

No More Passwords

Why web developers should start using an OpenID based single sign-on solution for web site authentication and account creation.

By Lukas Blakk

April 13, 2009

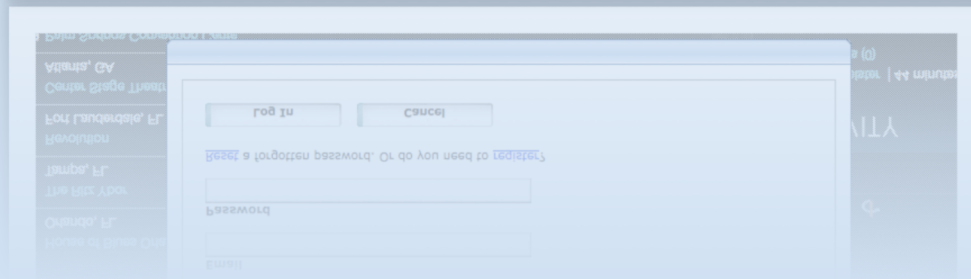
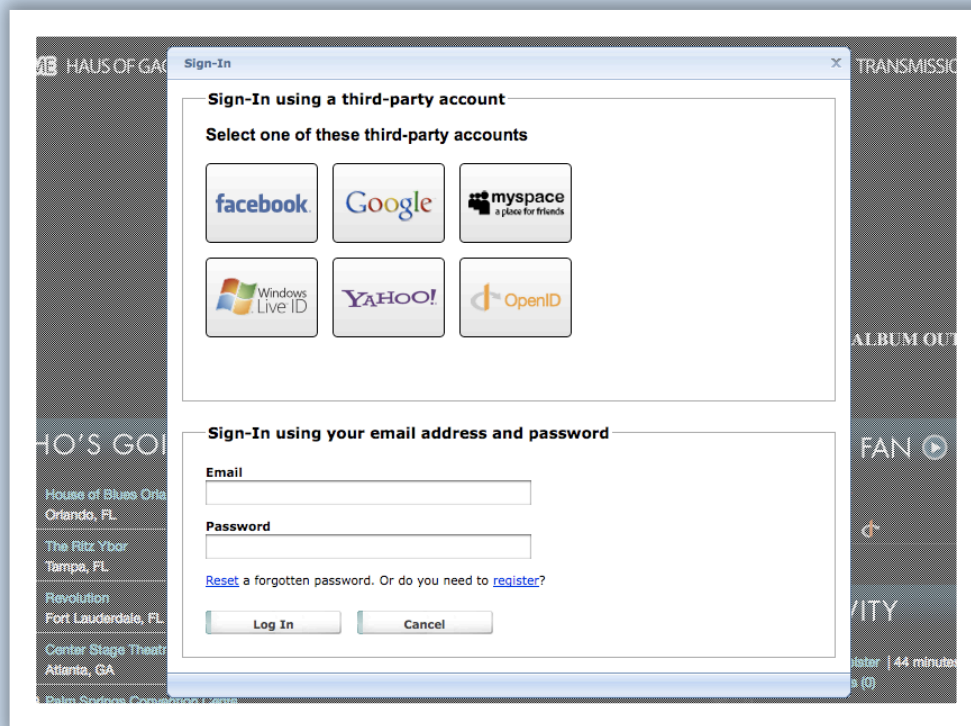


Table of Contents

TOO MANY PASSWORDS	2
"IT WON'T HAPPEN TO ME"	4
STEALING PASSWORDS MADE EASY	6
SINGLE POINT OF ACCESS	8
MICROSOFT PIONEERS	8
OPENID IS THE NEXT LEVEL	9
FACEBOOK JOINS THE MOVEMENT	10
OPENID AND USABILITY	11
OVERCOMING UI CHALLENGES	12
WHAT TO LOOK FOR IN AN OPENID SOLUTION	13
BENEFITS OF USING OPENID	15
RPX OPENID SOLUTION	15
GEFFEN SIGNS UP WITH RPX FOR 200 SITES	16
IMPLEMENT RPX AND FURTHER THE SECURE WEB	18
OPENID AND THE FUTURE OF SECURITY	18
REFERENCES	21

