LEDRA COLLEGE NICOSIA

Staying Safe on Social Networks

Alexis Michael
BSc, MSc, MBA, CISSP, CISA, CEH, EDRP, Security+

Social networks

- Social networking sites have become very popular avenues for people to communicate with family, friends and colleagues from around the corner or across the globe.
- Such sites are a part of our most important smartphone apps, are a vital tool for any serious job search, and are the new way to connect with current and new friends.
- While there can be benefits from the collaborative, distributed approaches promoted by responsible use of social networking sites, there are information security and privacy concerns

Social networks

- The volume and accessibility of personal information available on social networking sites have attracted malicious people who seek to exploit this information.
- The more information a person posts, the more information becomes available for a potential compromise by those with malicious intentions.
- How many times do potential employers base their hiring decisions on what they see on social media rather than on the resume? How many stories are there of people losing their jobs, health insurance coverage and even their relationships because of something on social media that seemed totally innocent at the time?
- It's obscene the level of personal privacy we have given up in the 21st century and most of us do not even realize it has happened.

The illusion of Internet privacy

- The internet is definitely not secure, no more secure than walking down a street in the middle of the day in a very large city
- Did you know you cannot 'delete' a photo from Facebook? You can remove it from your profile and the button is labelled 'delete', but Facebook keeps a copy, they always have, it is in your Facebook end-user agreement. Have you read it?
- Did you know you cannot delete your Facebook account? You can deactivate it but it will always be there and hackers love inactive accounts. The password never changes.

The illusion of Internet privacy

- On many occasions law enforcement has been able to track people and their activities based purely on internet activities alone.
- Most of the time this is for a good reason, to be sure, but have you ever asked yourself how they got access to this or that private chat message when they are obviously not a part of the social media circle in question?
- There's no privacy on the internet - Don't do, post or say anything on the internet you would not do in public.

Common dangers - XSS

- One of the scammers' favorite methods of attack at the moment is known as cross-site scripting or “Self-XSS” - Facebook messages such as the Facebook Dislike button take you to a webpage that tries to trick you into cutting and pasting a malicious JavaScript code into your browser’s address bar

- Facebook posts such as "In honor of Mother’s Day" seem innocuous enough, until you realize that information such as your children’s names and birthdates, pet’s name and street name now reside permanently on the Internet - Since this information is often used for passwords or password challenge questions, it can lead to identity theft.

http://nakedsecurity.sophos.com/2011/05/16/facebook-dislike-button-spreads-fast-but-is-a-fake-watch-out/

http://nakedsecurity.sophos.com/2011/05/08/how-mothers-day-facebook-celebrations-can-lead-to-identity-theft/

