Interested in learning more about security?

SANS Institute
InfoSec Reading Room

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

The Importance of Social Engineering for the Home Internet User

This paper discusses the necessity for educating home Internet users, recommending several areas of improvement that will help home users understand the need for securing their systems.

Copyright SANS Institute
Author Retains Full Rights

AD

The Importance of Social Engineering for the Home Internet User

Ron Dean
July 16, 2001
SANS Security Essentials GSEC Practical Assignment (Version 1.2c)

"Our high-speed broadband service makes the Internet so responsive, it's just like changing channels."[1] Great! How do I sign up? Speaking of channel surfing let me see what's on television right now. Hey, it's that new game show with the quick-witted English woman proclaiming, "You are the weakest link." Funny, that still makes me grin when she says that to somebody. Wait a minute, what if she is correct? Are we really the weakest link on the Internet? Is it possible that my spiffy new broadband Internet connection is providing easy access to my computer's processing resources as well my data to some hacker? Somehow that woman's assertion no longer seems so amusing.

The truth is, humans are often the weakest link when it comes to computer security. After reading through several articles on network security as well as attending training classes on the subject it has been made apparent that education (i.e. Social Engineering) of the users is every bit as important as the equipment put in place for protection. This being the case, why does it seem that education of the home Internet user is not a priority?

In this paper I will discuss the necessity for the education of home Internet users. In addition, I will recommend several areas of improvement that will help home users understand the need for securing their systems.

An Informal Poll

In order to get a feeling for the relative computer security of home Internet users I took an informal poll. Twenty people with different levels of computer experience from several fields of work responded to my poll. Twelve questions were asked which are listed below as well as their responses.

Do you consider your home PC resources/data to be of value?	**Yes** 90%	**No** 10%
Do you consider your home PC resources/data to be of value to a hacker?	**Yes** 40%	**No** 60%
Does your Internet Service Provider provide a security guideline for protection from attacks?	**Yes** 10%	**No** 90%
Do you disconnect/shutdown your internet connection when it is not in use? *	**Yes** 40%	**No** 60%
What type of internet connection do you have (broadband or dial-up)?	**Broadband** 65%	**Dial-up** 35%
Do you download software from the internet?	**Yes** 100%	**No** 0%

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

Do you have anti-virus software?				**Yes** 100%	**No** 0%
Is your connection to the internet behind a firewall? **				**Yes** 60%	**No** 40%
Are you using an intrusion detection system?				**Yes** 20%	**No** 80%
How often do you update your anti-virus software?	**Daily** 15%	**Weekly** 40%	**Monthly** 20%	**Yearly** 10%	**Never** 15%
How often do you check for Operating System updates?	**Daily** 15%	**Weekly** 15%	**Monthly** 35%	**Yearly** 5%	**Never** 30%
How often do you check for Application updates?	**Daily** 0%	**Weekly** 10%	**Monthly** 50%	**Yearly** 0%	**Never** 40%

* 85% of the broadband subscribers do not disable their Internet connection when not in use.
** 70% of the broadband subscribers use a firewall.

It is quite clear that the overwhelming majority of respondents believe their PC resources/data are of value and protect them with anti-virus software. However, the majority does not consider these same resources valuable to a hacker.

But, I have anti-virus software…

The concern with the integrity and availability of one's personal data is well founded. After all, computer viruses, Trojans, and worms are now headline news. It was hard to avoid hearing about Melissa, the Love Bug, or a handful of other 'high profile' computer viruses/Trojans/worms that were unleashed in the past couple of years. Fortunately, anti-virus software that is updated on a regular basis will provide protection from many of the known viruses and Trojans. From my informal poll it appears that most home Internet users have gotten the picture and update their anti-virus software on a regular basis.

Nevertheless, the best defense is a layered defense. This means that it is imperative for the home user to not only protect themselves through hardware/software solutions but also understand that their actions on the Internet could have serious consequences. Admittedly, that are several resources on the Internet where one can read about solutions for protecting themselves through security patches, anti-virus software, and firewalls. However, many home Internet users are not aware of a security guideline that they should follow.