Too Many Passwords

Passwords are an important component to current web usage. According to a large scale study of web passwords conducted by Microsoft the average computer user has 6.5 passwords, each of which is shared across 4 different sites, along with about 25 accounts that require passwords and she types in an average of eight passwords every day. (Florencio and Cormac 2007)

The first 10 websites listed in Alexa's top 500 all require an account in order to participate fully in what the site has to offer. (Alexa the Web Information Company) Even though users can be taught how to create a strong password (length, combining symbols and cases, using a phrase) not all websites allow passwords with such features. For example, TD Bank's online banking system EasyWeb™, will not allow anything longer than 8

characters and only alphanumeric characters at that. Users are at the mercy of webmasters when it comes to the security of their online data and assets.

As the web matures SaaS (Software as a Service) and SOA (Service-Oriented Architecture) have emerged as the two most important trends (Goth 2008), the connection needed for online interactions may become more dependent on a user having a profile and history of transactions that identify them as a trustworthy netizen.

Single sign-on systems have started to catch on in the past few years as an alternative to unique accounts on individual sites. These systems can give the user a single point of control over the security of a password and lets them integrate their data and account attributes into each new site they engage with. Single sign-on providers can also allow the user to maintain a profile about themselves with a range of categories including their employment history, scholastic achievements, all the way to favourite bands and movies.

This white paper will explore the benefits of implementing a single sign-on method of authentication as it pertains to web developers.

"It won't happen to me"

This seems to be the underlying mantra to most people's approach when it comes to internet security. According to the Internet World Stats website almost 250 million people, or 73%, of North America's population is online which accounts for 17% of the world's internet population. (Internet World Stats) These users are all likely to have at least one username and password, but approximately 43% of them are remembering 5 - 9 passwords. (PasswordResearch.com)

When people have a lot to remember they develop coping mechanisms that in turn can lead to bad habits. According to a usability study 54.6% of subjects use the same password for multiple accounts "Very Frequently" or "Always" and an additional 33% use variations of that same password. (Riley 2006, 3) If this password is not secure, they are vulnerable but when it is secure, they are more likely to forget it and this costs the IT help desks of with the heavy use of recovery support.

"According to the Gartner Group, between 20% to 50% of all help desk calls are for password resets. Forrester Research states that the average help desk labor cost for a single password reset is about \$70."(Mandyllion Research Labs 2006)

Mandyllion research also provides a cost calculator to help an organization discover how much password recovery support is costing them.

It would bring peace of mind if users were at least using different (and hopefully stronger) passwords for sites with a higher level of security risk such as banking, and other online financial transaction sites like PayPal. Shannon Riley's study of 328 Wichita University undergraduate students found otherwise.

"...nearly 60% of the respondents reported that they do not vary the complexity of their passwords depending on the nature of the site and 53% indicated that they never change their password if they are not required to do so. " (Riley 2006, 5)

Many websites perpetuate this by having a variety of user creation/authentication systems in place. One site may create a username while another uses the email address as a username. One might enforce a secondary question, which the user is prompted to answer when they sign in from an IP address that is unfamiliar while another site might only allow for an alphanumeric password, which can be easily cracked with a simple dictionary or brute-force attack.

In February of 2006, Bill Gates publicly called for an end to passwords (Fried and Evers 2006) and while many others since have taken up the cause, they are still the most popular and pervasive method of account security for access to online content or use web applications and services.

Stealing Passwords Made Easy

On February 19, 2009 InformationWeek's editor Dave Berlind was duped in a phishing scam targeting Facebook users. (Berlind 2009) The link took him to a dummy site with a login page that looked just like the usual Facebook login page. Only after logging in did Berlind realize his mistake and by then his information was already in the hands of the phishers.

Berlind says he had let his guard down.

