goto; conference aarhus

DEFENSIVE PROGRAMMING

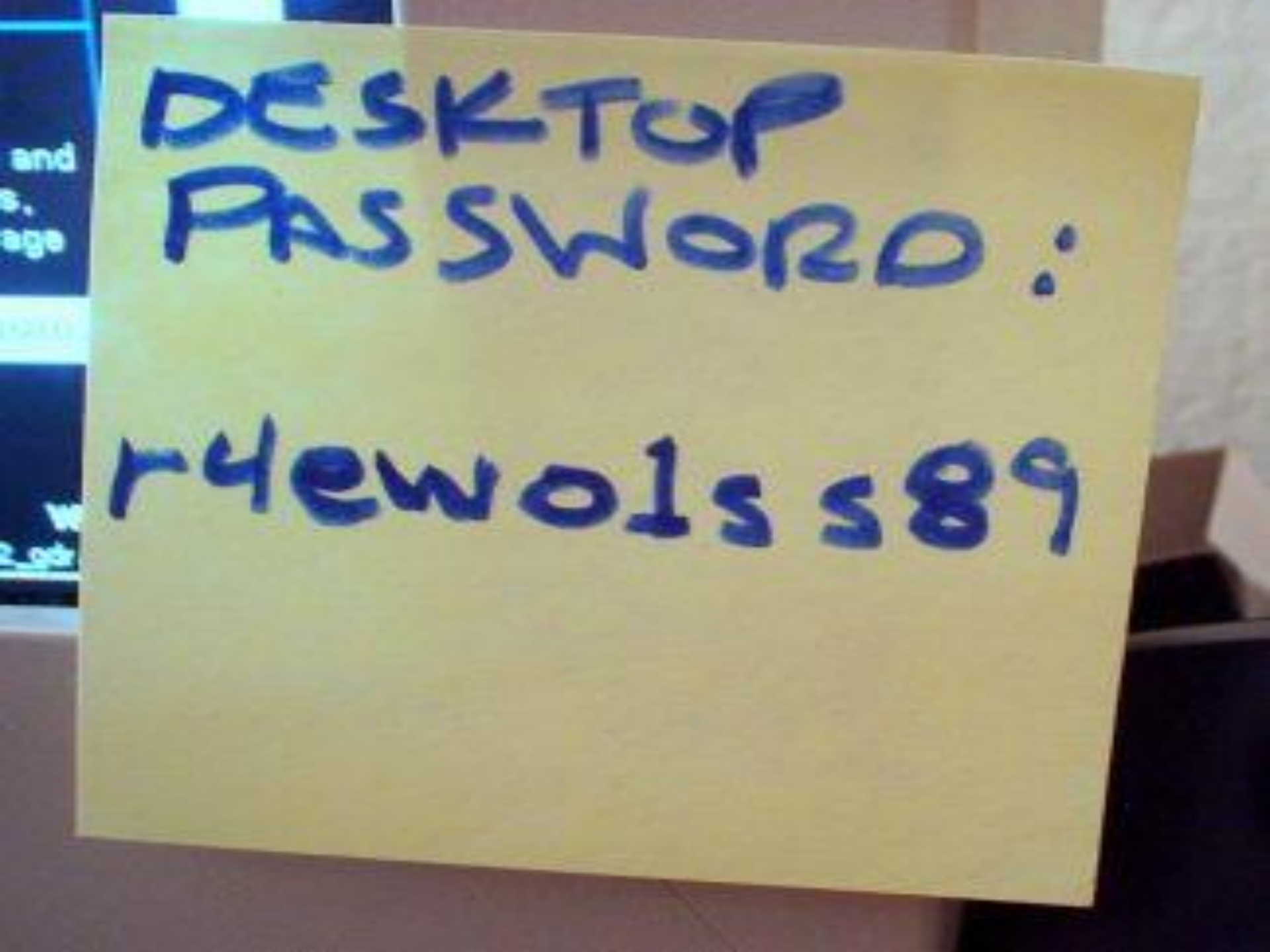
Niall Merrigan
Capgemini Norway

INTERNATIONAL SOFTWARE DEVELOPMENT CONFERENCE

gotocon.com


Security Fail
failblog.org

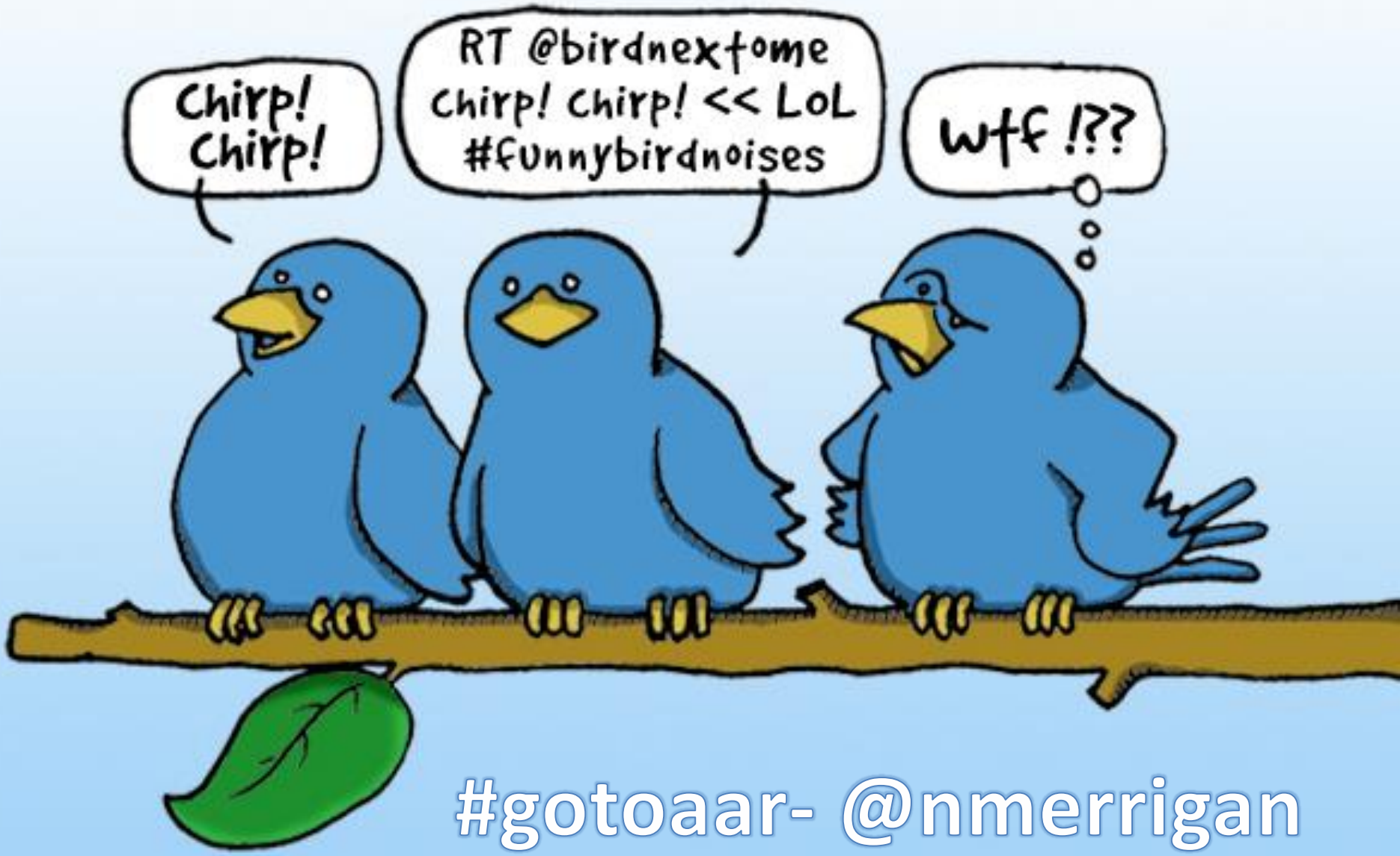

FAIL
failblog.org


DESKTOP
PASSWORD:
r4ewo1ss89


FAIL
failblog.org

Subminal message: You will love this talk and give it great marks

Defensive Programming 101



#gotoaar- @nmerrigan

HAVE YOU EVER BEEN SO DRUNK...

