Privacy and Security Advantages of Social Login

janrain®

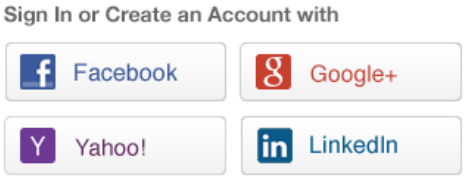
PRIVACY AND SECURITY ADVANTAGES OF SOCIAL LOGIN

Registration that relies on traditional

username/password authentication on the web suffers from a number of issues that reduce its efficacy, increase costs, and significantly increase risk for an organization. Fortunately, by leveraging social login, in which existing identities from social networks like Facebook, Google, and Twitter are used to register and sign in to sites, companies can mitigate these risks, reduce costs, and improve new customer conversion rates.

Let your users sign in with an account they already have

One of the most important trends to emerge from the social web has been the increasing use of portable online identities. Identity Providers (IDPs) such as Facebook, Twitter, and Google offer authentication APIs that make it easy for users to sign in to other websites using an existing profile. By leveraging these APIs, websites can create a personalized experience without requiring the user to register a username, password, and profile data.



Social networking has been a catalyst for making online identity portable and interoperable. Before social networks, people had no alternative to filling out registration forms when signing up for an account at a website. But now, in the social age, expecting people to once again re-enter their relevant identity data has become impractical, maybe even presumptuous.

While social networking itself has been a driving force for many sites in enabling social login from identity providers, it's becoming increasingly clear that encouraging people to sign in with an account that they already have, rather than creating a new one, can have many security benefits.

The trouble with passwords

For years, information security experts have emphasized the importance of practicing good password hygiene—that is, using a unique and unguessable password for every individual site on which registration is required. But online users are human, and password reuse happens a lot more frequently than security professionals would ever like to admit. In fact, a 2011 analysis by Troy Hunt, using real data from accounts that were compromised at Sony and Gawker in 2010, revealed that 67% of users registered at both Gawker and an affected Sony site used the same password at both sites. People who registered at two separate Sony sites reused the same password 92% of the time. And it's hard to blame them, as the task of remembering "strong" and unique passwords across the number of sites where your users are registered is nearly impossible.

The net result of this issue is that even if you believe you have impenetrable defenses against hackers, your users and your data are vulnerable if a completely different site is hacked, due to password reuse/fatigue. Furthermore, it's a rare company that truly has an impenetrable defense against hackers.

In addition to security issues, implementing traditional registration on a site also increases costs. Not only is there a cost to securing and encrypting registration data to prevent the kind of security breaches that have become all too common, but there are support costs, as well. Anyone running a site that requires users to sign in knows that the number one driver of customer support calls is users who can't remember their credentials. In fact, Forrester has reported that password reset requests comprise 20-50% of the customer support volume for an online business, at an average cost of $70 per password-related support request. Ironically, the very reason why these users can't sign in is often because they were practicing good password hygiene and can't remember their secure passwords.

There are hidden costs related to traditional registration, as well. In a 2012 study commissioned by Janrain, nine out of ten survey respondents admitted to having left a website when they could not remember the username or password they had registered there, costing companies customers and revenue.

To sum up some of the issues with traditional registration systems:

- They are expensive to build and maintain.
- They are vulnerable to security breaches due to password reuse from other sites.
- They incur the associated cost of supporting users who forget their credentials.
- They can lead to the loss of customers, as people either won't register in the first place, or will leave when they can't remember their username/password combination.

Thankfully, there is a simple solution to these problems, and that is social login—enabling your users to register and sign in using the well-established identities they have already created at sites like Facebook, Twitter, Google, and Yahoo!.

Benefits of using social login

Signing in with an account from a social login provider brings several advantages over signing in with a site-specific username and password.

- Security is improved by shifting the burden of data protection to large-scale operators like Facebook, Google, and PayPal.
- The cost of customer support required to help users who can't sign in is similarly transferred.
- It's less likely that your users will forget the more-commonly-used username/password combinations registered at their favorite social networking sites.
- No username/passwords are transmitted during the third-party authentication process, only authorization tokens.
- Site owners can leverage security technologies implemented by the top IDPs that they might never be able to replicate themselves.