Where does the responsibility reside?

The question with perhaps the most interesting and overwhelming response asks about security policy. In particular, does an individual's Internet Service Provider have a security guideline for the subscribers to follow? Ninety percent of the respondents stated that their ISP does not provide such a guideline. Is it truly possible that a company providing a service does not also supply a guide for

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

their subscribers to follow or, are the users not concerned enough to find out? I investigated three of the more popular ISPs in the area to find out if the problem lies with the ISP or the subscribers.

First, I scrutinized @Home's web site because of their large customer base and their popularity with the respondents of my poll. Two clicks were all that was required to pull up the On-Line Security Statement[2]. This page proved quite informative by providing a step-by-step guide to disabling file sharing for Macintosh computers as well as PCs running Windows 9x. In addition, there is also a section discussing the importance of running and updating anti-virus software. On the other hand, there was no mention of the value of installing/using a personal firewall or ensuring that operating systems as well as applications are updated with the most recent security patches. As a side note, @Home states that the filters within their cable modems provide some packet filtering capabilities. After asking some subscribers that also use a personal firewall about these capabilities I found that the modems do not block typical information gathering attempts such as port scans.

The second broadband ISP that I investigated was Road Runner. The closest thing I could find to a security guideline was located in their Frequently Asked Questions (FAQ)[3] section. Road Runner, like @Home, also recommends disabling file and printer sharing. There is no step-by-step procedure provided for this task but, they state the installation technician will perform this during the initial setup. In addition, Road Runner states that their modems are designed to "prevent the interception of data packets that any user sends or receives" [3]. There was no mention of using updated anti-virus software, checking for security patches for operating system and applications, or using personal firewalls.

The final ISP that I explored was Earthlink. Earthlink provides dial-up access across the country as well as DSL service in limited areas. I was unable to locate a security guideline that listed steps for the subscribers to take to secure their Internet connection but their web site[4] provides a link to Symantec's site for a free security scan. If the user opts to participate, a scan for vulnerabilities is run against your IP address and the results are displayed as well as a recommendation for how to increase your security with help from their software. This is probably the most user friendly way to encourage subscribers to add anti-virus and firewall software to their configuration. This alone goes a long way but there is no mention of checking for operating system or application updates on a regular basis.

Overall, it appears that the larger ISPs are taking some responsibility by providing a basic guideline or an interactive tool for helping to increase the security of their subscriber's resources. However, there is plenty of room for improvement.

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

It would be unfair to levy all the responsibility on the ISPs. As I mentioned before, popular media has made computer viruses headline news in the past couple of years. The question is, have they made overall home computer security as large of an issue? The answer is no, but, this may be changing as well. I searched the web sites of the New York Times and Time magazine to see if there were any articles about home Internet security. These searches turned up several applicable articles ranging from 'How Tos' for increasing your Internet security at home to tales of being attacked. A subscription is required to read the full articles from the New York Times but the titles of some of the available articles are included in the additional reading section. Direct links to the Time articles are provided in the additional reading section as well.

It is interesting to note that only forty percent of the respondents to my poll believe that they have data or resources that are valuable to a hacker. Of those forty percent the majority had either been the target of malicious activity in the past or have a background in network security. The message is out there it's just getting the users to pay attention.

Dial-up/Broadband Users…Lend Me Your Ear.

During my research I have gathered that most home Internet users are aware of many of the concepts of network security. A simple search for the keywords "network security" will provide the user with a wealth of information. The results of my informal poll clearly indicate that users consider their data/resources to be of value and protect themselves with anti-virus software. The problem is getting people to understand that not only are they at risk for loss of data but could also be used as a resource to attack others. It has been my experience that most users are willing to be good 'Internet neighbors' as long as it does not impede on their Internet enjoyment. Many home Internet users will make an effort to secure their systems provided that the steps are easy to find, easy to understand, and presented in a user friendly format. It also helps to offer the information in more than one format such as a web site and in printed documentation. I have listed some recommendations for ISPs on how to heighten the awareness of the home Internet user.

