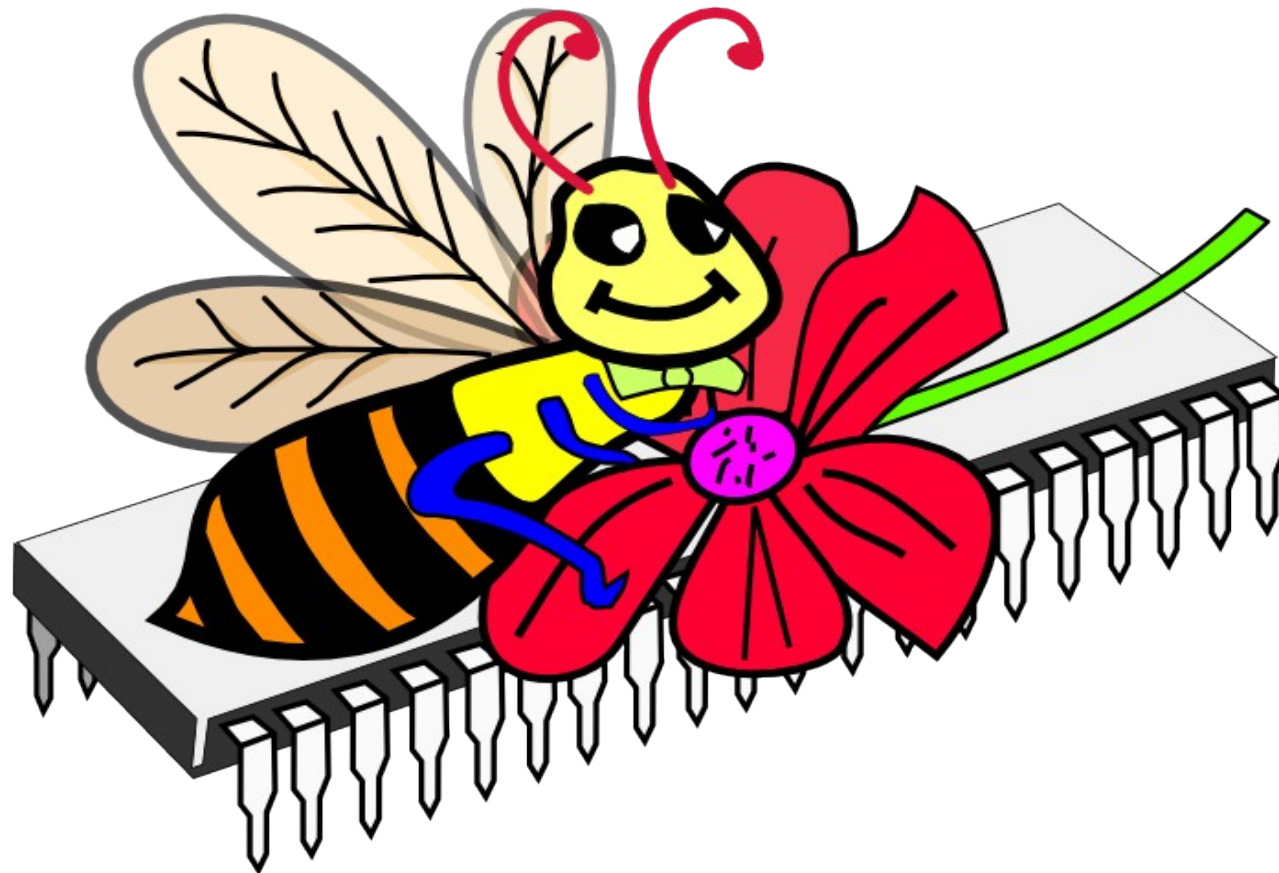


BCUG Internet Workshop 2010-10-07

Web Security and Popular Sites

By Gilbert Heaton < gilbert@heaton.net >

<http://www.bcug.com/>



Disclaimers

Information prepared for casual workshop on a quick effort basis and intended to supplement the presentation. Use at your own risk. Also some wording has been crunched down to fit the page/slides better.

BCUG is not a part of the college it happens to meet at.

Copyright 2010 by Gilbert Heaton under [Creative Commons Attribution-Noncommercial-Share Alike 3.0 Unported](http://creativecommons.org/licenses/by-nc-sa/3.0/)



Contents

Table of Contents

1 Trademarks.....	2
2 Web Security.....	3
2.1 Latest Attacks.....	3
2.2 Microsoft Patch Tuesday (2010-Jun-08).....	4
2.3 Other Security Tips From Prior Workshop.....	5
2.4 The 25 Most Common Mistakes In E-Mail Security.....	5
2.5 Custom E-Mail Addresses.....	6
3 Popular and Useful Web Sites.....	7
3.1 http://www.crazyloon.com/	7
3.2 http://webhosting.lifetips.com/	7
3.3 Redirecting Web Pages with 301.....	8
3.4 Avoid Popular HTML Mistakes.....	8
3.5 Inline Java Script Should Not Contain <tags>.....	9
4 Humor.....	11
4.1 Online Comics For Techies	11

1 Trademarks

This author has attempted to list trademarks used within this document. The names of actual companies and products mentioned herein may be the trademarks of their respective owners.

Google® and Google Maps® are registered trademark of Google Inc.

Microsoft®, Windows®, and Outlook® are registered trademarks of Microsoft Corporation. Bing, and/or other Microsoft products and services referenced herein may also be either trademarks or registered trademarks of Microsoft in the United States and/or other countries.

Mac® and Mac OS® are trademarks of Apple Inc., registered in the U.S. and other countries.

UNIX® is a registered trademark of The Open Group.

