Social Media Single Sign-On: Could You Be Sharing More than Your Password?

SESSION ID: HUM-W03B
2/26/14 (Wednesday) 11:20 AM - West|3005

Tom R. Smith
VP, Business Dev & Strategy, CloudEntr
www.CloudEntr.com
Tom.Smith@gemalto.com
I HAVE A NEW HOBBY. IT’S CALLED PHISHING.

I SEND FAKE BANKING E-MAILS TO GULLIBLE EXECUTIVES. THEN I FIND OUT THEIR FINANCIAL INFORMATION AND USE IT TO STEAL THE MONEY THEY DON’T DESERVE.

Dear Customer,
This is your bank. We forgot your social security number and password. Why don’t you send them to us so we can protect your money.

Sincerely,
I. B. Banker
“You already have zero privacy – get over it.”

- Scott McNealy
Agenda

- What’s being tracked and collected online
- What is Social Login
- Potential risks introduced
- Process flow for Social Login for B2C and B2E
- Suggested resources if you want to learn more
NSA is not the only one tracking you...

- What have you done today?
  - Use your credit card to buy coffee?
  - Login to wireless network at the RSA show?
  - Use your mobile phone?
  - Check your company’s e-mail?
  - Sent a text message, or tweet, or posted something to LinkedIn or Facebook?
When and how is information collected?

- User **intentionally** shares information (explicit consent) …
  - Buy something (billing info, credit card info, ship-to, etc.)
  - Create account or register at a website (name, login credentials, other…)
- Online behavior activity **silently tracked** (implicit consent)…
  - Click on a link in an e-mail or on a website (look at URL)
  - Open a web page (just the act of “viewing” a page)
  - Sign-on using social login (relying party requests profile info)
  - Other techniques: analytics, beacons, widgets, cookies, fingerprinting
What is “Social Login”? 

- Uses your existing Social Media account to register or login to website / online service 
- Benefits both the individual user and target website 
- Profile information may be exposed as part of login
Be clear on your intended use of Social Login

- What is the purpose of enabling Social Login?
  - Marketing / Sales (B2C, B2B, non-employees)
    - Enable/attract customers to access your product and services
    - Easy registration, immediate harvest of rich profile data
  - Security / Compliance (B2E, employees)
    - Login to company resources for employees
    - Provides a set of existing employee credentials
- Who is authoritative source for user identity and the assets?
  - Your company vs. social vendor (Facebook, Google, Twitter, etc.)
What can be retrieved during Social Login?

**User Social Data Capturing:** Get Accurate Data Including Verified Email Addresses

- Real-time social user data capturing
- Over 50 types of data fields
- Stores data in your database
- Receive normalized user data
- Access to raw data API

**Get Rich User Data**

When users authenticate via Social Login, they give your app permission to access rich, first-party social data. Detailed profile information such as interests, demographics, education, social connections, work history, and more can easily be stored in your own database, or automatically stored via Identity Storage - Gigya’s dynamic, cloud-hosted database. As users opt-in to marketing via Social Login you can:

- Deliver hyper-relevant content
- Create highly targeted email marketing campaigns
- Surface friend activity by leveraging a user’s social graph
- Target influential and high-intent users
Does using Social Login increase risk?

- Information = attack points
  - Individuals tend to be more lax in their personal lives and re-use or create weak passwords for their Social Media account
  - Socially engineered attacks are fueled by personal information
  - Social Logins create intermingled non-business entry points – Target, Sony, Evernote, Adobe, etc.

Source: http://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/
“Anonymous” wants access to website

New registration and/or login with Social Login service

Website requests, User allows Permissions

Website and Social accounts are Linked

User Profile info captured by website

“Known” User granted Access
Employee wants access to business app

Social Login credential used

Social credentials alone not trusted for requested resource

Trusted 2nd Factor Authentication required, and applied

Employee granted SSO access to all authorized apps

Social Login interaction limited to corporate identity and access management system only

Employee logged in to app
Summary…

- Social Logins for consumer facing websites
  - Convenient for both user and website
  - Middleware may simplify implementation, ongoing integrations
- Social Logins for employees to business assets
  - Social Login should only interact with corporate IAM system
  - Employee Identity is known, just use Social Login as credential
  - Augment with 2FA based on company policies
To learn more…

- Shallow end of pool: useful search terms…
  - Tools that block tracking on websites you visit: “privacy browser extensions”
  - Social Login middleware vendors: “social login”
- In depth: technical standards, and best practices…
  - [www.idecosystem.org](http://www.idecosystem.org)
  - [http://openid.net/connect/](http://openid.net/connect/)
  - [http://www.fidoalliance.org/](http://www.fidoalliance.org/)
Q & A…

Speaker contact info:

Tom R. Smith
VP, Business Dev. & Strategy, CloudEntr
www.CloudEntr.com
Gemalto (Austin, TX)
E-mail: tom.smith@gemalto.com
Phone: 512-605-2116