Security on Social Media

Combined Probus Club of Wheelers Hill Inc.

Introduction

- Since the arrival of early social networking sites in the early 2000s, online social networking platforms have expanded exponentially, with the biggest names in social media today being Facebook, Instagram, Twitter and Snapchat.
- The massive influx of personal information that has become available online and stored in the cloud has put user privacy at the forefront of discussion regarding the database's ability to safely store such personal information.
- Privacy concerns with social networking services is a subset of data privacy, involving the right of mandating personal privacy concerning storing, re-purposing, provision to third parties, and displaying of information pertaining to oneself via the Internet.

What is the Concern

- Features that invite users to participate in—messages, invitations, photos, open platform applications and other applications are often the venues for others to gain access to a user's private information.
- Through these websites many people are giving their personal information out on the internet, often without realising how far it can go.
- These social networks keep track of all interactions used on their sites and save them for later use.
- Issues include cyberstalking, location disclosure, social profiling, 3rd party personal information disclosure.

- Social networks are free for users but are commercial entities.
- They make their money by effectively selling their users to advertisers. Their users are the product.
- They also sell access to their user base to app developers.
- They all have privacy policies that users must acknowledge when they join.
- Most privacy agreements state the most important information at the end because it is assumed that people will not read it completely.
- The privacy agreement states that the social network owns all of the content that users upload. This includes pictures, videos, and messages, all stored in the social networks database even if the user decides to terminate his or her account.

Potential Risks

- Social profiling and 3rd party disclosure.
  - As Facebook demonstrates an illusion of privacy presented by a “for-friends-only” type of platform, individuals find themselves more inclined to showcase more personal information online.
  - Companies, such as Facebook, carry extensive amounts of private user information on file, regarding individuals’ , “likes, dislikes, and preferences”, which are of high value to marketers.
  - Social profiling is where Facebook and other social networking media websites filter the advertisements, assigning specific ones to specific age groups, gender groups, and even ethnicities.
  - As Facebook reveals user information to advertising and marketing organizations, personalized endorsements will appear on news feeds based on “surfing behaviour, hobbies, or pop culture preferences”.

- Identity theft
  - As there is so much information provided other things can be deduced, which can then be used as part of identity theft.
  - Cases have also appeared of users having photographs stolen from social networking sites in order to assist in identity theft.
  - Geotagged photos make it easy for third party users to see where an individual is located.
  - Birthdates are often shown, either directly or indirectly.
  - There is also growing use of phishing, which reveals sensitive information through secretive links and downloads. Social media has opened up an entirely new realm for hackers to get information from normal posts and messages.

- Pre-teens and early teenagers
  - Among all other age groups, in general, the most vulnerable victims of private-information-sharing behaviour are preteens and early teenagers.
  - Preteens and early teenagers are particularly susceptible to social pressures that encourage young people to reveal personal data when posting online.
  - They tend to share this information because they do not want to feel left out or judged by other adolescents who are practicing these sharing activities already.
  - This is concerning because preteens and teenagers are the least educated on how public social media is and how to protect themselves online.
  - Adolescents tend to post their real name, birthdays, and email addresses to their social media profiles.
  - In doing so they are running the risk of cyberbullying, stalking, and in the future, could potentially harm them when pursuing job opportunities

- Sexual predators
  - Most major social networking sites are committed to ensuring that use of their services are as safe as possible.
  - However, due to the high content of personal information placed on social networking sites, as well as the ability to hide behind a pseudo-identity, such sites have become increasingly popular for sexual predators.
  - In worst cases children have become victims of paedophiles or lured to meet strangers.
  - On-line ‘friends’ may not always be who they appear to be.

- Stalking
  - Popular social networking sites make it easy to build a web of friends and acquaintances and share with them your photos, whereabouts, contact information, and interests without ever getting the chance to actually meet them.
  - With the amount of information that users post about themselves online, it is easy for users to become a victim of stalking without even being aware of the risk.
  - 63% of Facebook profiles are visible to the public, meaning if you Google someone's name and you add "+Facebook" in the search bar you pretty much will see most of the person’s profile.
  - Services such as Facebook "Places," which is a Facebook service, publicises user location information to the networking community, including potential stalkers.

- Unintentional fame
  - Unintentional fame can harm a person's character, reputation, relationships, chance of employment, and privacy.
  - Information including pictures and videos can be circulated beyond a group of friends. Once posted, the original user has no control over it.
  - Many incidents of videos being posted on social networking sites highlight the ability for personal information to be rapidly transferred between users.

- Employment
  - Issues relating to privacy and employment are becoming a concern with regards to social networking sites.
  - Some employers and employment agencies search social networking sites in order to screen potential candidates.
  - For the majority of employers, such action is to acquire negative information about candidates.
  - Issues relating to privacy are also becoming an increasing concern for those currently in employment.
  - An ill-considered post about your boss or company could cost you your job.

Privacy Settings

- All social network users should be aware when they join up, that the default privacy settings favour the site, not the user.
- Finding the settings is not always simple, and there can be lots of them!
- When in doubt try Googling “privacy settings in XXX social network”.
- Be aware that settings can change when a site does an update.

References

- Australian Government Cyber Security site: https://www.cyber.gov.au/acsc/individuals-and-families
- Wikipedia: https://en.wikipedia.org/wiki/Privacy_concerns_with_social_networking_services