You Flipped A Tank?

NORWEGIAN ROAD PATROL

In Norway you don't exceed the speed limit. Ever.

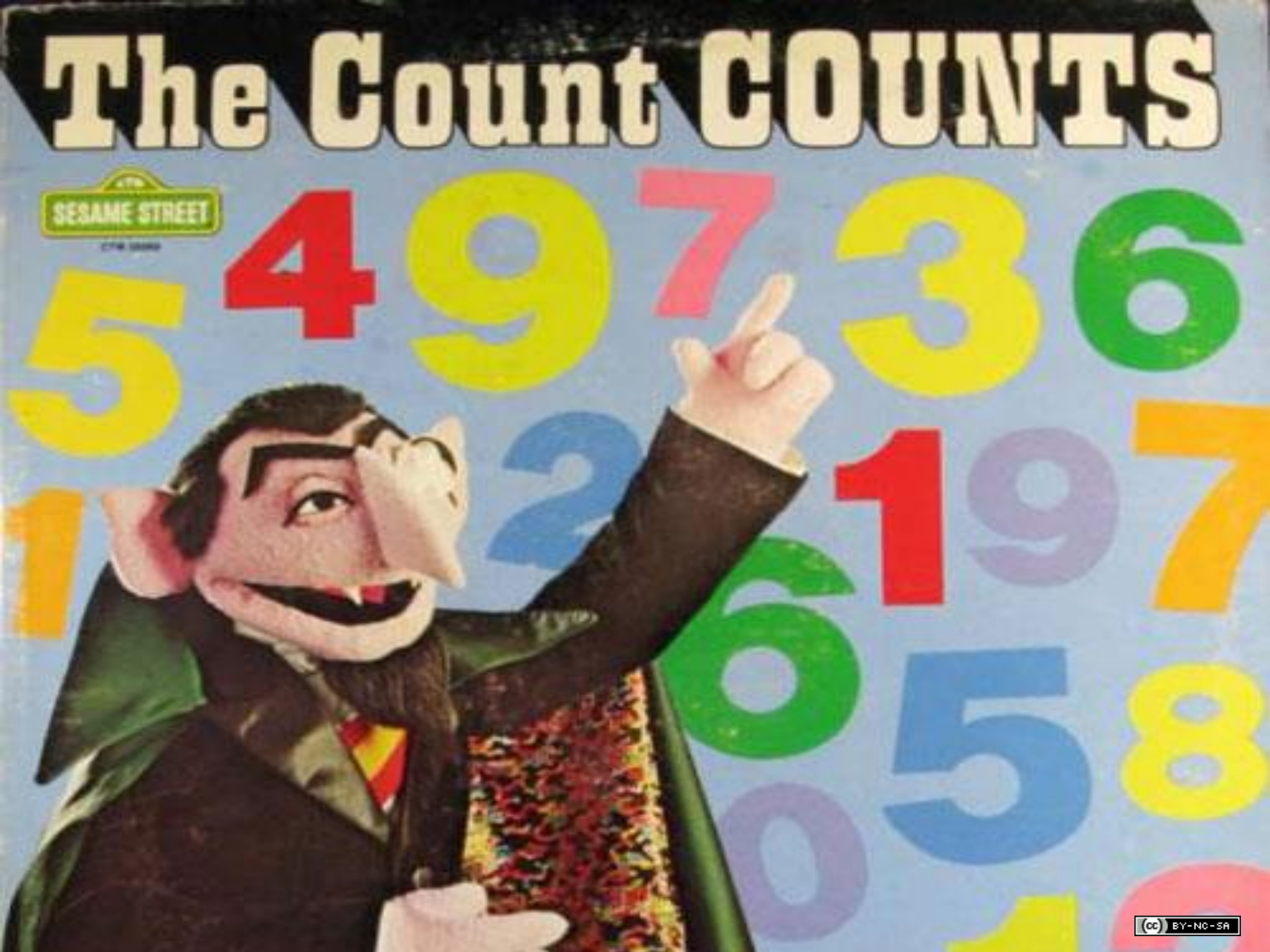
If you are reading this then your head is turned on its side and you look kinda funny


AwkwardFamilyPhotos.com

When all you have is a mallet, everything looks like Justin Bieber


If this text is too big you are sitting too close

The Count COUNTS




google it

PASSWORDS ARE LIKE UNDERWEAR

You shouldn't leave them out where people can see them.
You should change them regularly.
And you shouldn't loan them out to strangers.

