 digits have been sent, then the first 4 digits were correct and we can move to the second phase of the attack, namely guessing digits 5-7. This means that instead of $10^8 = 100,000,000$ different WPS keys there are only $10^4 + 10^3 = 11,000$ different keys that need to be attempted. On average, half that many would be attempted to correctly guess the WPS key.

For example, if the correct pin is 12345678, guessing 11111111 will return EAP-NACK after first 4 bytes sent. Guessing 12344444 returns EAP-NACK does not return until after all 8 bytes are sent. If we can make a guess and get a response every 3 seconds, then our attack should take $11,000 / 20 / 60 = 9$ hours 10 minutes for worst case scenario, and 4 minutes 35 minutes on average.

My results

There are two proof of concept programs available, Wpscrack by Stefan Viehböck and Reaver by Craig Heffner. I was able to get reaver to run on BT5R1 (BackTrack 5 Release 1) with a minimal amount of configuration. Once running, my router did not disable WPS after any number of attempts (others may do this to prevent a brute force attack.) My times to crack were 8:56, 8:57, 6:16, and 2:33, for an average of 6:40.

Theoretical attack

If you could get 5 systems running BT5 and each making an attempt every 3 seconds, then you should get the first half in $10,000/5/20/60 = 1:40$ and the second half in $1,000/5/20 = 10$ minutes. The average time would be half of that (~55 minutes).

Conclusions and recommendations

If you are not using WPS, disable it if you can. This should be simple to find on most routers, but there are some routers that there is no way to disable this feature. If you are using the feature, disable it unless you are actively connecting a new system to your router, and manually enable and disable this feature when you need to.

Hopefully, this will prevent an intruder from gaining access to your wireless router, until the next attack is discovered.

Sources:

Whitepaper on the attack by Stefan Viehböck: http://sviehb.files.wordpress.com/2011/12/viehbocket_wps.pdf


Reaver on code.google.com: http://code.google.com/p/reaver-wps/
In the current issue of The ISSA Journal our chapter Vice-President Dave Willson has an article that you might find very interesting. Many times we have been asked if it is legal to “hack back” against those who have hacked us. Dave presents a case where it just may be legal to do so. You may agree, or you may disagree. Regardless, check it out.

In the February ISSA Journal—One of our Very Own!

Hacking Back in Self-Defense: Is It Legal? Should It Be?

By David L. Willson – ISSA member, Colorado Springs, USA Chapter article originally published 1/17/2011 by Global Knowledge Training LLC, reprinted with permission.

The author argues that when plagued with a persistent bot, you can legally use automated code outside of your network, in specific circumstances and via specific means, to eliminate the threat in an act of self-defense or defense of property.

Your business has been hacked, leaving you with a persistent bot; now what?

Legal Disclaimer: The following theory is just that, a theory, and in no manner constitutes legal advice, nor should it provide justification for hacking back.

Okay, here it is: when plagued with a persistent bot, you can legally use automated code outside of your network, in specific circumstances and via specific means, to eliminate the threat in an act of self-defense or defense of property.

I don’t need to regurgitate numerous statistics to prove hackers seem to have an upper hand these days, but consider this: of 500+ companies surveyed, 90% admit being hacked with an average loss of $500,000 and higher. Most cybersecurity experts agree that getting hacked is no longer a matter of if, but when. One hundred percent security is a myth. So what can you do? Standard responses are slow and, in many cases, not very effective. Nation states can legally defend themselves but what about businesses?

A losing battle — Defending against the botnet

The presumption is that a business cannot reach outside its network in self-defense to block an attacker. I disagree! I am not advocating vigilante activity, but we are losing the war in cyberspace and must rethink our strategy and law. You must take control of your money and too many secrets are walking out the door unchecked. We need to open a dialogue and move the conversation down the road for better responses, solutions, and laws.

My focus in the botnet piece currently appears to pass the larger threat with millions of infected machines around the world being used to attack networks. Computers and networks are being infected through a variety of methods: phishing attacks, malware on legitimate and fake websites, employees visiting social media sites, and other methods. In 2003 and the first half of 2011, the top four botnets were:

<table>
<thead>
<tr>
<th>Top Botnets 2010 and First Half of 2011</th>
<th>2010</th>
<th>2011 (First Half)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Echo (BoltBot/Kitt)</td>
<td>60.2</td>
<td>46.4</td>
</tr>
<tr>
<td>Reepin (Mini/Spider)</td>
<td>41.9</td>
<td>33.8</td>
</tr>
<tr>
<td>Band/Deuce</td>
<td>28.3</td>
<td>23.9</td>
</tr>
<tr>
<td>Dream (Hulk/Jester)</td>
<td>27.4</td>
<td>21.2</td>
</tr>
<tr>
<td>Herd/Heretic</td>
<td>17.5</td>
<td>15.9</td>
</tr>
</tbody>
</table>

Current responses to these threats are to detect, block, clean up, and move on. Dealing with a bot in your network can be like getting your kids to clean their room. It takes a lot of work and a day later it is a mess again. What if, once dis
Defenses Against Hackers Are Like the Maginot Line, NSA Chief Says


U.S. companies still aren’t taking the threat of computer attacks seriously enough, despite a recent string of high-profile security failures, top government cybersecurity officials said this week.