- Include a security checklist in the 'Welcome' packages.
- Provide a link to vendors of anti-virus software and personal firewall vendors during the sign-up process for an ISP.
- Direct users to visit web sites such as the Gibson Research Foundation or Symantec that provide an on-line security check so they understand their vulnerabilities.
- Inform people that network security is not just for large corporations anymore. Many of the same basic rules and precautions apply in the home.

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

Making the Internet Safe by Securing Our 'Neighbors'

The majority of the aforementioned recommendations are fairly straightforward with the exception of the security checklist for 'Welcome' packages. So, what should a checklist provided by an ISP include? First of all, it should clearly indicate that although the ISP attempts to provide a safe and secure connection there is always the possibility for those safeguards to be compromised. Second, the checklist should be easy to follow and have step-by-step instructions where applicable. I have created an example of such a checklist that illustrates my points. I have omitted the step-by-step configurations in the interest of brevity.

Welcome to XYZ Internet Service!

We here at XYZ Internet Service would like to ensure our customers that we make every effort to protect the safety and security of our subscribers. However, like the locks on you front door, there are individuals with malicious intent that may defeat these safeguards leaving your computer's security in jeopardy. That is why we recommend that all of our customers take a moment to step through our Security Guideline to make certain they are protected. Like preparing for an outing in the cold the best defense is provided by layers of protection. Please ensure that all the points below are addressed the first time you log-on.

- Install anti-virus software on each computer that will be using your Internet connection.
- Update your anti-virus definitions on a regular basis. We recommend that you have your anti-virus software check for updates on a weekly basis.
- Check to see if you have the latest security patches for your Operating System and Applications. These are generally available from the vendor's web site.
- Make sure file extensions are visible.
- Install a personal firewall such as Zonealarm, BlackICE Defender, Norton Personal Firewall, or McAfee Personal Firewall.

Other Recommendations from XYZ Internet Service

- Check for Operating System security patches on a regular basis. We recommend that you check for security patches on a weekly basis (this may be an automated process for some systems).
- Check for security patches for your applications on a regular basis.
- Remove applications that you no longer use.
- Do not download software unless it is from a trusted site.
- Scan software that you download with your anti-virus software before use.

(Continued on next page)

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

- Disable your Internet connection when it is not in use. Dial-up subscribers should ensure that the auto-answer feature of their modems are disabled.
- Do not open attachments, even from colleagues, without scanning them for viruses.
- Use encryption when transmitting data that you consider sensitive.

A simple checklist with the aforementioned points would go a long way in providing new users guidelines to protect themselves from data loss as well as making them less likely to have their resources used in an attack.

Conclusion

Even with the overwhelming information available for securing one's home computer from attack/unauthorized use a number of individuals are not taking the necessary steps to secure their resources. It is imperative to demonstrate to the home user that they do provide a resource that many hackers target. Individuals with broadband access provide a particularly tempting resource for these same hackers. It seems that it is merely a matter of time before they are scanned and then potentially attacked or used to attack others. If the basic precautions that were outlined above were taken by each subscriber it would be much more difficult for an attacker to round up the resources they require in order to pull off an attack. In order for this to happen home Internet users must understand that they are not only at risk themselves but they may actually pose a risk to others. If ISPs were to take some of the steps outlined in the previous sections of this paper I believe more of their subscribers would take the steps to secure their systems.