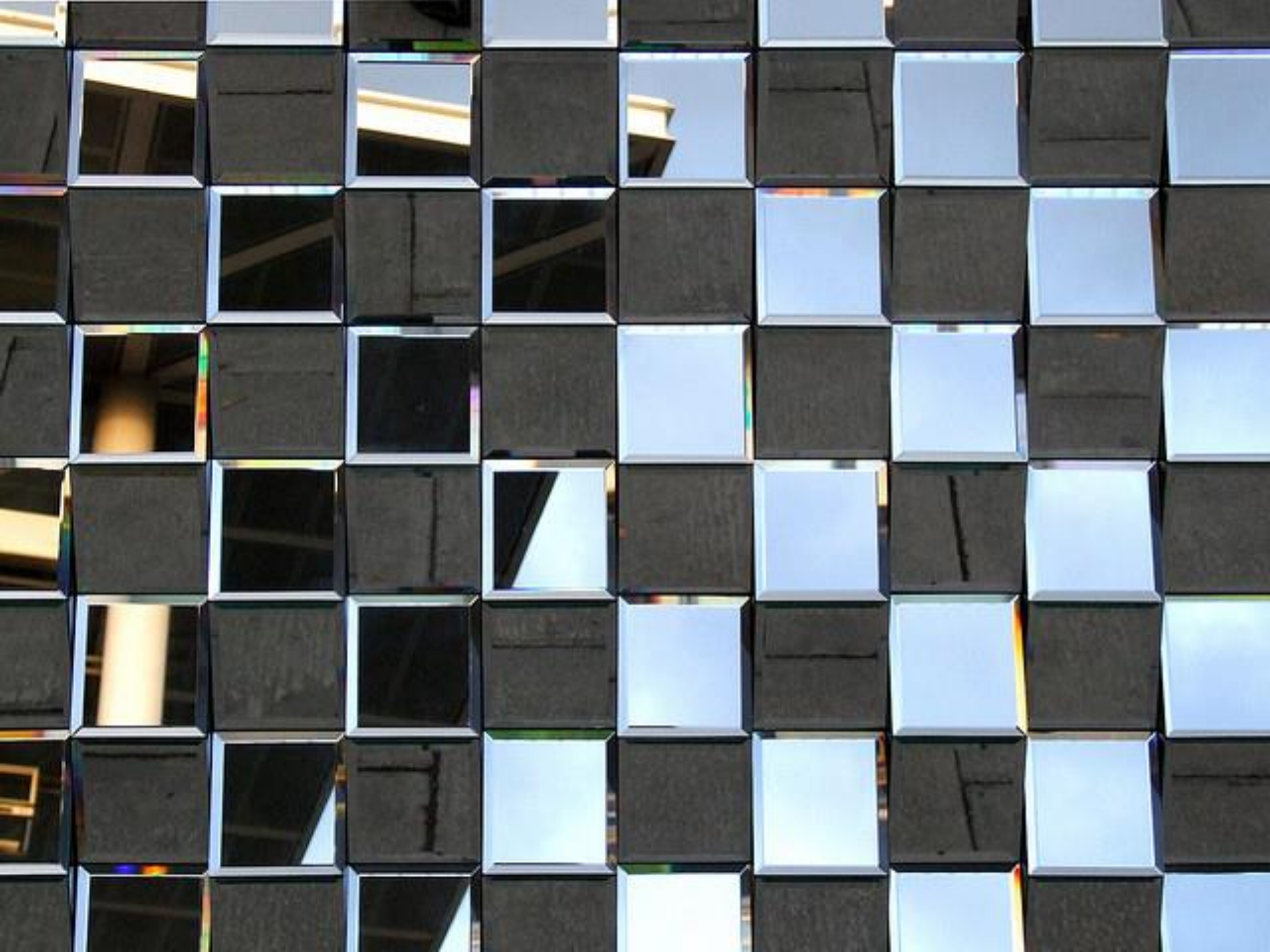
"Sorry about the odor. I have all my passwords tattooed between my toes."