"I missed the fact that it was sent to my TechWeb address, which is not the e-mail address of record for my Facebook account. I also didn't bother to do what I usually do with links in e-mail messages (before clicking on them); I didn't mouse-over the message to double-check that the URI being displayed in the message wasn't an imposter that was masking a non-Facebook URL. As can be seen from below, it was. I also missed that once I clicked through, the URL in Firefox was pointing to <http://facesbookcom.awardspace.com>. I was asleep at the keyboard." (Berlind 2009)

Facebook's notifications always contain a link to the message on the Facebook server and the message Berlind received looked no different. However after he logged in the refreshed page asked for his password again and that was what finally tipped him off. The criminals had redirected their phishing page to the real login page. This simple middleman attack would fool most users who, after entering their password a second time and continuing to the real page, might not ever know that something was amiss.

In the fall of 2008 Vice Presidential candidate Sarah Palin's Yahoo account was hacked when someone exploited Yahoo's "forgot-my-password" service:

"The mechanism allows customers to retrieve or change their password if they can verify their identity by confirming personal information such as birthdate, postcode and the answer to a "secret question", such as a childhood pet's name or school mascot.

Palin's hacker was challenged to guess where Alaska's governor met her husband, Todd.

Palin herself recounted in her speech at the Republican National Convention that the pair began dating two decades ago in high school in Wasilla, a town near Anchorage.

"I found out later though (sic) more research that they met at high school, so I did variations of that, high, high school, eventually hit on 'Wasilla high'," the person wrote." (Moses 2008)

As these two examples demonstrate, passwords are not robust, and they are easily compromised either through phishing or the site's own password retrieval service. These are only two examples out of an immeasurable amount of daily scams and hacks on the internet. There are a number of sites dedicated to phishing specifically for PayPal and eBay account information. There are sites with forums where hacking into hotmail accounts is explained in great detail. For users who choose to use only one password for all their internet transactions, their time will come if it hasn't already. Once a hacker gets that password they will have the keys to the castle for that user's web identity.

Single Point of Access

Microsoft Pioneers

Along comes single sign-on, a new way to do authentication on the internet. It can work in several ways, and we will be looking at the “keys to the castle” style. With single sign-on there are many benefits:

- Reduce password fatigue caused by having different user name and password combinations
- Reduce the amount of insecure passwords
- Reduce IT costs, through less help desk requests about lost passwords
- Allows for open, decentralized standards to be created for authentication and access control
- Security on all levels of access to systems (entry/exit) without having to re-prompt users

The most notable pioneer of a single sign-on platform was Microsoft with their .NET Passport, the predecessor to the current Windows Live ID. Microsoft wanted Passport to be a single sign-on solution for all web commerce but due to some errors on their part, this venture was not successful. According to Michael Chaney's site, on December 24, 1999 the passport.com domain name expired and this meant that all Passport enabled sites as well as Passport users would be locked out of their accounts. (Michael Chaney) Chaney managed to make the \$35 payment on the outstanding amount and the Passport system was restored within 24 hours.

Following this, there were accusations that Microsoft's privacy agreement allowed them too much access to users' private data

and transaction information. In 2001 they adapted the privacy agreement (Olsen 2001) but soon after in 2003 another flaw came to light. In 2003 a software developer named Faisal Danka found a flaw, a simple browser exploit that allowed malicious persons to crack hotmail and therefore Passport accounts. Following these blows to its reputation, Passport had large companies like eBay and Monster.com discontinuing their support of the system and it lost all momentum. (Mittal, 2004) Windows Live ID eventually supplanted Passport in 2007 and in 2008 Windows Live ID became an OpenID provider.

OpenID is the Next Level

OpenID is a protocol created by Brad Fitzpatrick and released in 2005 as a way to offer an open, decentralized, free framework for user-centric digital identity. (OpenID) The goal of OpenID was to offer a simple way for users to carry one digital identity around with them on the internet. While not technically a single sign-on solution (since it still requires the user to sign in at each OpenID enabled site) it does give the user the option of only remembering one login. The point of OpenID is to establish identity (or many identities). Then every site you want to join can reference that identity to find out about you. How you prove that you own any one of your identities is up to you (or more likely your OpenID provider).