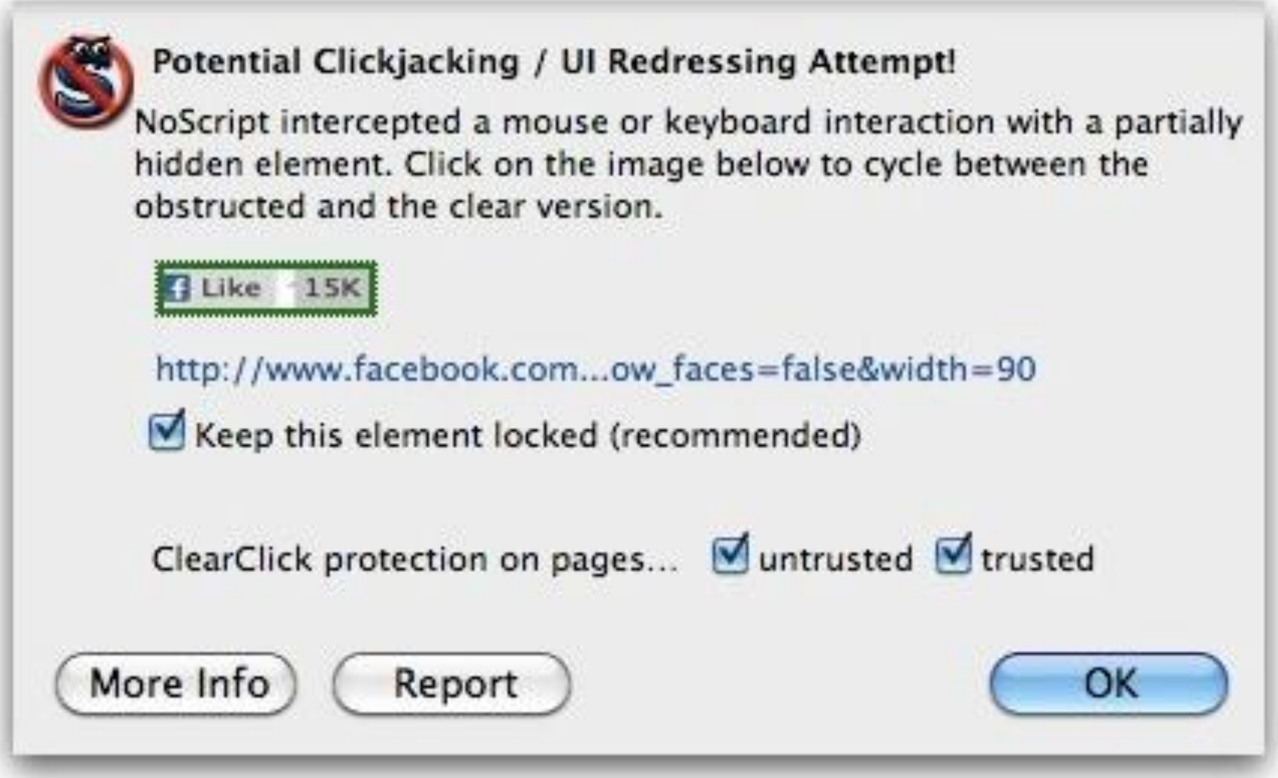
Common dangers - Clickjacking

- Other attacks on Facebook users include "clickjacking" or "likejacking," also known as "UI redressing."
- Scammers try to pique your curiosity with messages like "The World Funniest Condom Commercial – LOL". Clickjacking scams take users to a webpage urging them to watch a video. By viewing the video, it's posted that you "like" the link and it's shared with your friends, spreading it virally across Facebook.

http://nakedsecurity.sophos.com/2011/05/31/world-funniest-condom-commercial-facebook-viral-likejacking

Common dangers - Clickjacking

"NoScript" Add-on for Firefox



Potential Clickjacking / UI Redressing Attempt!

NoScript intercepted a mouse or keyboard interaction with a partially hidden element. Click on the image below to cycle between the obstructed and the clear version.