References

1. "Clear your mind. Experience @Home."
   URL: http://www.@home.com/index_flash.html (16 July 2001)
2. "@Home – Online security statement"
   URL: http://www.@home.com/security.html (16 July 2001)
3. "\[Welcome to ROAD RUNNER\]"
   URL: http://rrcorp.central.rr.com/hso/faq.asp (16 July 2001)
4. "Free Security Check™"
   URL: http://www.earthlink.com/home/tools/freescan/index.html (16 July 2001)
5. Lo, Joseph. "Trojan Horse Attacks." 4 June 2000.
   URL: http://www.irchelp.org/irchelp/security/trojan.html (16 July 2001)
6. Lo, Joseph. "Trojan Horse or Virus?" 6 May 2000.
   URL: http://www.irchelp.org/irchelp/security/trojanterms.html (16 July 2001)

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

Additional Reading

1. Jackson, David; Locke, Laura; Shannon, Elaine. "Time.com – Internet Insecurity." URL: http://www.time.com/time/covers/1101010702/index6.html (16 July 2001)
2. "Time.com – Internet Insecurity. Protect Yourself: 10 Ways to more secure cybersafety." URL: http://www.time.com/time/covers/1101010702/tips.html (16 July 2001)
3. Hutsko, Joe. "BASICS; Safe Online at Home: Keeping Out Uninvited Guests." 19 April 2001. URL: http://www.nytimes.com/pages/technology/index.html (search under firewalls, 16 July 2001)
4. Austen, Ian. "Higher-Speed Lines Leave Door Ajar for Hackers." 8 July 1999. URL: http://www.nytimes.com/pages/technology/index.html (search under firewalls, 16 July 2001)

Additional Resources

1. Gibson Research Foundation: URL: http://grc.com/default.htm (16 July 2001)

© SANS Institute 2001, Author retains full rights.

Last Updated: May 24th, 2013

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

SANS Malaysia @ MCMC 2013	Cyberjaya, MY	Jun 03, 2013 - Jun 08, 2013	Live Event
SANS Pen Test Berlin 2013	Berlin, DE	Jun 03, 2013 - Jun 08, 2013	Live Event
Industial Control Systems Security Training - Houston	Houston, TXUS	Jun 10, 2013 - Jun 15, 2013	Live Event
Security Impact of IPv6 Summit 2013	Washington, DCUS	Jun 14, 2013 - Jun 16, 2013	Live Event
SANSFIRE 2013	Washington, DCUS	Jun 14, 2013 - Jun 22, 2013	Live Event
SANS Canberra 2013	Canberra, AU	Jul 01, 2013 - Jul 13, 2013	Live Event
Digital Forensics & Incident Response Summit 2013	Austin, TXUS	Jul 09, 2013 - Jul 16, 2013	Live Event
SANS London Summer 2013	London, GB	Jul 09, 2013 - Jul 16, 2013	Live Event
SANS Rocky Mountain 2013	Denver, COUS	Jul 14, 2013 - Jul 20, 2013	Live Event
SANS Mumbai 2013	Mumbai, IN	Jul 22, 2013 - Jul 27, 2013	Live Event
SEC528 SANS Training Program for the CompTIA® New Advanced Security Practitioner (CASP) Certification	Washington, DCUS	Jul 22, 2013 - Jul 26, 2013	Live Event
SANS San Francisco 2013	San Francisco, CAUS	Jul 29, 2013 - Aug 03, 2013	Live Event
SANS SEC 560: Network Penetration Testing @ Bangalore 2013	Bangalore, IN	Aug 05, 2013 - Aug 10, 2013	Live Event
SANS Boston 2013	Boston, MAUS	Aug 05, 2013 - Aug 10, 2013	Live Event
Critical Security Controls Summit	Washington, DCUS	Aug 12, 2013 - Aug 18, 2013	Live Event
Industrial Control Systems Security Training - DC	Washington, DCUS	Aug 12, 2013 - Aug 16, 2013	Live Event
SANS Thailand 2013	Bangkok, TH	Aug 19, 2013 - Aug 31, 2013	Live Event
SANS Virginia Beach 2013	Virginia Beach, VAUS	Aug 19, 2013 - Aug 30, 2013	Live Event
Mobile Device Security Summit 2013	OnlineCAUS	May 30, 2013 - Jun 06, 2013	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced