doi: 10.36689/uhk/hed/2021-01-093 HED Hradec Economic Days

Security Concerns of Social Login Usage at the 3rd Party Cloud Services

Martin ZBOŘIL

Prague University of Economics and Business, Prague, the Czech Republic; zbom01@vse.cz

Abstract: Social login presents a method that facilitates authentication to cloud services and other applications where users leverage their already created accounts at social networks like Facebook or Twitter. This approach brings many benefits to the users, however, as with each technology, the social login is linked with multiple security concerns. These concerns might present a significant risk to the users and should be always considered when establishing social login authentication. This article is dedicated to the research of current security concerns related to social login usage. In total, the author of this article identified six main concerns and provided a detailed explanation of each of them. Some of the concerns cover cyber attacks that might be performed over the social account or the related services. At these attacks, the author included and designed simulations of them in a form of diagrams that contain the activities taken during the attacks.

Keywords: social login; social media; accounts; security; authentication; cloud services

JEL Classification: L86

1. Introduction

Laziness of people has always been a driving force that pushes solutions to be more effective, automatic, faster, and eligible. This fact is especially true in the nowadays world of information modern technologies. Examples of such technological innovations that came or became popular in the last years are the Internet of Things, Blockchain, Big Data, or Artificial Intelligence (Kim, 2020). The innovations are, however, visible not only in these greatly known and standalone technologies but also in smaller and not so obvious areas. One of these areas is the possibilities of user authentication that this article is dedicated to. This article, to be more precise, focuses on one particular authentication method – social login.

Social login might be defined as *„the sign-in option that allows a user to access a website using their ID and password from a social network application like Yahoo! or Amazon. The social network for login is referred to as the social platform"*. (JANUS Associates, 2016) Another definition talks about social login as *„Social login, as used herein, refers to an authentication technique that allows a user to use a single account in order to access many different cooperating websites and services). The single account functions as the digital identity of a user for any number of services or websites."* (Roee, 2018) Examples of how the social login looks at the associated cloud services (mostly the Software-as-a-Service cloud services) are visible in Figure 1.

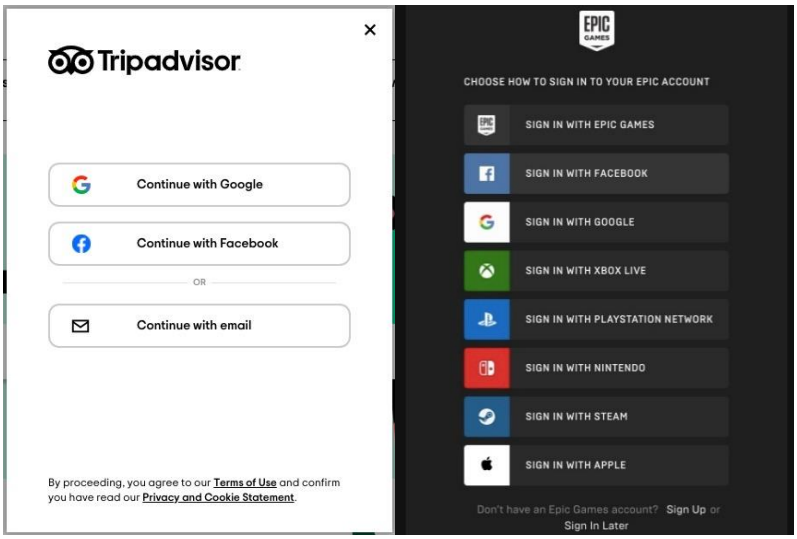

Figure 1. Example of social login at Tripadvisor and Epic Games

For the social login, not only traditional social networks like Facebook, Twitter, or Instagram are considered as a social network, but it involves also Google account. The number of users that leverage social login depends greatly on the number of social network users. From this point of view, social login has an extremely wide scope of potential users. According to the last researches at Statista, e.g. Facebook has currently 2,700 million users, Instagram has 1,150 million users and Twitter has 350 million users (Statista, 2020). Besides, 1,800 million active users have created Gmail that is linked with Google Account (SaaS Scout - Research Group, 2020).