"OpenID takes advantage of already existing internet technology (URI, HTTP, SSL, Diffie-Hellman) and realizes that people are already creating identities for themselves whether it be at their blog, photostream, profile page, etc. With OpenID you can easily transform one of these existing URIs into an account which can be used at sites which support OpenID logins." (OpenID)

Another important aspect of OpenID is that it is completely free to use and distribute. This led to several large companies getting on board with both becoming providers of OpenID identities as well as relying parties by enabling users to authenticate with OpenIDs. Among these companies were large organizations like AOL, Microsoft, Sun, and Novell. Today it is estimated that there are over 160-million OpenID enabled URIs with nearly ten thousand sites supporting OpenID logins. (OpenID) In October of 2008 Microsoft and Google both announced plans to support OpenID with Microsoft integrating it with the LiveID platform and Google supporting any user with a Google account. (OpenID, 2008)

Facebook Joins the Movement

Facebook Connect is the newest arrival to the single sign-on implementation options. With Facebook Connect, the promise to adopters is that users will get many benefits (Facebook Connect):

- Seamlessly "connect" their Facebook account and information with your site
- Connect and find their friends who also use your site
- Share information and actions on your site with their friends on Facebook

Facebook users largely use their real identities on the site and so this trust can then be extended to the website which chooses to

enable Facebook Connect. The use of Facebook Connect is expected to widen a web of trust where all information continues to synch up to Facebook and where users can carry their social networks with them from Facebook as they venture to other sites. This two-way communication is persistent and updated regularly so that both the implementing site and Facebook keep up with a user's web activities dynamically. Facebook Connect is currently still in a fledgling state. Facebook originally stated it would launch with 24 partners, among them such well-known sites as Twitter, Digg, Hulu, CBS.com and CNET. However at the time of writing, Facebook Connect's website only displays 4 examples of the technology in action and it seems that the partners have yet to implement Facebook Connect or make it publicly available.

OpenID and Usability

In the fall of 2008 Google and Yahoo! did some usability experiments with users who were new to OpenID. In the tests they explained what OpenID would allow them to do: use one log in to multiple sites. However, once the subjects were left to the task of signing into websites 4 out of 6 still used their username/password combinations even when presented with the option of using an OpenID. Part of the confusion was that these users had trouble grasping that their Yahoo! or Google username was in fact an OpenID identity. Many of them found the user interface confusing because there was no password field. (Sachs 2008)

Yahoo! and Google both came out of the testing with a list of recommendations for improving the UX of OpenID logins as well

as some solid feedback about the process from the users' perspective. While the subjects of the research understood the benefit to them of not having to create a new account and not having to do email/password logins they felt there were still a lot of cons (Yahoo! 2008, 4):

- 3rd party site doesn't always return you to the right page
- Feels like opening a new account because it's so much work
- Might forget to log out of Yahoo!
- Fearful of global access

Overcoming UI Challenges

The challenge with all the open sign-in services at present is to get users to change their habits when it comes to creating accounts and signing in. With very few sites implementing Facebook Connect and with the confusion about how to use an OpenID URL users are not latching on to this concept as quickly as the providers might have hoped. It's very likely that at this moment almost every internet user in North America has an OpenID account but not many of them know or make use of it. It takes an extra step or two in order to log in with an OpenID because of the need to pop over to the provider to confirm the authentication before being logged in at the site where access was sought. Sometimes the user can get lost in the chasm between the relying party (RP) and the identity provider (IDP).

This seems to be changing. In a January 2009 Wired blog post, Michael Calore claims that OpenID is "...gaining a whole lot of traction in one particular area -- comments on blogs." (Calore, 2009) The speculated cause for this is due to the nature of blog comments being a transient, short transaction where multiple

logins would be too frustrating to the user. Regular blog commentators must have picked up on the ability to log in with OpenID credentials and found that to be a speedier solution. As a result most of the large and well-known blogging software providers such as TypePad, Blogger, and WordPress have integrated OpenID protocol into their code.

"Some have added support for Facebook Connect as well. These systems are being installed and used across the web with great success -- proof that OpenID can be implemented in the real world and, more importantly, understood by real users.