State-of-the-art security: Facebook, Google, Yahoo

The top IDPs employ state-of-the-art security systems and full-time security teams that most smaller sites would never be able to match. For example, Yahoo! has sophisticated technology that analyzes every sign-in attempt in real time, taking into account the user's previous behavior, the reputation of the IP address, and the geographical location of the sign-in attempt. Yahoo! even lets users review their recent sign-in activity, listing the time and location where each sign-in occurred to help users detect unauthorized activity on their account. fig. 1

Google has similar tools that allow users to view their current sessions, and also gives users the the ability to sign out of sessions remotely. Remote sign-out can be a lifesaver if you've ever forgotten

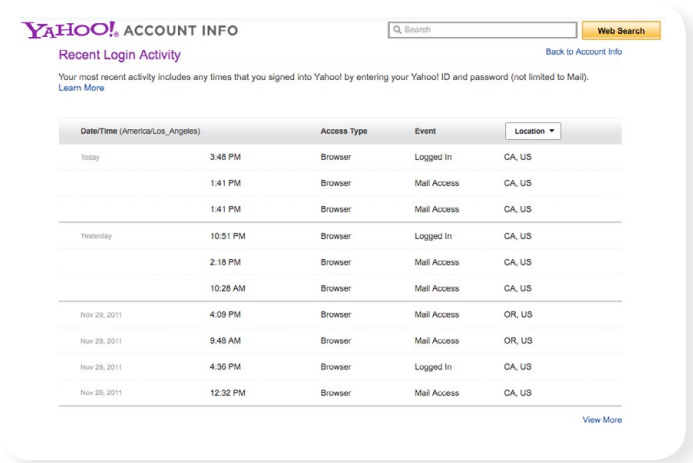


Figure 1

to sign out after borrowing a friend's computer, or after using a public computer at an internet cafe.

Additionally, Google alerts users when unusual activity is detected on their account. For instance, if a user has a pattern of signing in from a particular city or state, and then signs in from a distant country on the other side of the world, Google will notify the user by email. If this security tactic sounds familiar, it should—credit card companies employ the same mechanisms to prevent and detect unauthorized activity.

Figure 2

Just as Facebook has revolutionized the web with its social graph and innovative user experience, it has also brought tremendous innovation to authentication security. fig. 2

Facebook Notifications are a major driver of referral traffic to social content and games, and now serve to notify users about account security issues as well. Among Facebook's security arsenal is the Session Classifier application, which uses location, device, and other account details to detect suspicious activity. For example, if a user typically signs in from California, and then tries to access their account from Africa, a Facebook Notification will alert them to the discrepancy. fig. 3

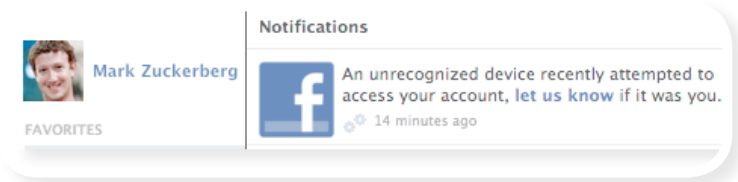


Figure 3

Multi-factor authentication

Using Google, Facebook, or PayPal as an IDP gives users the option of leveraging those providers' implementations of multi-factor authentication.

Multi-factor authentication began as an industrial-strength security feature, used mainly by financial websites and enterprise applications, where users sign in using both a password and a short-lived, single-use code generated by a specialized device. This method is significantly more secure than signing in with a password alone, because compromising the user's account would require both the user's password and the correct, briefly-valid code. fig. 4

Figure 4

As secure a method as it is, however, multi-factor authorization with specialized devices is cumbersome and expensive to implement, and few consumer-oriented sites are able to adopt it successfully on their own.

Fortunately, a growing number of IDPs give security-conscious users the option to enable multi-factor authentication on their accounts. In these systems, signing in with username and password results in a numeric code being sent to the user's mobile phone, via SMS, that must be entered to complete the sign-in. [fig. 5] This option provides an improvement over legacy two-

