Password Managers, Single Sign-On, Federated ID:
Have users signed up?

Konstantin (Kosta) Beznosov
Open ID
OpenID

• open and user-centric Web single sign-on protocol

• OpenID Foundation (2007) [1]
  • Microsoft, Google, IBM, Yahoo, VeriSign, Facebook, PayPal, PingIdentity

• over one billion OpenID enabled user accounts provided by Google, Yahoo, AOL...[1]

how OpenID works

Identity Provider

authentication request

authentication response

Discover

login request

user name: alice.myopenid.com
password: xxxxxxxxx
HAVE USERS SIGNED UP?
NO
WHY HAVE NOT USERS SIGNED UP?
BECAUSE THEY CAN!

ha-ha!
if we really want to know, then why not to ask users?

interviews with 51 participants
no perceived urgent need for Web SSO

• most are “comfortable” with weak or reused password
• 23% used the password manager feature in the browse
single-point of failure concern

• 26% of participants identified this issue and expressed concern about it
security misconceptions and incorrect mental models

- majority thought they were giving their user name and password to the RP websites directly
- some had the impression that their user name and password were stored on the local computer
password phishing attacks

Sign in with OpenID

user name: alice.myopenid.com
password: xxxxxxxxx

Google accounts

Sign in with your Google Account. Learn more

Sign in with your Google Account

Email:
eg pat@example.com

Password:

Stay signed in

Sign in

Can't access your account?

Don't have a Google Account?
Create an account now
phishing concerns

• once informed, all expressed great concerns about IdP phishing attacks
• even when prompted, half couldn’t find any distinguishing features on a phishing login form
privacy concerns

- 40% were hesitant to consent to the release of personal profile information when prompted by the RP
- 26% requested and were provided with an anonymous OpenID account for the study
lack of user trust

• 36% stated that they would not use SSO on websites that contain valuable personal information or involve potential monetary loss (e.g., banking, stock websites)

• many stated they would not use a Web SSO system on websites which they do not believe to be trustworthy or are not familiar with
account linking

• most did not understand the purpose and concept of account linking
• they became confused and frustrated when they were prompted to create or associate an account on the RP website
ANY IDEAS?
identity-enabled browser

Alice/password

identity provider

relying party
UI consistent across sites