'[With] the exception of some larger sites, like AOL's MapQuest which integrated OpenID last year, both OpenID and Facebook Connect are seeing more rapid adoption in areas where people are used to not bothering with creating a new account,' says Six Apart open platform technical lead David Recordon in an e-mail to Wired.com." (Calore, 2009)

Facebook Connect has tackled the usability issue by designing their login box in such a way that it becomes a pop-up on the site being accessed instead of sending the user over to Facebook's page to confirm. This is a step in the right direction when it comes to keeping the user clear on what site they are trying to access and lessens the "chasm of death" (having to go to a third site to authenticate and getting lost on the return) experience OpenID is known for.

What to Look For in an OpenID Solution

Web developers looking to start integrating open authentication options into their sites have several options. It is possible to use the API for several of the OpenID providers in order to an in-house solution. This can take up a lot of a programmer's time, which

could be better spent on other areas of the site. This paper's author strongly recommends considering third party software as service option instead. This lets web developers focus on the specifics of their business and leave the open authentication implementation to the domain experts. It also lets that third part provider keep up to date on the latest changes when they arise. Most businesses are less likely to update their websites as often as these protocols might change and fluctuate. When building a site and wanting it to interface with open authentication providers you should look for several key components:

- Simple to implement and understand
- A system that will work regardless of what updates are made to OpenID protocols or what new platforms and systems are added
- Platform agnostic code with no proprietary technologies needed so that the functionality can be brought in house if need be
- A solution that takes care of security, monitoring, upgrading, uptime and scaling
- Strong interoperability with large providers such as Google, Yahoo, MySpace ID, Facebook Connect and OpenID
- An interface that is clean and encourages best practices, putting OpenID logins front and center to foster user adoption
- A user experience that is clear and requires as few clicks as possible for the user to achieve their goals

In February of 2009, Plaxo and Google did A/B testing to try a new way of using OpenID log in that only required 2 clicks from the user and was targeted specifically at Google users because of the likelihood that they were already logged in to their Google accounts. The results of their test were staggering. The biggest concern when sending the user off to confirm their OpenID identity is that the user will get lost and never return. What Plaxo's "Two-Click Signup Experiment" (McCrea 2009) found was that 92% of the users it tested returned and confirmed access to their contact

list. The other 8% chose to log in with a username and password combination instead. With these results, they realized that the impact on their business is tremendous. 17% of their customers are Google users and the 56% of their other users come from Yahoo, Microsoft and AOL. This means that 73% of their users already have OpenIDs.

Benefits of Using OpenID

There are several benefits to websites that use a third party open identification provider.

To the user:

- Keep your data with you as you travel between sites
- Less re-entering of the same basic profile information
- Bring your friends and contacts with you
- Ability to set privacy settings

To the website or business:

- Access to user data
- No need to maintain passwords for users
- No account scraping
- Happy users who have one less account to keep track of

RPX OpenID Solution

JanRain has a solution that fits all budgets and meets the criteria of what to look for when an open authentication option is desired. They have created a software as a service layer that sits between a website and the open authentication technologies.

*"...JanRain is providing a solution that solves a problem for developers - how to efficiently implement the variety of logins - and users - how to log into sites with the most familiar credential. As an added bonus, JanRain is getting OpenID out in front of the public at large, putting it in direct context with other distributed login options, and - perhaps best of all - beginning to collect data on which options users choose for their login credentials."
(Turoczy, 2008)*

JanRain has come out with their software as a service solution to open authentication interfaces with a product called RPX. RPX provides a simple interface offering login options via the larger open authentication providers (Google, MySpaceID, Facebook, OpenID, Yahoo!, and WindowsLiveID). For smaller site implementations, JanRain offers a basic service level at no cost. Where a larger website demands an enterprise level solution, JanRain has one to match and their price points are based on user numbers so that the solution can scale. Their package offers a lot of advantages to the websites who implement it, their solution:

- Is non-proprietary
- Normalizes data
- Uses existing web standards and protocols
- Is scalable
- Comes with technical support (for Plus and Pro levels)
- Promotes best practices for security

Geffen Signs Up With RPX for 200 Sites

In December of 2008 Interscope Geffen A&M implemented JanRain's RPX interface on its 200 artist websites (PR Web Press Release Newswire). Certainly the fact that RPX works with MySpaceID and Facebook Connect was a driving force behind this

decision since those two sites would comprise a large portion of a music label's target market.