The social login concept is useful also for the providers of social networks as the social login promotes the social networks and the providers collect more information about users. Even without the information of the associated cloud services, providers collect an enormous amount of information about all of the users. The examples of the issues linked with stored personal information and relevant security breaches are presented in (Oken-Tatum, 2019), (Rehman, 2019) and (Fuller, 2019).

The reason why social login is such a popular concept is that the providers of associated cloud services see this option as an opportunity to increase the usage of their service as the social login facilitates and quickens the process of user registration. Besides, another reason for its usage is that the big social network providers publicly offer the documentation on how to integrate the social login to their site where anybody may retrieve the information of APIs and other requirements to implement it.

Social login was already described and discussed in multiple articles, however, none of the articles focused clearly on the detailed description of the security concerns that are linked with the social login usage. The article (Schroers, 2019) describes the concept of authentication with social networks and discusses the benefits and issues linked with the usage. The technical solution of social login for mobile applications is explored in the article (Ho & Katuk, 2016). The authors focused on the description of the solution based on the OAuth protocol. The objective of a publication (Nissim & Gafni, 2014) was to identify and assess the

factors that affect the decision on using social login or not. One part of the article is the description of social login adoption benefits and barriers.

The main objective of this article is to provide the research of the most significant security concerns linked with social login.

2. Methodology

This article, as is stated above, is dedicated to the research with the aim to identify a comprehensive list of major security concerns related to social login. The author investigated a great number of recent articles that are related to social login and its security concerns. The author compared then the identified results to business reports and other types of resources and found that the investigated articles already contained all required and usable information.

The description of the conducted research is split into Sections 3.1–3.6 where each section is dedicated to one specific security concern linked with social login.

3. Results

Social login brings many usability benefits to the users; such examples are single account for multiple sites, spared time with faster registration, updates only on a single point, or personalization (Nissim & Gafni, 2014). Moreover, social login brings also several security advantages like the requirement for remembering only one password, trust in security mechanisms on a big social provider's side, or possible built-in multi-factor authentication (Janrain, 2012).

When considering the usage of social login, however, the security risks of this type of authentication need to be counted as they may negatively influence the security posture of your accounts.

3.1. Social Account Breach – Associated Services

The usage of social login, leveraging of one account from a social network at multiple cloud services, gives space for performing several scenarios of cyberattacks. The following paragraphs are dedicated to such attacks.

The first option for how the social login might be exploited is when a hacker successfully attacks the social network that's account is used also for other services. When users want to see a list of associated sites, they may get the information usually through the social network platform. An example is the Facebook setting in Figure 1 where usage of social login at TripAdvisor is visible.

