ComputerScience

Boston University

What is Facebook?

Facebook is a popular free social networking website that allows registered users to create profiles, upload photos and videos, send messages, and keep in touch with friends, family and colleagues.

How does Facebook keep your information safe?

- Facebook uses HSTS.
- All connections are encrypted using TLS1.2.
  - "The connection is encrypted and authenticated using AES_128_GCM and uses ECDHE_ECDSA as key exchange mechanism.
- Facebook is verified by DigiCert-SHA2 High Assurance Server, CA.
- IE key exchange is used to establish shared keys, and symmetric crypto techniques are then used.

Cookies and tracking:

Facebook Uses Cookies for a for a variety of reasons.

Authentication:

- These cookies alert Facebook when a user is logged in.
- Allows Facebook to relay relevant social information
  - One example would be the way social plug-ins are implemented

Security and Site Integrity:

- These cookies aid in keeping Facebook safe and secure

Site Features and Services:

- These cookies store user preferences, track interactions with Facebook Services.

Advertising, insights and Analytics and research:

- Cookies, tracking pixels and other such technologies are used by Facebook to create targeted advertisements-- its number one source of revenue.
- Persistent cookies that allow Facebook to "provide advertisers with insights about the people who see and interact with their adds, visit their websites, and use their apps."

REMARK: Facebook does not sell user information.

