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.

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/