

Re: Internet security on "hotspots"

## Re: Internet security on "hotspots"

---

*Source:* <http://www.derkeiler.com/Mailing-Lists/securityfocus/focus-ms/2006-04/msg00088.html>

---

- *From:* James Harless <[jharless@xxxxxxxxxxxxxxxxxxxxxx](mailto:jharless@xxxxxxxxxxxxxxxxxxxxxx)>
  - *Date:* Thu, 20 Apr 2006 10:02:46 -0500
- 

I agree with everything you said. Also, I suppose my 'dangerous to assume' wasn't a complete thought. Basically, if I told a user 'only do important things via HTTPS'....I would assume they are incapable of following those instructions to a degree with which I would feel safe.

I hope that clears it up. I didn't intend to put words into Andy's mouth with my writing.

--

James Harless  
Network Security Engineer

Kidwell Companies  
kCOM kE kTECH  
900 S. 26th Street  
Lincoln, NE 68510

13336 Industrial Road  
Suite 101  
Omaha, NE 68137

Main: 402-475-9151  
Fax: 402-475-9186  
[jharless@xxxxxxxxxxxxxxxxxxxxxx](mailto:jharless@xxxxxxxxxxxxxxxxxxxxxx)  
[www.kidwellcompanies.com](http://www.kidwellcompanies.com/) <<http://www.kidwellcompanies.com/>>

On 4/20/06 9:34 AM, "mcclenbw@xxxxxxxxxxxx" <[mcclenbw@xxxxxxxxxxxx](mailto:mcclenbw@xxxxxxxxxxxx)> wrote:

I reread Andy's post, and I don't see the he was assuming 'she's only visiting HTTPS sites so, she doesn't need encryption'. He stated if that was the case, then a VPN wasn't needed. If it's not the case, use a VPN. Although, probably not a likely case I agree.

You are correct to not underestimate the value of leaked information and I would point out that not even a VPN, a firewall, HTTPS, etc. can

Re: Internet security on "hotspots"

protect her 100%. Set aside all the data encryption for a minute and all that other stuff us geeks always migrate to when as about security and focus on her physical surroundings. If I'm sitting in Panera and the guy behind me can see everything on my screen, and perhaps what I type, no amount of encryption and/or tunneling is going to help. And yes there are people out there that can read keystrokes as you type in your password.

Just a reminder that your data is not the only thing in the public when using hotspots. You are in public as well. Be sure no one is "looking over your shoulder." Social engineering is just as big a threat. Although personally I think in this case it's more like "stalking engineering"...

Brady McClenon  
Systems Administrator  
State University College at Oneonta

-----Original Message-----

From: James Harless [<mailto:jharless@xxxxxxxxxxxxxxxxxxxxxx>]

Sent: Thursday, April 20, 2006 9:27 AM

To: Andy.Kitzke@xxxxxxxxxxxxxxxxxx; focus-ms@xxxxxxxxxxxxxxxxxxxx

Subject: Re: Internet security on "hotspots"

Personal firewalls had already been covered by many posts including the Original Poster. I didn't see any need to reiterate that since the post asked for 'other ideas or thoughts'. I assume that everything mentioned is in addition to a personal firewall.

Also, it's dangerous to assume that 'she's only visiting HTTPS sites so, she doesn't need encryption'. Are you sure? Is she going to check/send email? POP3? SMTP? Is there anything I, as an attacker, can gain by learning her email address/password + the fact that she visits [www.herpersonalbank.com](http://www.herpersonalbank.com)? Can I do anything with that information? What if I also learn the email addresses of trusted senders? What if she fires up SSH to her home? Is her username the same as her email address, per chance? A lot of users will use the same or similar passwords, even.

I would never underestimate the value of 'leaked' information. Potential attackers would even be sizing her up as a target based on how she dresses and the type of tech she's carrying.

---

Re: Internet security on "hotspots"

James Harless  
Network Security Engineer

Kidwell Companies  
kCOM kE kTECH  
900 S. 26th Street  
Lincoln, NE 68510

13336 Industrial Road  
Suite 101  
Omaha, NE 68137

Main: 402-475-9151  
Fax: 402-475-9186  
jharless@xxxxxxxxxxxxxxxxxxxxx  
www.kidwellcompanies.com <<http://www.kidwellcompanies.com/>>

On 4/19/06 12:38 PM, "Andy.Kitzke@xxxxxxxxxxxxxxxxxxxxx"  
<Andy.Kitzke@xxxxxxxxxxxxxxxxxxxxx> wrote:

A VPN would work well for keeping her traffic safe but if  
her laptop

wasn't safe then the VPN would be moot. I think using a  
VPN is  
complicating the situation beyond what the user maybe was

looking for.

The two places to secure would be the end node and the  
traffic in  
between. The traffic could be secured by a VPN, but that

would still

leave the end node vulnerable to attack. I think with the

amount of

threats currently in the wild, browsing the internet without a  
personal firewall can be a dangerous venture.

If she's looking for the most secure approach I would say a  
personal

Re: Internet security on "hotspots"

firewall and a VPN connection to a trusted source. If she is just looking for machine security I think a personal firewall would be plenty. I would steer towards a firewall with good reviews

that looks

at more than just ports, like IE requests and such. If she

used SSL

sites anytime she was divulging personal information her

traffic would

be encrypted and there wouldn't really be a need for a VPN.

Andy Kitzke  
Network Engineer  
In-Sink-Erator

-----Original Message-----

From: James Harless  
[mailto:jharless@xxxxxxxxxxxxxxxxxxxxxx]  
Sent: Wednesday, April 19, 2006 8:53 AM  
To: focus-ms@xxxxxxxxxxxxxxxxxxxxxx  
Subject: Re: Internet security on "hotspots"

Have her connect to a VPN that is available to her. If her company doesn't have one available, there are many easy to

implement solutions

for setting up a PPTP VPN. Then, she can connect to an insecure Wireless AP but, all of her traffic would flow encrypted to the VPN and out to the 'net from that remote location.

-----  
-----  
-----  
-----

Re: Internet security on "hotspots"