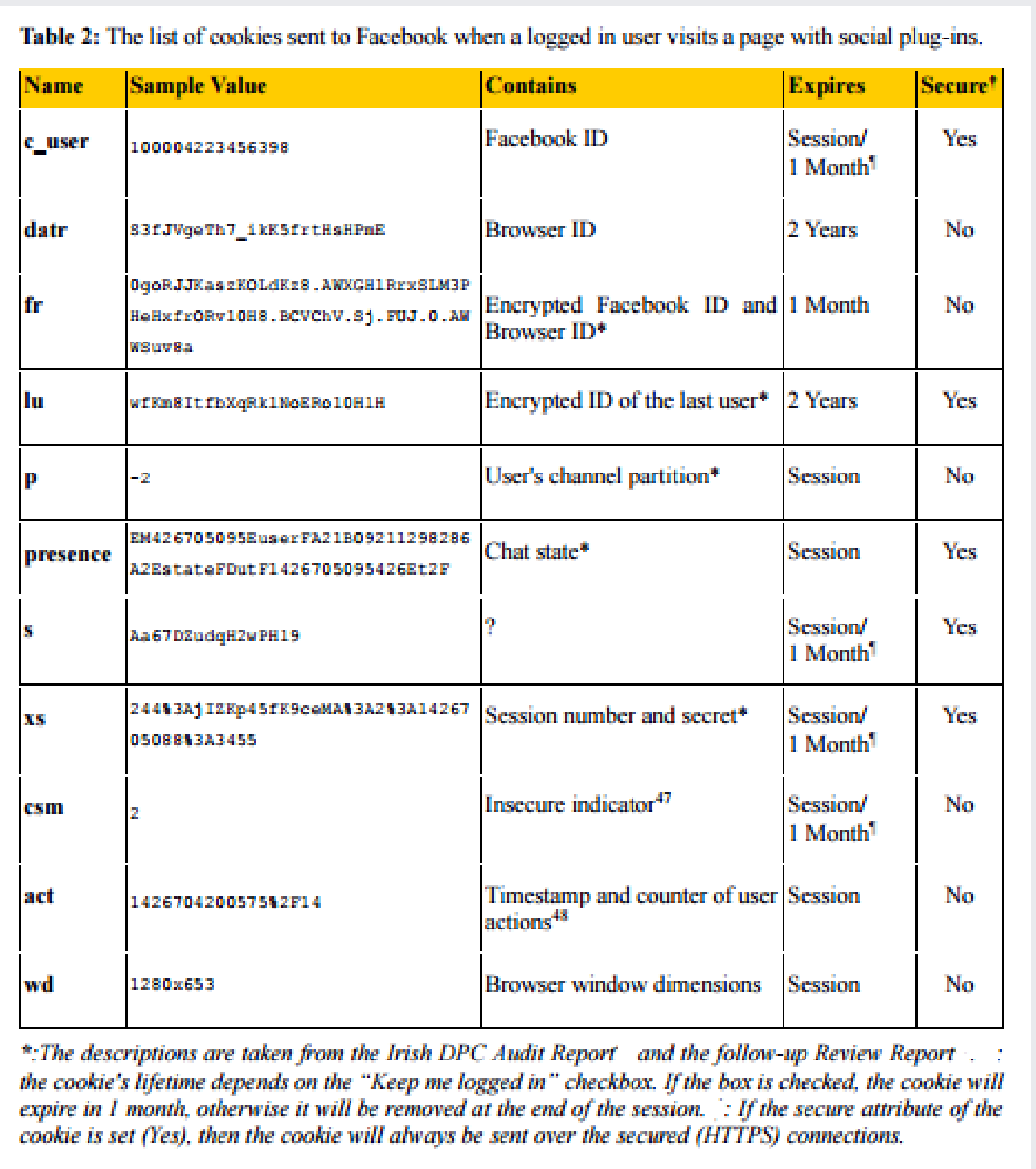
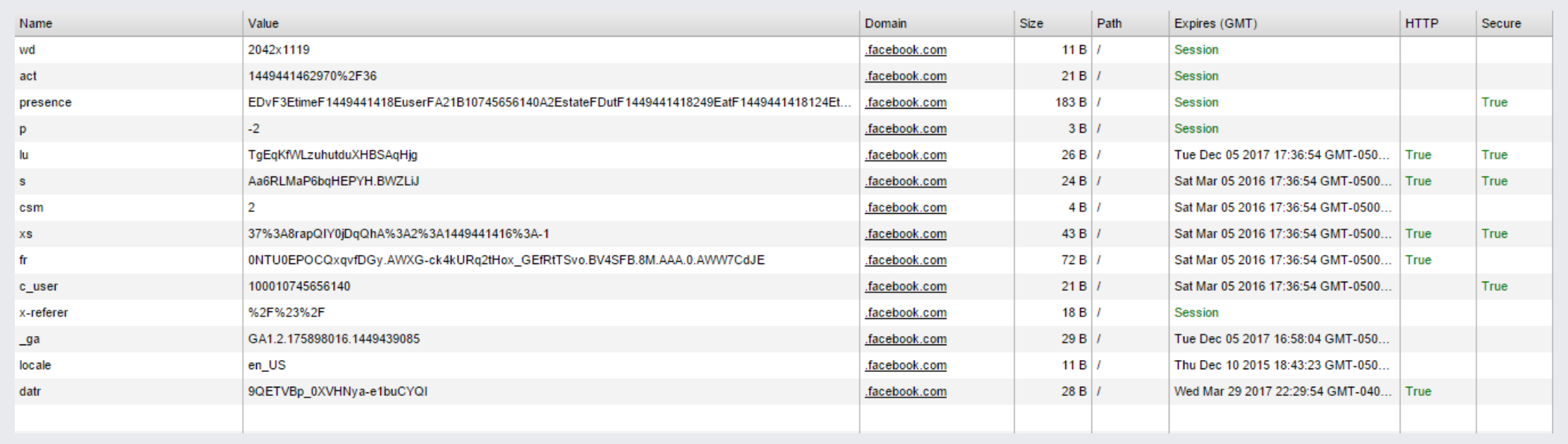


Table 2: The list of cookies sent to Facebook when a logged in user visits a page with social plug-ins.

