Is OpenID too open?

Lori MacVittie, 2008-20-10

One password to fool them all

One password to find them

One password to steal them all and in the ether become them

[with many apologies to J.R.R. Tolkien]

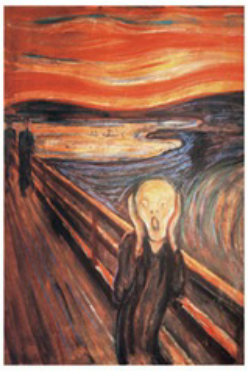
For years we've had it beat into our heads that using the same username and password for everything on the web leaves us open to compromise and identity theft. The on-demand nature of conversations and social networking has apparently left us all bereft of our wits as we embrace the very concept we've been warned about for years. But is it really as dangerous as we've been led to believe?

The concept of a single identity that can be shared across disparate sites is hardly new. Liberty Alliance proposed SAML as the underlying technology to provide a single sign on (SSO) functionality for the web years ago and it competed with Microsoft's Passport for mindshare.

But neither took off; both were "ahead of the times". Social networking hadn't taken over the web yet, and people didn't really see a need to take the risk.

That was then, this is now.

OpenID is succeeding where the Liberty Alliance with SAML and Microsoft's Passport (now "Live ID") failed. It's easy to use, easy to integrate with your own site, and seems to be everywhere. Just set up a single identity at OpenID or a participating site like Technorati and you can use that same identity over and over to sign into hundreds of social networking sites around the web.



Despite knowing that it's dangerous (or so we're told), that it's a risk (and a big one at that, they say), hundreds of thousands of us (and that 'us' is mutually inclusive, mind you) use OpenID either directly or indirectly by tying our identities at myriad social networking sites to a single identity. We do this despite knowing that if that single identity is compromised that it can be used against us at every site through which we use that identity to interact with others.

The uber-security minded folks may now commence screaming and holding their head in pain as they morph into something out of an Edvard Munch painting at what I'm going to say next.

HOW MANY WALLETS DO YOU CARRY?

The risk appears to be minimal, despite the advertisements and scary articles to the contrary, and the benefits apparently outweigh that risk. Much in the same way we rail against additional security precautions at the airport, referring to them as unnecessary and doing nothing but offering a false sense of security, perhaps the "never use the same password" precaution, too, offers little more than a false sense of security.

As Alan Shimel unfortunately discovered recently, separate identities doesn't really add a lot of security when the identity information is aggregated in a single place, which it all too often is. Compromise of your primary e-mail account is also likely to end up with your online identity compromised, whether you used OpenID or not.

The risks for you and I (I assume you aren't Alan Shimel, Robert Scoble, or Paris Hilton) having our identities targeted and stolen are likely on the same level as having our wallet stolen. If we leave it out on the table and walk away, yeah, it's probably going to get stolen. The digital equivalent would be, oh, posting the information somewhere public or using that single identity on a site that seems a bit less than trustworthy - or isn't implementing best practices in securing that data and preventing theft.

If you don't carry more than one wallet to protect your multiple credit cards and your identity, then is it really a problem using only one "digital wallet" to store you identity online? Probably not, as long as the owners of the sites at which you can use your OpenID are taking steps to ensure the security of the site and the underlying data.

MITIGATION OF THE RISK IS ON THE SITE, NOT THE USER

The risk of theft really has very little to do with users today, as we don't typically share our identities and passwords publicly. The risk has to do with the sites we frequent and what kind of security they have in place to prevent exploitation of vulnerabilities and data theft. There are no real regulations in place regarding notification of data loss for sites not storing personally identifiable information, as there are for financial and healthcare related institutions, so we may never know. And it's unlikely that your bank is going to offer OpenID as a means of identifying yourself. I shudder to even consider that as an option.

All things considered, using OpenID or at least the manual implementation of OpenID (same username/password over and over) doesn't seem to be really all that much of a risk unless you also use it for your online financial and healthcare information.

And I know ***none*** of us are doing that, are we?

F5 Networks, Inc. | 401 Elliot Avenue West, Seattle, WA 98119 | 888-882-4447 | f5.com

F5 Networks, Inc.
Corporate Headquarters
info@f5.com

F5 Networks
Asia-Pacific
apacinfo@f5.com

F5 Networks Ltd.
Europe/Middle-East/Africa
emeainfo@f5.com

F5 Networks
Japan K.K.
f5j-info@f5.com