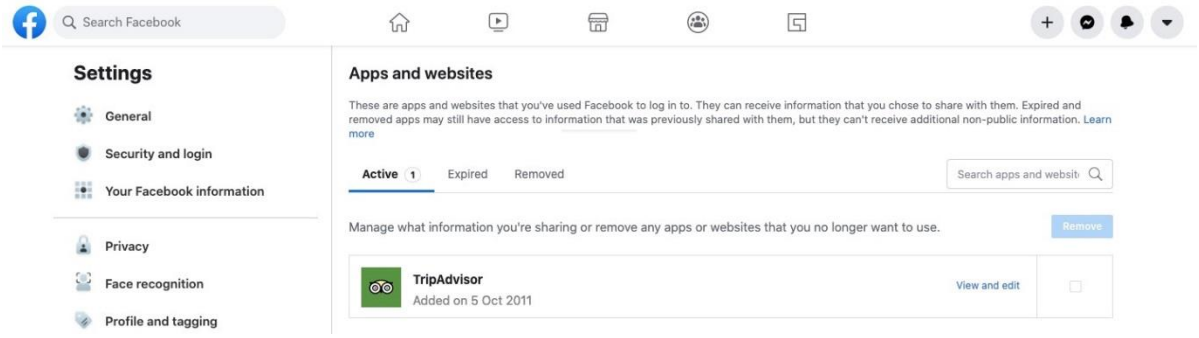

Figure 2. List of associated sites through the social network at Facebook

Attackers may then easily go to the breached account's setting and see there the sites where they may log in with the account. Everything in the IT world is moving to automized solutions so also this exploitation needs not to be manual as described above but may be automatic with the usage of APIs. Social network providers offer users/developers documentation with described APIs that may use to connect to the network (e.g. www.developers.facebook.com for Facebook).

The exemplary simulation of the above-described scenario is shown in Figure 3.

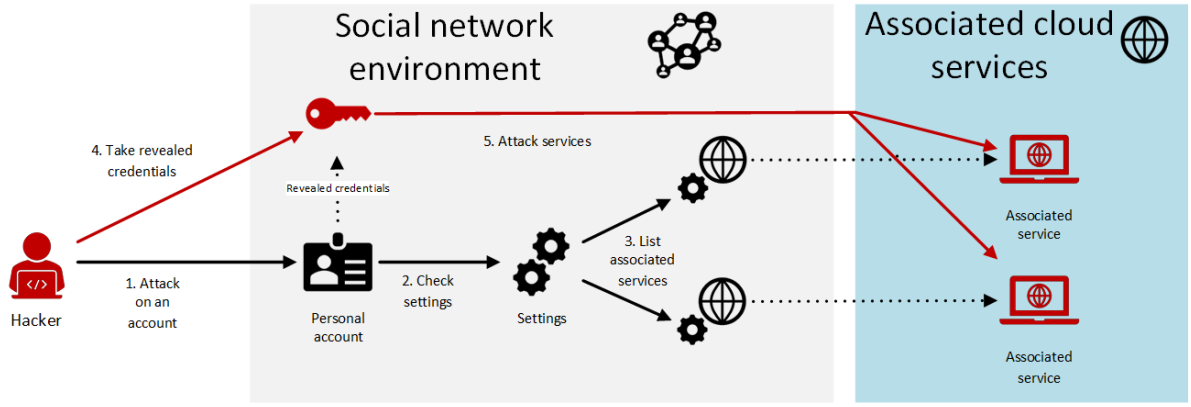

Figure 3. A simulated attack on associated services through listing the services on a hacked social network account

3.2. Social Account Breach – Leaked Credentials

The breached social accounts enable also another attack path without knowing the list of associated accounts. As mentioned in the Introduction, attackers also perform brute-force attacks with the usage of huge tables with credentials of breached accounts. In the previous scenario, the attackers always know where to successfully log in. In this scenario, however, they are guessing whether the account is present on a certain site or not.

From the implementation cost point of view, this scenario demands less manual or development work as attackers do not need to perform the steps manually or develop the scripts for leveraging the APIs, they just take already existing tools for performing the attack (e.g. available by default on Kali Linux instances). On the contrary, the attack requires higher computational power as they are trying to login with a countless number of credentials and they need to perform more attacks as the success rate is logically low.

The exemplary simulation of the above-described scenario is shown in Figure 4.