BY-NC-SA


IKEA
Server Error in
'/KNBR_Prod' Application.
Unspecified error

Server Error in '/' Application.

Could not find file 'C:\clients\IMA\ima\App_Data\breadcrumb.xsl'.

Description: An unhandled exception occurred during the execution of the current web request. Please review the stack trace for more information about the error and where it originated in the code.

Exception Details: System.IO.FileNotFoundException: Could not find file 'C:\clients\IMA\ima\App_Data\breadcrumb.xsl'.

Source Error:

```
[No relevant source lines]
```

Source File: c:\WINNT\Microsoft.NET\Framework\v2.0.50727\Temporary ASP.NET Files\root\4bd08171\5720103a\App_Web_a0tt5xo5.4.cs **Line:** 0

Stack Trace:

```
[FileNotFoundException: Could not find file 'C:\clients\IMA\ima\App_Data\breadcrumb.xsl'.]
   System.IO.__Error.WinIOError(Int32 errorCode, String maybeFullPath) +2013773
   System.IO.FileStream.Init(String path, FileMode mode, FileAccess access, Int32 rights, Boolean useRights, FileShare share,
   System.IO.FileStream..ctor(String path, FileMode mode, FileAccess access, FileShare share) +114
   System.Web.UI.Control.OpenFileAndGetDependency(VirtualPath virtualPath, String physicalPath, CacheDependency& dependency)
   System.Web.UI.WebControls.Xml.LoadTransformFromSource() +273
   System.Web.UI.WebControls.Xml.Render(HtmlTextWriter output) +32
   System.Web.UI.Control.RenderControlInternal(HtmlTextWriter writer, ControlAdapter adapter) +25
   System.Web.UI.Control.RenderControl(HtmlTextWriter writer, ControlAdapter adapter) +121
   System.Web.UI.Control.RenderControl(HtmlTextWriter writer) +22
   System.Web.UI.Control.RenderChildrenInternal(HtmlTextWriter writer, ICollection children) +130
   System.Web.UI.Control.RenderChildren(HtmlTextWriter writer) +24
   System.Web.UI.Control.Render(HtmlTextWriter writer) +7
   System.Web.UI.Control.RenderControlInternal(HtmlTextWriter writer, ControlAdapter adapter) +25
   System.Web.UI.Control.RenderControl(HtmlTextWriter writer, ControlAdapter adapter) +121
   System.Web.UI.Control.RenderControl(HtmlTextWriter writer) +22
   System.Web.UI.Control.RenderChildrenInternal(HtmlTextWriter writer, ICollection children) +130
   System.Web.UI.Control.RenderChildren(HtmlTextWriter writer) +24
   System.Web.UI.HtmlControls.HtmlForm.RenderChildren(HtmlTextWriter writer) +59
   System.Web.UI.HtmlControls.HtmlForm.Render(HtmlTextWriter output) +68
   System.Web.UI.Control.RenderControlInternal(HtmlTextWriter writer, ControlAdapter adapter) +25
   System.Web.UI.Control.RenderControl(HtmlTextWriter writer, ControlAdapter adapter) +121
   System.Web.UI.HtmlControls.HtmlForm.RenderControl(HtmlTextWriter writer) +37
   ASP.ima_main_master.__Render__control1(HtmlTextWriter __w, Control parameterContainer) in c:\WINNT\Microsoft.NET\Framework
   System.Web.UI.Control.RenderChildrenInternal(HtmlTextWriter writer, ICollection children) +2068203
   System.Web.UI.Control.RenderChildren(HtmlTextWriter writer) +24
   System.Web.UI.Control.Render(HtmlTextWriter writer) +7
   System.Web.UI.Control.RenderControlInternal(HtmlTextWriter writer, ControlAdapter adapter) +25
```