“We need to become more active in our defense,” said General Keith Alexander, the director of the National Security Agency, on Thursday at the Federal Bureau of Investigation’s International Conference on Cyber Security.

Gen. Alexander compared current business defenses to the Maginot Line, the French fortifications built after World War I that failed miserably once Germany attacked in World War II. “We put up a defensive perimeter and then we wait,” said the general, who is also commander of the U.S. Cyber Command.

Instead of waiting, he said, companies and Internet providers should be actively scanning for “signatures” that might indicate new types of attacks and should then share these with others who could be affected.

Gen. Alexander and others at the conference said attacks were becoming more prevalent. They pointed to a string of well publicized attacks beginning with the hacking of NASDAQ systems in October 2010 and including the compromise of companies such as Sony and security firm RSA last year.

“People ask, ‘What’s wrong with these guys?’” Gen. Alexander said. “Actually, they’re the gold standard for securing cyber. They’re the ones that know they’ve been hacked.” Often, he said, government investigators will find that companies have been victims for many months and haven’t noticed.

In spite of a steady drumbeat of stories about such attacks, “people still ignore the threat,” said Shawn Henry, executive assistant director of the FBI. “They don’t see this risk,” he said.

Mr. Henry said there is a misconception that only e-commerce and banking companies are vulnerable to attacks but that the real danger now comes from theft of internal information such as personal data, research and development or intellectual property.

But the problem doesn’t lie only with the potential victims, speakers said. Rob Joyce, deputy director of the information assurance directorate of the NSA, said it needs to be easier for companies to protect themselves without devoting huge amount of staff to the task.

“Eighty percent of the compromises can be thwarted by basic blocking and tackling,” he said. “Automation is the only way we close the 80% threat.”

Source:

Upcoming ISSA Events

Mar 22, Thursday, Crowne Plaza (Conference), 7:30 – 5:00
May 16-17, Wednesday and Thursday, CISO Conference (Denver)
Aug 1-2, Wednesday and Thursday, Crowne Plaza (CSTC)
Oct 24-26, Wednesday through Friday, Disney Hotel, Anaheim, ISSA Annual Conference
Nov Conference, Date and location to be determined, 7:30 – 5:00
January 23, Wired – (International) I spy your company’s boardroom. Researchers from Rapid7 discovered they could remotely infiltrate conference rooms in some of the top venture capital and law firms across the country, as well as pharmaceutical and oil companies and even the boardroom of Goldman Sachs — all by calling in to unsecured videoconferencing systems they found by doing a scan of the Internet. One of the researchers found he was able to listen in on meetings, remotely steer a camera around rooms, as well as zoom in on items to discern paint flecks on a wall or read proprietary information on documents. Despite the fact the most expensive systems offer encryption, password protection, and the ability to lock down the movement of cameras, the researchers found administrators were setting them up outside firewalls and failing to configure security features to keep out intruders. Some systems, for example, were set up to automatically accept inbound calls so users did not need to press an “accept” button when a caller dialed into a videoconference, opening the way for anyone to call in and eavesdrop. Using a program the researchers wrote, they found the conference rooms by scanning the Internet for videoconference systems set up outside firewalls and configured to automatically answer calls. In less than 2 hours, they found systems installed in 5,000 conference rooms, including an attorney-inmate meeting room at a prison, an operating room at a university medical center, and a venture capital company where prospects were pitching their companies while laying out their financial details on a screen in the room. Companies sometimes set up systems outside firewalls so other companies can easily call into the videoconferencing system without having to set up complex, but safer configurations. As a result, the researchers found they could easily hijack systems, and also access systems they otherwise could not find through an Internet scan. Source: http://www.wired.com/threatlevel/2012/01/videoconferencing-hijacked/

February 08, DFI News—Steganography and Smart Phones. Over the course of the past year, a new crop of data hiding and steganography programs have emerged. These new Apps run on Android, iOS, and Windows mobile platforms. As one would expect, the ability to conceal, hide, and protect private information on smart mobile platforms is essential. In addition to the obvious benefits of protecting confidential information, there is a need for the ability to communicate covertly using these devices. Whether, this is benign communication between friends, insiders leaking company secrets, insider trading information, or communication between criminals, these new Apps provide mechanisms that enable covert information sharing. From a corporate, legal, investigative, or law enforcement perspective, being aware of this capability and being able to identify these Apps and the resulting covert communications is, of course, essential. Source: http://www.dfinews.com/article/steganography-and-smart-phones