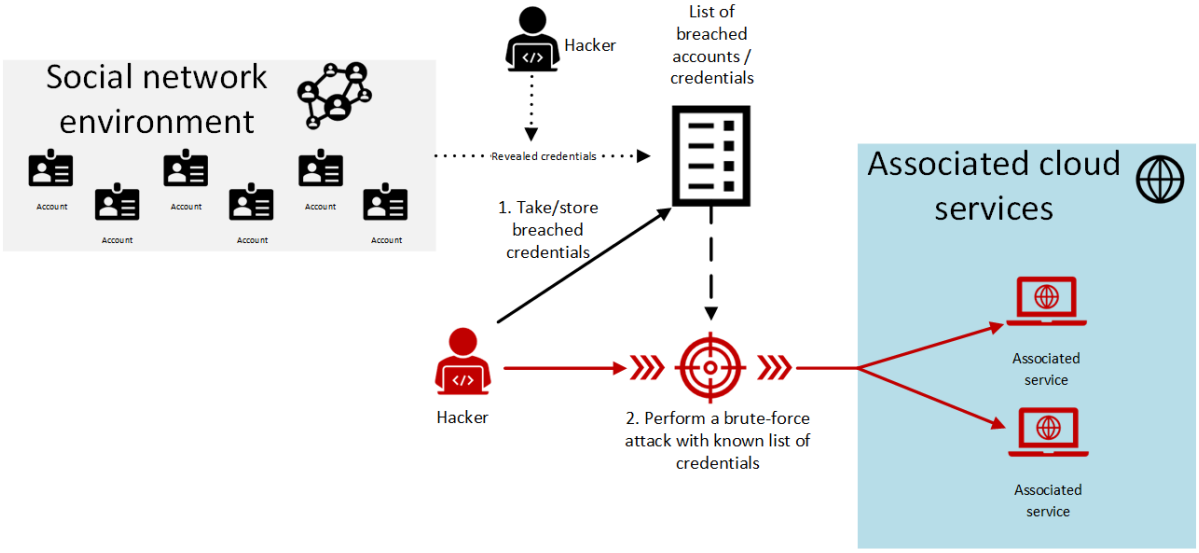

Figure 4. A simulated attack on associated services with the use of a list of breached accounts

3.3. Low Credentials Complexity

Social networks are open to all users and their primary objective is to gather and connect as many users as possible. This implies that social network providers do not want to discourage users with strong requirements for password/authentication complexity. As a result, users tend to create simple and easy-to-remember passwords. This fact is generally known among the security community but it was also proven by many kinds of research, like (Daojing et al., 2020), (Gärdekrans, 2017), (Yıldırım & Mackie, 2019) or (Choong, 2015).

An especially important factor linked to social networks and passwords is the usage of personal information for password creation as it eases users to remember created passwords. The reason why it is especially important is that the majority of personal information is often present on the user's accounts on social networks. Accordingly, attackers exploit this publicly available personal information to try to guess the password or use it for the brute force attack. Exactly this area was a part of the research presented at (Gafni, Pavel, Margolin, & Weiss, 2017). The results showed that according to the included questionnaire, 71% of respondents use personal data to create their passwords. Besides, 27% of respondents answered that they also use other family information, not only their own. However, this type of information is often also present on social networks and publicly accessible through the user's account.

The all above indicates that the password for social network accounts could have a weak password established. This implies that the weak password could be established also for all associated services through the social login if a user establishes a weak password at their social network account. As a result, all the accounts at the associated services are vulnerable to brute-force attacks.

The exemplary simulation of the above-described scenario is shown in Figure 5.