DEMO

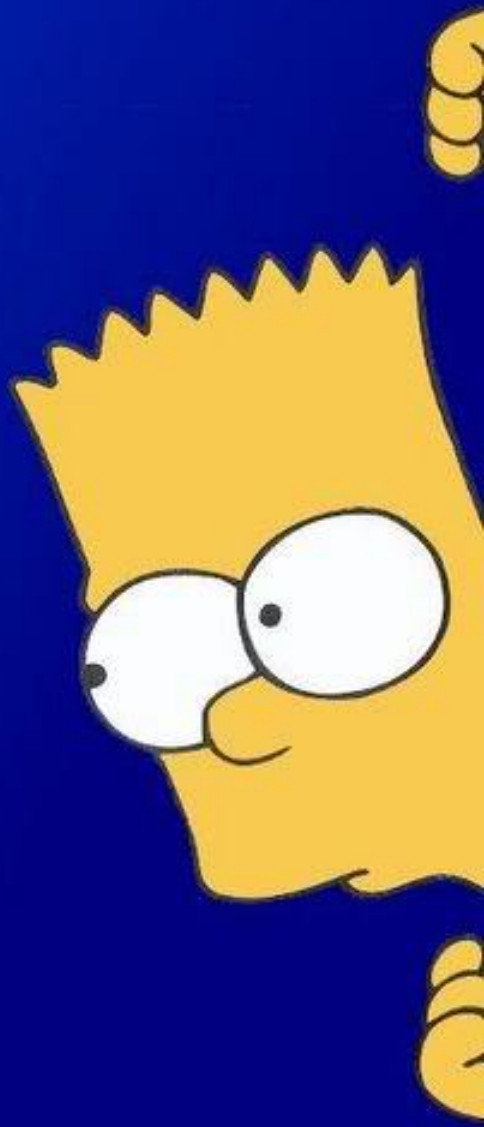
3

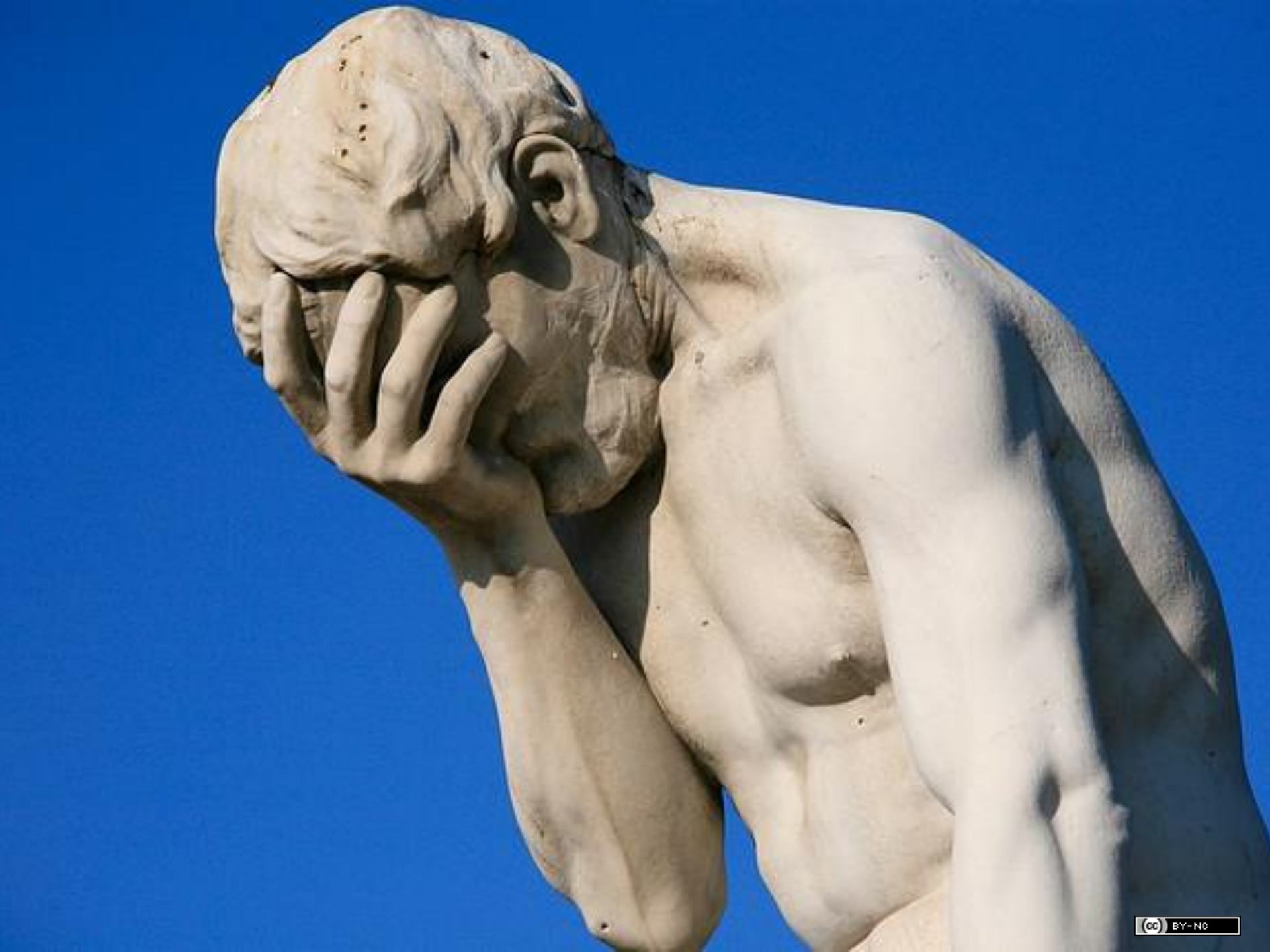
THE COOKIE MONSTER

is serious about his cookies


2
4
6

Demo





ASP.NET Resources

- OWASP Top 10 by Troy Hunt - http://www.troyhunt.com/2011/12/free-ebook-owasp-top-10-for-net.html
- Basic Security Practices for Web Applications - http://msdn.microsoft.com/en-us/library/zdh19h94(v=vs.100).aspx
- ASP.NET MVC Security - http://www.asp.net/mvc/overview/security
- Combating ClickJacking With X-Frame-Options - http://blogs.msdn.com/b/ieinternals/archive/2010/03/30/combating-clickjacking-with-x-frame-options.aspx
- AntiXSS Toolkit - http://wpl.codeplex.com/
- ASafaWeb - https://asafaweb.com/
- ASP.NET Security Wiki - http://wiki.asp.net/page.aspx/27/security/

IIS Resources

- Security Guidance for IIS - http://technet.microsoft.com/en-us/library/dd450371.aspx
- IIS Lockdown tool - http://technet.microsoft.com/en-us/library/dd450372(v=ws.10).aspx
- URLScan – http://www.iis.net/learn/extensions/working-with-urlscan
- IIS Configuring security - http://learn.iis.net/page.aspx/88/configuring-security/
- IIS Security Tools - http://www.iis.net/community/Security
- Penetration Testing Tools list - http://projects.webappsec.org/w/page/13246988/Web%20Application%20Security%20Scanner%20List