Name	Sample Value	Contains	Expires	Secure[†]
c_user	100004223456398	Facebook ID	Session/ 1 Month[¶]	Yes
datr	83fJVgeTh7_ikK5frtHsHPmE	Browser ID	2 Years	No
fr	0goRJJKaszKOLdKz8.AWXGH1RrxSLM3PHeHxfrORv10H8.BCVChV.8j.FUJ.0.AWWSuv8a	Encrypted Facebook ID and Browser ID*	1 Month	No
lu	wfKm8ItfbXqRk1NoERo10H1H	Encrypted ID of the last user*	2 Years	Yes
p	-2	User's channel partition*	Session	No
presence	EM426705095EuserFA21B09211298286A2EstateFDutF1426705095426Et2F	Chat state*	Session	Yes
s	Aa67DZudqH2wPH19	?	Session/ 1 Month[¶]	Yes
xs	244%3AjIZKp45fK9ceMA%3A2%3A1426705088%3A3455	Session number and secret*	Session/ 1 Month[¶]	Yes
csm	2	Insecure indicator[47]	Session/ 1 Month[¶]	No
act	1426704200575%2F14	Timestamp and counter of user actions[48]	Session	No
wd	1280x653	Browser window dimensions	Session	No

**:The descriptions are taken from the Irish DPC Audit Report and the follow-up Review Report . : the cookie's lifetime depends on the "Keep me logged in" checkbox. If the box is checked, the cookie will expire in 1 month, otherwise it will be removed at the end of the session. : If the secure attribute of the cookie is set (Yes), then the cookie will always be sent over the secured (HTTPS) connections.*