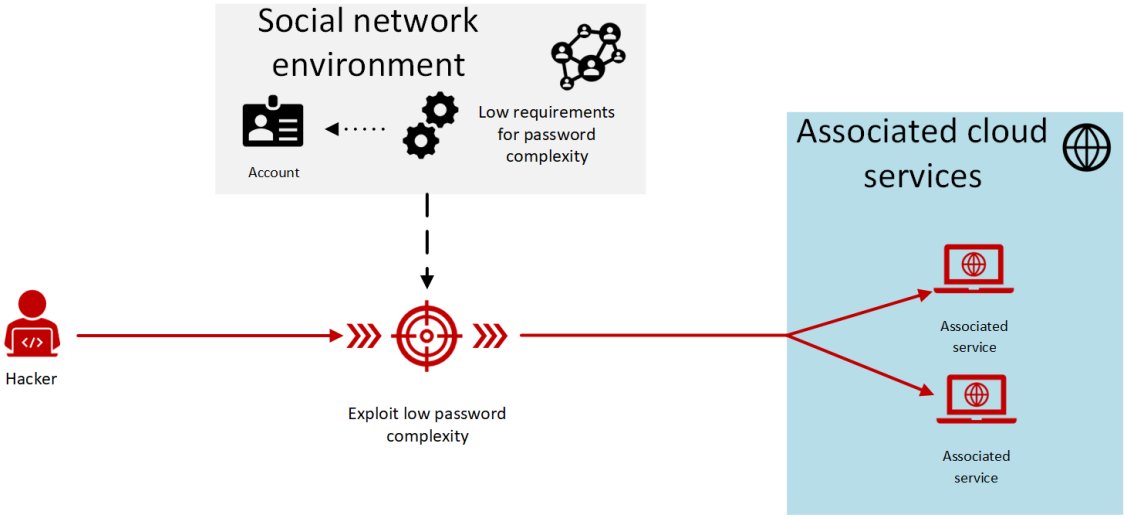

Figure 5. A simulated attack on a social network due to low password complexity configured at a social network.

3.4. Technical Vulnerabilities

Each technology and technical solution bring their vulnerabilities; social login implementations are not exceptions. The vulnerabilities of social login usage are primarily linked with authentication protocol vulnerabilities, such as Open ID. Common Vulnerabilities and Exposures, abbreviated as CVE, is a world-widely known database of commonly known vulnerabilities. **Chyba! Nenalezen zdroj odkazů.** provides an overview of vulnerabilities linked to social login, present in the official database of CVEs, with an official description:

Table 1. CVE vulnerabilities linked to "social login" – official descriptions (Common Vulnerabilities and Exposures, 2020).

ID	Description
CVE-2019-11015	A vulnerability was found in the MIUI OS version 10.1.3.0 that allows a physically proximate attacker to bypass Lockscreen based authentication via the Wallpaper Carousel application to obtain sensitive Clipboard data and the user's stored credentials (partially). This occurs because of paste access to a social media login page.
CVE-2017-3125	An unauthenticated XSS vulnerability with FortiMail 5.0.0-5.2.9 and 5.3.0-5.3.8 could allow an attacker to execute arbitrary scripts in the security context of the browser of a victim logged in FortiMail, assuming the victim is social engineered into clicking an URL crafted by the attacker.
CVE-2017-18501	The social-login-bws plugin before 0.2 for WordPress has multiple XSS issues.
CVE-2017-1000004	ATutor version 2.2.1 and earlier are vulnerable to a SQL injection in the Assignment Dropbox, BasicLTI, Blog Post, Blog, Group Course Email, Course Alumni, Course Enrolment, (…) Content Menu, Auto-Login, and Gradebook components resulting in information disclosure, database modification, or potential code execution.
CVE-2016-4048	An issue was discovered in Open-Xchange OX App Suite before 7.8.1-rev11. Custom messages can be shown at the login screen to notify external users about issues with sharing links. This mechanism can be abused to inject arbitrary text messages.
CVE-2015-5511	The HybridAuth Social Login module 7.x-2.x before 7.x-2.13 for Drupal allows remote attackers to bypass the user registration by administrator only configuration and create an account via a social login.

CVE-2015-4395	The HybridAuth Social Login module 7.x-2.x before 7.x-2.10 for Drupal stores passwords in plaintext when the "Ask user for a password when registering" option is enabled, which allows remote authenticated users with certain permissions to obtain sensitive information by leveraging access to the database.
CVE-2014-6092	IBM Curam Social Program Management (SPM) 5.2 (…) requires failed-login handling for web-service accounts to have the same lockout policy as for standard user accounts, which makes it easier for remote attackers to cause a denial of service (web-service outage) by making many login attempts with a valid caseworker account name.
CVE-2014-4576	Cross-site scripting (XSS) vulnerability in services/diagnostics.php in the WordPress Social Login plugin 2.0.3 and earlier for WordPress allows remote attackers to inject arbitrary web script or HTML via the xhrurl parameter.