Wikipedia ® is a registered trademark of the not-for-profit Wikimedia Foundation.

2 Web Security

2.1 Latest Attacks

<http://www.zdnet.com/blog/government/beware-twitter-password-reset-messages/9050?tag=nl.e589>

Another surge of forged “password reset” notices attempting to gain your account information.

Ignoring the fact that genuine companies do not send you helpful links, at least if the company is interested in security. If you want a URL use a trusted search engine, such as Google, Yahoo!, or Bing, to search for the company name or URL. This avoids being spoofed to go to bcug.net.ru instead of bcug.com.

The true key for noticing the problem is to look at the HTML using “view source”:

`Brookdale Computer Users Group`

Be sure the address within `<a>` is exactly correct.

Any address in the bottom of the browser can not be trusted to be correct. You can believe wrong addresses are evil, but good address can be spoofed.

This is what you see on the browser's screen. Security wise it counts for nothing.

`http://www.bcug.com/`

Most phishing attempts can be spotted by playing the “what doesn't belong” game:

`Brookdale Computer Users Group`
`Brookdale Computer Users Group`
`<a href="http://www.example.com/www.bcug.com/"`
`mouseover="spoof();" >http://www.bcug.com`

“Almost spelled right” names are popular phishing bait. Foil by using search engines to find URLs.

A little “mouseover”, or other JavaScript, and you can write anything you want to the browser's status line.

Top Level Domain (TLD) is wrong, especially if it's for nation with history of cyber crime.

bcug.com is *not* in the first set of slashes.

`Brookdale CUG`

Lots of % escapes in a domain name is a red flag as they hide the real address.

`http://www.voice-from.god/`

2.2 Microsoft Patch Tuesday (2010-Jun-08)

This is a massive patch for lots of things. Including IE. Your XP should be at SP3 to keep up with security patches. Though I will be waiting awhile to install it “JIC”.

2.3 Other Security Tips From Prior Workshop

Comparison Of Web Browsers:

<http://www.bcug.com/files/Internet-2009-12WebBrowsers.doc>

2.4 The 25 Most Common Mistakes In E-Mail Security

<http://www.itsecurity.com/features/25-common-email-security-mistakes-022807/>

1. Using just one e-mail account
2. holding onto spammed-out accounts too long.
3. Not closing browsers after logging out.
4. Forgetting to delete browser caches, history, and passwords, especially on public machines.
5. Using insecure email accounts to send and receive sensitive information.
6. Forgetting the phone
7. Not using BCC

8. Being trigger happy with Reply All

9. Not stripping E-mail addresses off of forwarded E-mail.

See article for more points, and full details.

2.5 Custom E-Mail Addresses

If you pay for a subscription, some E-mail services, such as Yahoo!, allow you to create any number of aliases to your main E-mail address. In Yahoo! the addresses start with your main name, have a dot, and the alias.

No matter how the ISP allows you to set up aliases, each place you subscribe to can be given their own alias. Once your done with it you can request the sender stop sending to you then delete the alias. Once the alias is deleted you will never hear from the sender again at the now vanished E-mail address.

3 Popular and Useful Web Sites

3.1 <http://www.crazyloon.com/>

Site rich in content for those making web pages.

Dig live to interest. Some ideas of my own

- Internet >> Web Master >> Domain >> [Your Own DNS](#)

- If you are serious about your web site, getting your own domain name *server* (DNS) can be key to keeping your up time up and site features rich.

3.2 <http://webhosting.lifetips.com/>

The importance of SSL:

<http://webhosting.lifetips.com/tip/90530/website-security/website-security-tips/importance-of-ssl-website-security.html>

3.3 Redirecting Web Pages with 301

<http://www.stevenhargrove.com/redirect-web-pages/all-comments/>

3.4 Avoid Popular HTML Mistakes

When building links to cgi-bin programs with '?' arguments, avoid the common mistake:

```
http://bad.example.com/cgi/page.asp?a=1&b=2&c=hello world
```

The correct way is to use & escapes for characters to remain intact when the browser sends them to the server and % escapes for characters the server needs to process.

```
http://good.example.com/cgi/page.asp?a=1&amp;b=2&amp;c=hello%20world
```

```
http://good.example.com/cgi/page.asp?a=1&amp;b=2&amp;c=hello+world
```

In name=value pairs, both the *name and value* should be % escaped (% is followed by a two-digit hexadecimal value for the character):

- 1.If you do not control the characters in a name to assure they are “safe” alphanumeric names, then % escape the names beyond your control. Little

known fact is that “a&b%c” is a valid name. Basically escape any “trouble” characters, including space, %, +, &, <, >, ?, and =. Any character that is a metacharacter to & or % escapes or HTML tags. Good ideas include quotes and anything else in doubt. Space can be replaced with a single character “+”, which makes it necessary to % escape + signs.

2.% escape the value *separately* by the same rules.

3.Build the list of name=value pairs with & delimiters.

3.5 Inline Java Script Should Not Contain <tags>

Inline JavaScript should not contain anything that looks like HTML <tag>s of any type. Escaping the < or > with \< and \> is not sufficient.

The < and > escapes will often work, especially for text in document.write() calls.

Use \x60 or \x62 escapes for < and >, if & escapes will not work.

Or construct expressions using characters in the clear with + to obscure them:

```
var string = "<" + "h1" + ">Heading<" + "/h1" + ">";
```

4 Humor

4.1 Online Comics For Techies

Dilbert (www.dilbert.com) is just a start, but others tend to be more technical.

- *User Friendly* - <http://userfriendly.org/static/>
- *The Watering Hole* - <http://blogs.oreilly.com/wateringhole/>
- XKCD - <http://xkcd.com/>