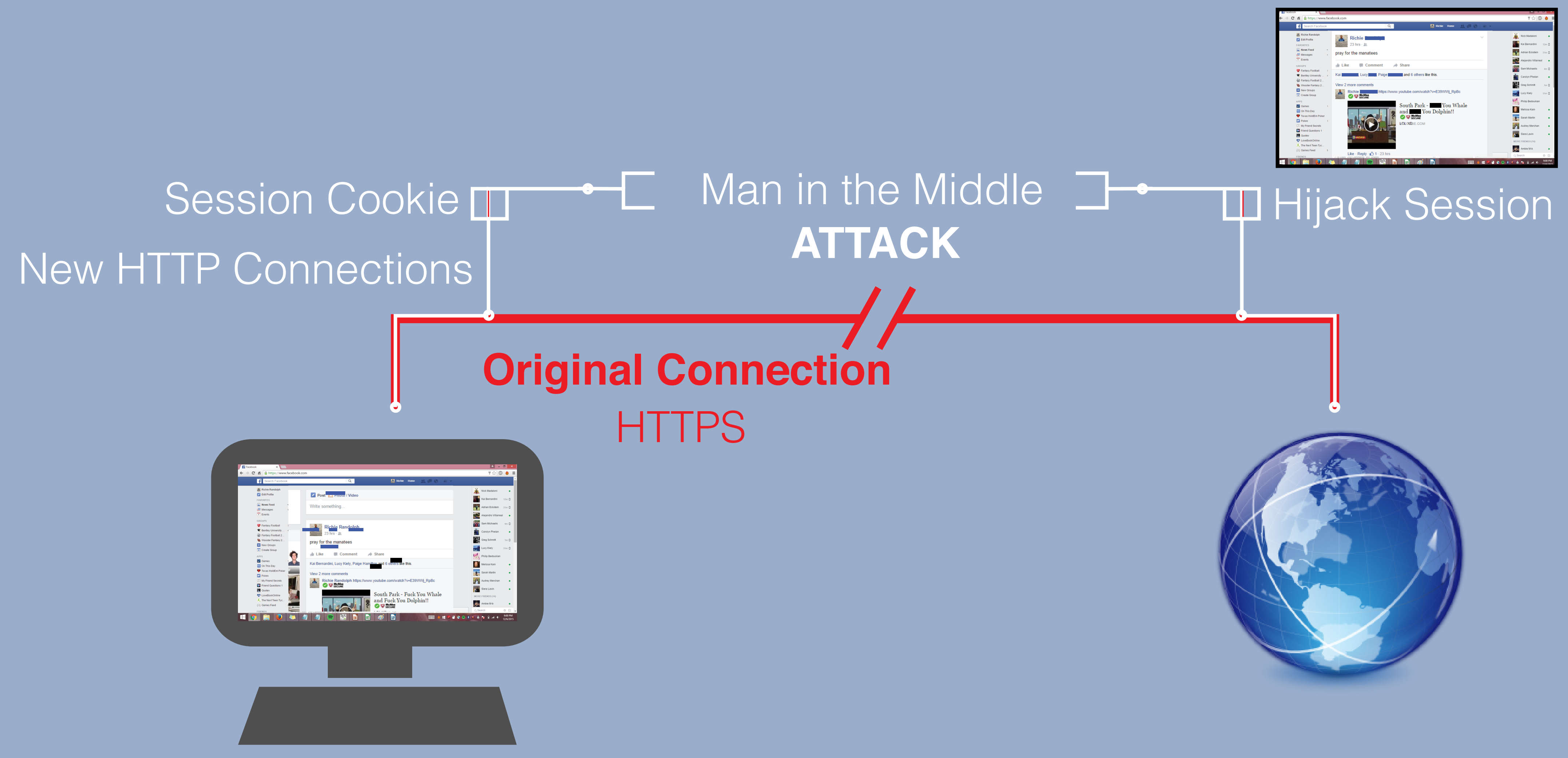


Name	Value	Domain	Size	Path	Expires (GMT)	HTTP	Secure
wd	2042x1119	.facebook.com	11 B	/	Session		
act	1449441462970%2F36	.facebook.com	21 B	/	Session		
presence	EDvF3EtimeF1449441418EuserFA21B10745656140A2EstateFDutF1449441418249EatF1449441418124Et...	.facebook.com	183 B	/	Session		True
p	-2	.facebook.com	3 B	/	Session		
lu	TgEqKfWLzuhutduXHBSAqHjg	.facebook.com	26 B	/	Tue Dec 05 2017 17:36:54 GMT-050...	True	True
s	Aa6RLMaP6bqHEPYH.BWZLiJ	.facebook.com	24 B	/	Sat Mar 05 2016 17:36:54 GMT-0500...	True	True
csm	2	.facebook.com	4 B	/	Sat Mar 05 2016 17:36:54 GMT-0500...		
xs	37%3A8rapQIY0jDqQhA%3A2%3A1449441416%3A-1	.facebook.com	43 B	/	Sat Mar 05 2016 17:36:54 GMT-0500...	True	True
fr	0NTU0EPOCQxqvfDGy.AWXG-ck4kURq2tHox_GEfRtTSvo.BV4SFB.8M.AAA.0.AWW7CdJE	.facebook.com	72 B	/	Sat Mar 05 2016 17:36:54 GMT-0500...	True	
c_user	100010745656140	.facebook.com	21 B	/	Sat Mar 05 2016 17:36:54 GMT-0500...		True
x-referer	%2F%23%2F	.facebook.com	18 B	/	Session		
_ga	GA1.2.175898016.1449439085	.facebook.com	29 B	/	Tue Dec 05 2017 16:58:04 GMT-050...		
locale	en_US	.facebook.com	11 B	/	Thu Dec 10 2015 18:43:23 GMT-050...		
datr	9QETVBp_0XVHNya-e1buCYQI	.facebook.com	28 B	/	Wed Mar 29 2017 22:29:54 GMT-040...	True	

It is worth noting that social networking websites, such as Facebook, are in a unique and dangerous position, as they can easily correlate browsing behavior of a user to their online profile. In many cases, their profile is their real world identity.

Hacking Richie:

Method 1 (Session Hijacking): With Richie's permission, and the help of WireShark, BurpSuite, TCPDump, OVMS,SSLStrip2,DNS2PROXY, we were able to retrieve Richie's Session Cookie (now inactive) over an HTTP connection.
With the Cookie in possession, we then used a cookie injector to log into his Facebook without knowledge of his Login username or password.
FIX: VPN
Potential Damage: He could have been forced to like Donald Trump, the Miami Dolphins, and Crocs.



Method 2 (Social Experiment): Using Facebook's "Forgot Password" service, we are able to view enough of Richie's email to determine his primary email is COMCAST, which allows for security questions.
From there, it was simply a matter of guessing his favorite sports team and typing in his home address
We then gained access to his primary email and were then able to reset his password this way.
If Richie had enabled Login notifications and Login Approvals, this could have been prevented.
A special thank you to Richie for being such a good sport!

references
https://www.facebook.com/whitehat/
https://www.facebook.com/help/cookies/

www.facebook.com
Your connection to this site is private.