3.5. Decreased Anonymity

As was already mentioned in previous the introduction, providers of social networks keep an enormous amount of data about their users. The described issues and current approaches imply that when a social login is used, users should also care about the fact that their anonymity on the Internet is decreased. The lower anonymity might be seen from two perspectives.

The first perspective was also touched on in the previous section and involves revealed information about the accounts between the social account provider and associated cloud service. For example, users should consider whether they want that Google knows what they are searching for on the Tripadvisor site if they are using a Google account for social login.

The second perspective involves the revealed information between the users themselves. The example is that a user leverages a Facebook account to login into an associated cloud service where the account/profile has the same name, nickname, email, and avatar/picture. Based on this information, some other users from the cloud service can find the user's profile on Facebook and much information about the user (personal details, pictures, friends, posts, favorite things, political opinion, sexual orientation, etc.). Regarding this issue, social networks offer usually configurations that may restrict such public visibility, as was shown in Figure 6.

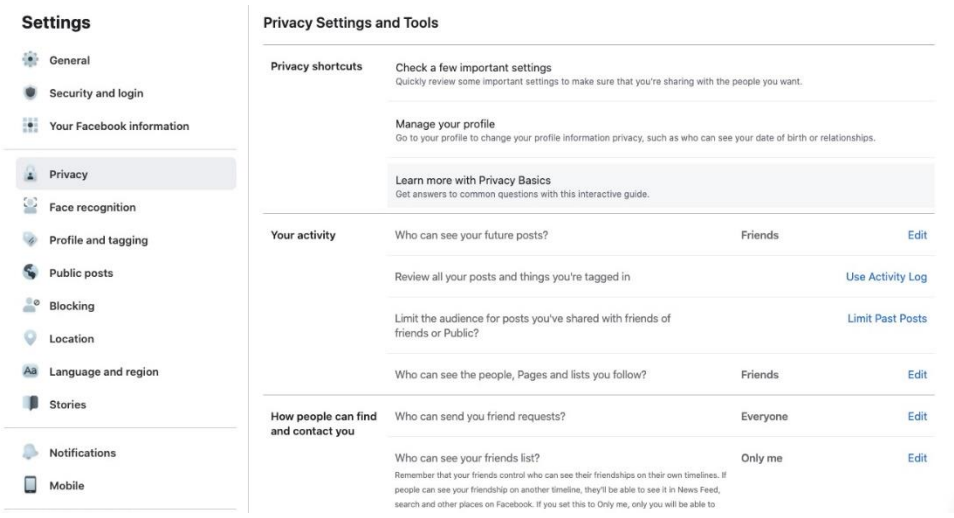

Figure 6. Exemplary configuration at Facebook

3.6. Account Lock

The last concern is not linked directly with security concerns, but with the usage of the cloud service. The accounts on social networks could be deleted, due to potential inactivity periods but mainly due to manual deletion of the accounts by users themselves. Since the authentication to associated cloud services is through the potentially deleted account, users would have issues with login into the cloud service. Then, it depends on the particular implementation of whether the access would be completely restricted or whether the inserted credentials would be compared to stored hashes. Nevertheless, the second option would bring also limitations, e.g. no possibility to reset passwords.

4. Discussion and Conclusion

Social login brings multiple benefits, however, security concerns should always be bared in mind when establishing this type of authentication. This article helped readers to get an overview of what main security concerns are linked with the social login. The security concerns were not only focused on the security in the technical meaning (Sections 3.1, 3.2, 3.3, 3.4) but touched also other parts of the security area, like decreased anonymity (Section 3.5), and account lock (Section 3.6). Users of social login have limited options on how to deal with the technical concerns, except for setting a nontrivial password. However, mainly the decreased anonymity concerns depend partly on the behavior and configuration of users themselves.