Image Credits

1. Security Fail - http://1121fail.blogspot.no/2010/01/fail.html
2. Fail - http://www.japemonster.com/funny-fails-new-selection-47-pics
3. Password - http://klaatu.anastrophe.com/index.php/2007/01/12/passwords-on-post-its-you-bet/
4. Security Fail #2 - http://www.japemonster.com/funny-fails-new-selection-47-pics
5. Highscore - Gal - http://www.flickr.com/photos/83476873@N00/4116381
6. Twitter - http://joshhealey.org/wp-content/uploads/2012/08/Twitter-funny-cartoon-birds-image.jpg
7. Tank - http://cheezburger.com/3545425664
8. Norwegian Road Patrol - http://cheezburger.com/3833542912
9. G is for Goggles - Don -http://www.flickr.com/photos/60648084@N00/2349550374
10. Family - http://www.awkwardfamilyphotos.com
11. Hacker - http://trynerdy.com/wp-content/uploads/2012/04/hacker.jpg
12. Geek Ipad - http://sfnewtech.com/wp-content/uploads/ipad-geek.jpg
13. Door Slam - http://www.reactiongifs.com/tag/door-slam/
14. [Taken in Paris (France) - 23Oct11] - philippe leroyer - http://www.flickr.com/photos/52499764@N00/6754312999
15. My favourite record - Mauricio Balvanera - http://www.flickr.com/photos/80039525@N00/491480800
16. Red 10 - darwin Bell- http://www.flickr.com/photos/53611153@N00/412631864
17. Illusion – http://www.cookdandbombd.co.uk/forums/index.php?topic=30742.120
18. Google It – Mez Love - http://www.flickr.com/photos/mezdeathhead/4533915662/
19. The Nine - Daniel Kulinski- http://www.flickr.com/photos/7729940@N06/4000276979
20. What's your password - Michael Moore - http://www.flickr.com/photos/therealmichaelmoore/6055748207/
21. Passwords are like underwear - http://thenextweb.com/shareables/2010/02/09/passwords-are-like-underwear/

Image Credits

22. Password joke - http://www.freeduh.com/2011/10/05/i-asked-my-dad-where-the-children-came-from/sorry_about_the_idor/
23. 8 Mosaic – LEOL30 - http://www.flickr.com/photos/lwr/101593950/
24. Check – http://www.flickr.com/photos/yersinia/2982093881/
25. Park 7 -Yersinia pestis - holeymoon - http://www.flickr.com/photos/81335564@N00/2004700172
26. Image, à la main, inconnu, ombre, 3456x2848 - http://xn--80aqafcrtq.cc/fr/?p=471951
27. Against the glass – http://www.fantom-xp.com/wp_23_~_Shadowgraph_desktop_backgrounds.html
28. 6 in six seconds – pshutterbug - http://www.flickr.com/photos/95565118@N00/922632392
29. IKEA YSOD - http://www.mikepope.com/blog/AddComment.aspx?blogid=1743
30. Yet Another Helpful Error - http://linkaider.com/category/hacks/
31. 5 - svenwerk- http://www.flickr.com/photos/11864250@N00/369136782
32. This is Happening without your Permission - What What - http://www.flickr.com/photos/99136715@N00/32022937
33. Quatre - Kat... - http://www.flickr.com/photos/20195637@N00/2277229055
34. Me Burns - http://newarchivist.com/2009/10/01/three-things-i-didnt-learn/
35. Three - Grant Hutchinson - http://www.flickr.com/photos/13522901@N00/59231687
36. the perfect drug - Dave Campbell - http://www.flickr.com/photos/19365001@N00/223731385
37. Cookie Monster - http://www.mobypicture.com/user/AmpleKing/view/6347653
38. Smiles and Rainbows - Pol Neiman - http://www.flickr.com/photos/37518559@N00/336380075
39. Cookie 2 – http://www.seriouseats.com/2007/07/photo-of-the-day-angry-cookie.html
40. A hit of the bubbly...– Adriane Dizon - http://www.flickr.com/photos/ev0luti0nary/7332541940/
41. Gimp in a mask.!!! - DigiTaL~NomAd - http://www.flickr.com/photos/39865537@N03/4311168437
42. Bart Hiding behind a wall - http://www.wallpaperswala.com/bart-simpson/
43. 1 - LEOL30 - http://www.flickr.com/photos/49968232@N00/305130907
44. Head in Hands - Alex Proimos - http://www.flickr.com/photos/34120957@N04/4199675334
45. I Know Who Dies! – Bart - http://www.flickr.com/photos/cayusa/891079569/

Contact

- Twitter: @nmerrigan
- Blog: http://www.certsandprogs.com
- Email – via blog

Contact Details

Resources

Twitter

Follow Me


Questions?