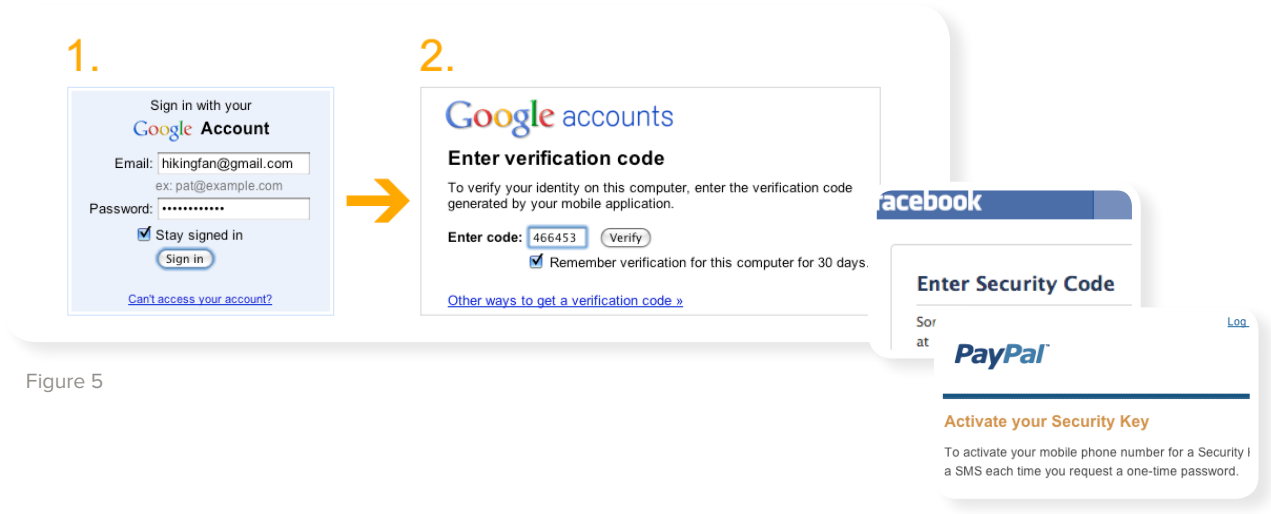


Figure 5

factor systems because users don't have to carry around a special device. Instead, users get the code from their mobile phone, which they likely have with them anyway. Additionally, users need only to enter the code occasionally, when signing in from a new computer for the first time, or after their verification code expires. On subsequent visits over a given period, most often 30 days, the user needs only to enter her password.

IDPs for the government and for the future

The US government has taken notice of industry trends and is working with private industry to open up government websites to let citizens identify themselves using accounts that they already have with private IDPs. Because many interactions with the government require high levels of security, the government is working with private industry though organizations like the OpenID Foundation and the Open Identity Exchange (OIX) to define certification requirements for private IDPs to be used on government websites.

FICAM compliance

For those organizations requiring advanced security measures, such as those outlined in the Federal Identity, Credential, and Access Management (FICAM) framework, compliance can be achieved, cost-effectively, through the use of IDPs that support the Provider Authentication Policy Extension (PAPE), such as Google, PayPal, and Symantec (formerly Verisign).

When FICAM support is requested by a website at user sign-in, all API calls to the IDP include the request that FICAM policies be applied to the authentication and user data shared with the site by the consumer.

Your shortcut to social login

Allowing your users to register and sign in using a social media account they already have can protect your site from the risks associated with weak and reused passwords, leverage the world-class security features implemented by these large-scale operators, improve your new customer conversion rates, and save money for your organization.

References

Troy Hunt's password analysis of the Sony and Gawker breaches:
http://www.troyhunt.com/2011/06/brief-sony-password-analysis.html

Gawker password hacking; Facebook users were not affected:
http://lifehacker.com/5712785/faq-compromised-commenting-accounts-on-gawker-media#1

University of Cambridge Computer Lab password re-use study:
http://www.lightbluetouchpaper.org/2011/02/09/measuring-password-re-use-empirically/

Top 50 passwords used:
http://blogs.wsj.com/digits/2010/12/13/the-top-50-gawker-media-passwords/

Sony password hacking:
http://www.informationweek.com/news/security/attacks/229900111

Facebook security infographic:
http://thedinfographics.com/2011/11/21/facebook-security-everything-you-ever-wanted-to-know/

Two-factor authorization at Google:
http://googleblog.blogspot.com/2011/02/advanced-sign-in-security-for-your.html

US Government ICAM Trust Framework:
http://openidentityexchange.org/trust-frameworks/us-icam

Forrester: Mastering Login Issues
http://www.forrester.com/Mastering+Login+Issues/fulltext/-/E-RES58051?objectid=RES58051

ABOUT JANRAIN

Janrain makes it easy for companies to truly know their customers and personalize every interaction. The Janrain Customer Identity Management Platform helps companies acquire customers online, recognize these customers across all digital touch points and better understand them by collecting and utilizing demographic, psychographic and behavioral profile data. Our solutions, including social login, social sharing, comprehensive registration, customer profile data collection and storage,single sign-on and digital strategy services, improve the effectiveness of digital marketing initiatives for leading brands such as Universal Music Group, Whole Foods, Mattel, Pfizer, Samsung and Dr Pepper. Founded in 2002, Janrain is based in Portland, Oregon. For more information, please call 1-888-563-3082 or visit www.janrain.com and follow @janrain.