The social logins approach is significantly dependent on the protection of the social network account as is obvious from the described security concerns; therefore, users should sufficiently protect their accounts. The most fundamental countermeasure is to configure such a level of password complexity that assures the account's protection against brute-force and dictionary attacks. An additional and recommended level of protection is authentication through MFA (multi-factor authentication), where users e.g. insert a code from SMS that they receive or confirm the authentication on a special mobile application. MFA ensures that even though the brute-force attacks successfully reveal the user's credentials, the attackers are still not able to authenticate to the account. Although the protection requirements for a complex password and MFA are generally known, still many users are not touched with that and keep their simple and easy-to-guess passwords.

The author of this article plans to follow up with quantitative research focused on social login usage and awareness about security concerns and benefits.

References

Common Vulnerabilities and Exposures. (2020, December 4). Retrieved from https://cve.mitre.org/cgi-bin/cvekey.cgi?keyword=social+login

Daojing, H., Zhou, B., Yu, H., Cheng, Y., Chan, S., Zhang, M., & Guizani, N. (2020). Group-based Password Characteristics Analysis. *IEEE Network*, 1-7. https://doi.org/10.1109/MNET.001.1900482

Fuller, M. (2019). Big data and the Facebook scandal: Issues and responses. *Theology*, *122*(1), 14-21. https://doi.org/10.1177/0040571X18805908

Gafni, R., Pavel, T., Margolin, R., & Weiss, B. (2017). Strong password? Not with your social network. *Online Journal of Applied Knowledge Management, 5*(1), 27-41. https://doi.org/10.36965/OJAKM.2017.5(1)27-41

Gärdekrans, R. (2017). Password Behaviour. *Bachelor Degree Project*. University of Skövde. https://www.diva-portal.org/smash/get/diva2:1109665/FULLTEXT01.pdf

Ho, L. K., & Katuk, N. (2016). Social Login with OAuth for Mobile Applications: User's View. In *IEEE Symposium on Computer Applications & Industrial Electronics (ISCAIE)* (pp. 741-759). https://doi.org/10.1109/ISCAIE.2016.7575043

Choong, Y.-Y. (2015). *Employee Password Usability Survey.* Gaithersburg, MD, USA: National Institute of Standards and Technology. https://csrc.nist.gov/CSRC/media/Presentations/Employee-Password-Usability-Survey/images-media/day2_research_430-530pt2.pdf

Janrain. (2012). *Privacy and Security Advantages of Social Login.* User Management Platform for the Social Web.

JANUS Associates. (2016). *Social Login Security Risk Assessment For Massachusetts Libraries.* Stamford.

Kim, B. (2020). Moving Forward with Digital Disruption: What Big Data, IoT, Synthetic Biology, AI, Blockchain, and Platform Businesses Mean to Libraries. L*ibrary Technology Reports*, *56*(2).

Nissim, D., & Gafni, R. (2014). To Social Login or not Login? Exploring Factors Affecting the Decision. *Informing Science and Information Technology, 11*, 57-72. https://doi.org/10.28945/1980

Oken-Tatum, B. (2019). Facebook will pay an unprecedented $5B penalty over privacy breaches. *Central Penn Business Journal*.

Rehman, I. u. (2019). Facebook-Cambridge Analytica data harvesting: What you need to know. *Library Philosophy and Practice. University of Nebraska - Lincoln*.

Roee, P. (2018). *Detecting social login security flaws using database query features.* International Business Machines Corporation.

SaaS Scout - Research Group. (2020). *Gmail Statistics, Users, Growth And Facts For 2020*. Retrieved from https://saasscout.com/statistics/gmail-statistics/

Schroers, J. (2019). I have a Facebook account, therefore I am – authentication with social networks. *International Review of Law, Computers & Technology*, *33*(2), 211-223. https://doi.org/10.1080/13600869.2018.1475895

Statista. (2020, November 31). *Most popular social networks worldwide as of October 2020, ranked by number of active users*. Retrieved from https://www.statista.com/statistics/272014/global-social-networks-ranked-by-number-of-users/

Yıldırım, M., & Mackie, I. (2019). Encouraging users to improve password security and memorability. *International Journal of Information Security, 18*(6), 741-759. https://doi.org/10.1007/s10207-019-00429-y