January 17, Reuters – (International) Symantec says hackers stole source code in 2006. Symantec Corp. said a 2006 breach led to the theft of the source code to its flagship Norton security software, reversing its previous position that it had not been hacked. The world’s biggest maker of security software previously said hackers stole the code from a third party, but corrected that statement January 17 after an investigation found Symantec’s own networks were infiltrated. The unknown hackers obtained the source code to Norton Antivirus Corporate Edition, Norton Internet Security, Norton Utilities, Norton GoBack, and pcAnywhere, a Symantec spokesman said. The week of January 9, the hackers released the code to a 2006 version of Norton Utilities and said they planned to release code to its antivirus software January 17. It was unclear why the source code was being released 6 years after the theft. The spokesman said the 2006 attack presented no threat to customers using the most recent versions of Symantec’s software. Yet, an analyst with ITIC who helps companies evaluate security software, said Symantec’s customers should be concerned about the potential for hackers to use the stolen source code to figure out how to defeat some protections in Symantec’s software. Symantec said earlier in January its own network was not breached when the source code was taken. However, the spokesman said January 17 an investigation into the matter revealed the company’s networks were compromised. He also said customers of pcAnywhere, a program that facilitates remote access of PCs, may face “a slightly increased security risk” as a result of the exposure. Source: http://www.reuters.com/article/2012/01/17/us-symantec-hackers-idUSTRE80G1DX20120117
Reporting Illegal Activity

The Department of Homeland Security (DHS) and the FBI encourages reporting information concerning suspicious or criminal activity to the local FBI Joint Terrorism Task Force and the State and Major Urban Area Fusion Centers.

The FBI’s 24/7 Strategic Information and Operations Center can be reached by telephone number 202-323-3300 or by email at SIOC@ic.fbi.gov.

The DHS National Operations Center (NOC) can be reached by telephone at (202) 282-9685 or by email at NOC.Fusion@dhs.gov. FBI regional phone numbers can be found online at http://www.fbi.gov/contact/fo/fo.htm and Fusion Center information may be obtained at http://www.dhs.gov/files/resources/editorial_0306.shtm.

For information affecting the private sector and critical infrastructure, contact the National Infrastructure Coordinating Center (NICC), a sub-element of the NOC. The NICC can be reached by telephone at (202) 282-9201 or by email at NICC@dhs.gov.

When available, each report submitted should include the date, time, location, type of activity, number of people and type of equipment used for the activity, the name of the submitting company or organization, and a designated point of contact.

Chapter Meetings

<table>
<thead>
<tr>
<th>Date</th>
<th>Time</th>
<th>Location</th>
</tr>
</thead>
<tbody>
<tr>
<td>Feb 22</td>
<td>5:30 to 7:30</td>
<td>Bambino's Italian Eatery and Sports Bar, 2849 East Platte Avenue, Colorado Springs, 719) 630-8121</td>
</tr>
<tr>
<td>Mar 14</td>
<td>5:30 to 7:30</td>
<td>Bambino's</td>
</tr>
<tr>
<td>Apr 18</td>
<td>11:00 to 1:00</td>
<td>Bambino's</td>
</tr>
<tr>
<td>May 23</td>
<td>5:30 to 7:30</td>
<td>Bambino's</td>
</tr>
<tr>
<td>Jun 20</td>
<td>11:00 to 1:00</td>
<td>Bambino's</td>
</tr>
<tr>
<td>Jul 8</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>TBD</td>
</tr>
</tbody>
</table>

**SAVE THE DATE:** Thursday, March 22, 2012— the March 2012 Conference, Crown Plaza Hotel, Colorado Springs,
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 Newsletter?
If you would like to submit an article...

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!

Bluetooth + Fashion = Novero

*The Gadgeteer*, 13 May 2010: Novero has announced the Victoria Collection, a line of contemporary Bluetooth earpieces that double as jewelry. These Bluetooth headsets are designed to be worn as a necklace and are constructed with precious metals and gems. I recently reviewed their TalkyOne Bluetooth speakerphone, which I’m continuing to use because it works well and I like the look of it. But I don’t think I could ever see myself wearing a headset as a necklace though. I guess I’m just not that fashionable They have styles for men and women – any guys out there think they would be willing to wear one? Source: [http://the-gadgeteer.com/2010/05/13/bluetooth-fashionnovero/](http://the-gadgeteer.com/2010/05/13/bluetooth-fashionnovero/)