Many others have followed suit since the RPX solution removes the debate about which open authentication method to implement, or how to integrate more than one. Website developers can have RPX up and running in a single day and be open to getting logins from several reliable providers, with an easy to use JSON and XML response coming back.

RPX has put effort into making their interface easy to use and understand. They have also used a pop up window like Facebook, they make OpenID sign-in the first choice, and they use the name of the service on the buttons as Yahoo! UX research suggested. (Yahoo! 2008) When the user selects a provider they are still momentarily directed to the provider's site in order to accept the authentication. Hopefully this part of the interface will improve as the adoption rate increases and users demand a clearer path from logging in at one site in order to access another. Or perhaps users will get used to this one extra step in favour of not having to create any more accounts.

Implement RPX and Further the Secure Web

What is probably the strongest case for using RPX over an in house solution is that "RPX is a Web service...No library or runtime upgrades are needed when new protocols come online. When new features, providers, or extensions come online, they'll instantly be available via the RPX API." (JanRain). In addition to the benefits to the company itself, sites who jump on the OpenID bandwagon will be part of ushering in the future of web security.

OpenID and the Future of Security

The fact that most OpenID providers offer a username/password combo to log in is a shortcoming of those providers, not the OpenID protocol itself — the providers could switch to implementing login through fingerprints if they wanted to offer something more secure. The point is that how you authorize a site to access your identity has nothing to do with how OpenID works.

Web developers can lead the change towards using open authentication protocols first, and at the same time providers of OpenIDs can begin to offer stronger methods of authentication that move beyond passwords.

A computer science student in Amsterdam wrote a guide on how to phish for OpenID passwords in order to help educate providers and users about the security issues.

“...the web user will have to generate and respond to challenges and therefore will have to use some separate authentication mechanism. We can not rely on the webpage to compute challenges as the webpage may easily have been bugged. This could be done with a browser-toolbar or built-in, a program on USB stick, or a part of the Operating System...Users will only be tempted into this way of authentication when such tools have become mainstream. Firefox 3 and Windows Cardspace are about to give a boost, but at this moment we're simply not ready yet. “ (Slot)

Web developers should start implementing RPX on their sites. This will help the website service providers in that there will be less storage of passwords, more user data passed around without the users having to fill in forms, and easier maintenance of protocols since RPX will take care of keeping the service updated. Getting users comfortable and familiar with open authentication is also a benefit to both user and businesses. In the next few years, as OpenID and others get more recognition it will become more feasible to then add a second form of authentication such as a smart card or a root client certificate. It is generally agreed that adding a second form of authentication is more secure and if users have migrated to using one primary account as their internet identity, then the move to a stronger encryption or a smart card will be easier for them to adopt.

Over the next five years, websites new and old should start to ask for open authentication from their users first before offering a username/password option. It will also be important for sites to allow users to bring with them their profile information as well as friends and contacts from other applications. Users will expect to have this functionality when they see it on large and popular sites like Facebook. After going to the trouble of setting up an identity

profile, a user should be protected from having to re-enter that information on a new site so as much as possible web developers should not only implement RPX, but also use the account information that comes back to show the user that what they have chosen to share with the site is being leveraged to the full extent.

It's time to get ready. As the web matures and is becoming used as much for social activities and community building as for business transactions, trust and having a solid identity on the web will become an important factor for the billions of internet users worldwide. Choosing when and where users can identify themselves and allowing them to carry their data and contacts with them will be a factor in which sites succeed and which fail to connect.