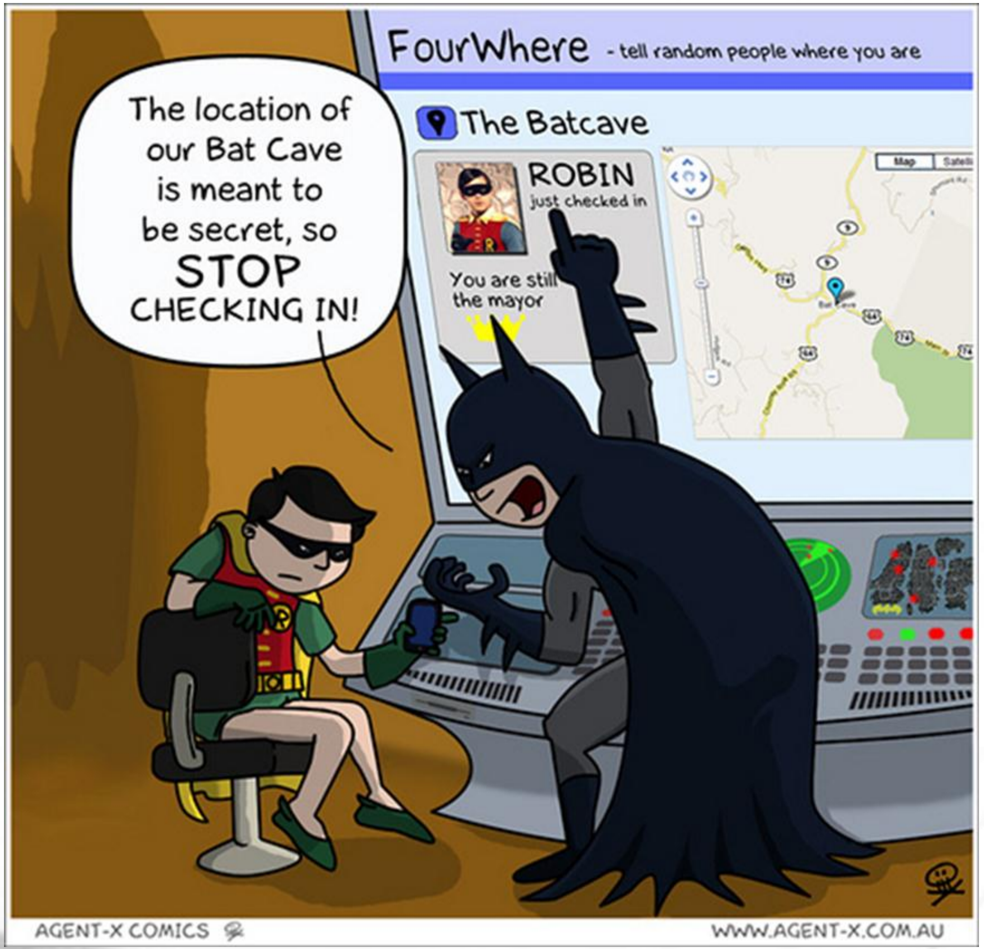
http://www.facebook.com...ow_faces=false&width=90

☑ Keep this element locked (recommended)

ClearClick protection on pages... ☑ untrusted ☑ trusted

Common dangers – Check-ins

- "Checking-in" everywhere you go! **WHY?**


FourWhere - tell random people where you are
The Batcave
ROBIN just checked in
You are still the mayor
The location of our Bat Cave is meant to be secret, so STOP CHECKING IN!
AGENT-X COMICS
WWW.AGENT-X.COM.AU

Common dangers - Privacy

- Never do, post or say anything on the internet that you would not want repeated over and over again and which you would not do in public - Everything that goes on the internet stays on the internet probably for ever as far as your concerned.
- You should only post information you are comfortable disclosing to a complete stranger.
- Review a site's privacy policy – Would Facebook become so popular if users read the policy before signing-up?

Other social networking safety tips

- **Customize privacy options** – Try to limit information others can see about yourself – you can even set different privacy settings between people on your friend list!
- **Think well about your "security question" for resetting your password** – Is your pet's name so hard-to-find information?
- **Ensure that any computer you use to connect to a social media site has proper security measures in place** - Use and maintain anti-virus software and keep your application and operating system patches up-to-date
- **Use caution when clicking a link to another page or running an online application, even if it is from someone you know** – And remember to "LongURLplease" for short addresses! (E.g. goo.gl/iemxgl)

Other social networking safety tips

- **To avoid giving away email addresses of your friends, do not allow social networking services to scan your email address book** – Do you really believe them about not storing this information?
- **Your online reputation can be a good thing:** Your profile will be looked at by potential employers! –Your current employer might also have a glance, when you're on a sick leave!
- **Be wary of third-party applications** - Third-party applications may provide entertainment or functionality, but do you really trust them?
- **Treat the social networking sites as you would treat any other dangerous site** – Use the proper protection mechanisms