References

- Alexa the Web Information Company. "Alexa Top 500 Sites".
http://www.alexa.com/site/ds/top_sites?ts_mode=global (accessed March 25, 2009).
- Berlind, David. 2009. "InformationWeek Editor Duped In Facebook Phishing Scam".
http://www.informationweek.com/blog/main/archives/2009/02/informationweek_5.html
(accessed March 20, 2009).
- Calore, Michael. 2009. "Want Proof OpenID Can Succeed? Just Scroll Down".
<http://blog.wired.com/business/2009/01/want-proof-open.html> (accessed March 20, 2009).
- Facebook Connect. <http://developers.facebook.com/connect.php> (accessed March 24, 2009).
- Florencio, Dinei and Cormac Herley. 2007. A Large-Scale Study of Web Password Habits. Microsoft Research. <http://research.microsoft.com/~cormac/Papers/www2007.pdf>
(accessed March 25, 2009).
- Fried, Ina and Evers, Joris. 2006. "Gates: End to passwords in sight".
<http://news.cnet.com/2100-7355-6039177.html> (accessed March 20, 2009)
- Greg Goth. 2008. Software-as-a-Service: The Spark That Will Change Software Engineering?. IEEE Distributed Systems Online 9(7):art. no. 0807-o7003.
- Internet World Stats. 2008. <http://www.internetworldstats.com/stats14.htm> (accessed March 21, 2009)
- JanRain. 2009. <http://www.janrain.com/> (accessed March 29, 2009).
- Mandylion Research Labs. 2006. <http://www.mandylionlabs.com/PRCCalc/PRCCalc.htm>
(accessed April 5, 2009)
- McCrea, John. 2009. "What an RP wants". <http://www.slideshare.net/johnmccrea/what-an-rp-wants?type=presentation> (accessed April 5, 2009).
- Michael Chaney. "Michael Chaney's Personal Web Page at Doublewide".
<http://www.doublewide.net/> (accessed April 5, 2009).
- Mittal, Sushubh. 2004. Search Engine Journal. "Microsoft Passport Dumped by Ebay".
<http://www.searchenginejournal.com/microsoft-passport-dumped-by-ebay/1203/> (accessed April 5, 2009).

Moses, Asher. 2008. "How I hacked Sarah Palin's email account".
<http://www.theage.com.au/news/technology/security/how-i-hacked-sarah-palins-email-account/2008/09/19/1221331144691.html?page=2> (accessed March 21, 2009).

Olsen, Stefanie. 2001. "Privacy terms revised for Microsoft Passport".
http://news.cnet.com/Privacy-terms-revised-for-Microsoft-Passport/2100-1023_3-255310.html?tag=bplst (accessed March 21, 2009).

OpenID. <http://openid.net/> (accessed March 19, 2009).

OpenID. 2008. "Microsoft and Google announce OpenID support".
<http://openid.net/2008/10/30/microsoft-and-google-announce-openid-support/> (accessed April 5, 2009).

PasswordResearch.com. 2006. <http://www.passwordresearch.com/stats/statistic246.html>
(accessed March 21, 2009)

PR Web Press Release Newswire. 2008. "Interscope Geffen A&M Deploys JanRain's RPX Solution for Simplified User Login Experience".
<http://www.prweb.com/releases/2008/12/prweb1725444.htm> (accessed April 5, 2009).

Riley, Shannon. 2006. Password Security: What Users Know and What They Actually Do. Usability News volume 8, issue 1,
<http://psychology.wichita.edu/surl/usabilitynews/81/Passwords.asp> (accessed March 25, 2009).

Sachs, Eric. 2008. "Thoughts on combining Google & Yahoo UX research".
<http://sites.google.com/site/oauthgoog/UXFedLogin/CombineGoogYahoo> (accessed April 4, 2009).

Slot, Marco. "Beginner's guide to OpenID phishing". <http://marcoslot.net/apps/openid/>
(accessed April 4, 2009)

Turoczy, Rick. 2008. "JanRain Offers Distributed Social Options Galore, Interscope Geffen A&M Bites".
http://www.readwriteweb.com/archives/janrain_rpx_distributed_social_interscope_geffen_am.php (accessed April 5, 2009).

Yahoo!. 2008. "Yahoo! OpenID Usability Research".
<http://developer.yahoo.com/openid/openid-research-jul08.pdf> (accessed April 4, 2009).