SOCIAL MEDIA HACKS

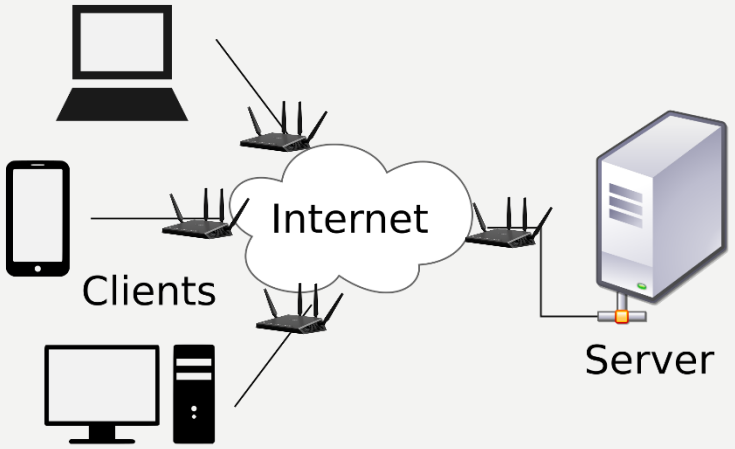
BY

GARRETT, AMEEN, & GEORGE

TABLE OF CONTENTS

HOW SOCIAL MEDIA GETS HACKED

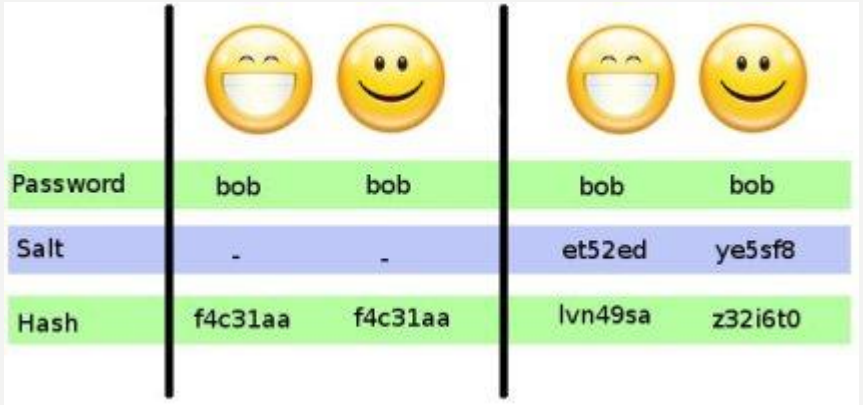
OVERVIEW



SERVER SIDE THREAT

Example: LinkedIn Failed to Properly Salt Hashed Passwords

- Allegedly breached by SQL Injection, but LinkedIn denies
- In 2012, Russian Hackers stole close to 6.5 million hashed passwords and other personal info
  - Estimated to be 5% of user base
- LinkedIn failed to salt hashed passwords properly before they were stored in SQL database
- Used well known and outdated hashing algorithm, SHA-1



https://nakedsecurity.sophos.com/2012/06/21/linkedin-slapped-with-5-million-class-action-suit-over-leaked-passwords/

https://nakedsecurity.sophos.com/2012/06/06/millions-of-linkedin-passwords-reportedly-leaked-take-action-now/

SERVER SIDE THREAT

EXAMPLE: LinkedIn Failed to Salt Passwords CONTINUED

If the Social Media website you are using has been breached then the data they store about you and your profile is at risk.

http://www.zdnet.com/article/linkedin-will-pay-1-25-million-to-settle-suit-over-password-breach/

http://www.zdnet.com/article/linkedin-hit-with-5-million-class-action-suit/

http://www.pcworld.com/article/257045/6_5m_linkedin_passwords_posted_online_after_apparent_hack.html

CLIENT SIDE THREAT

EXAMPLE: "The Snappening"

- Over 200,000 images leaked by hackers
- Snapchat did not allow users to save their snaps, so users would install 3rd party apps to work around this and save photos/videos
- Snapchat's API for providing images to the app, was reverse engineered
  - Allowed developers to make unauthorized requests for images as long as the user was authenticated (gave login/password to 3rd party app)
  - IE request to /ph/find_friends could find out if a phone # was attached to an account

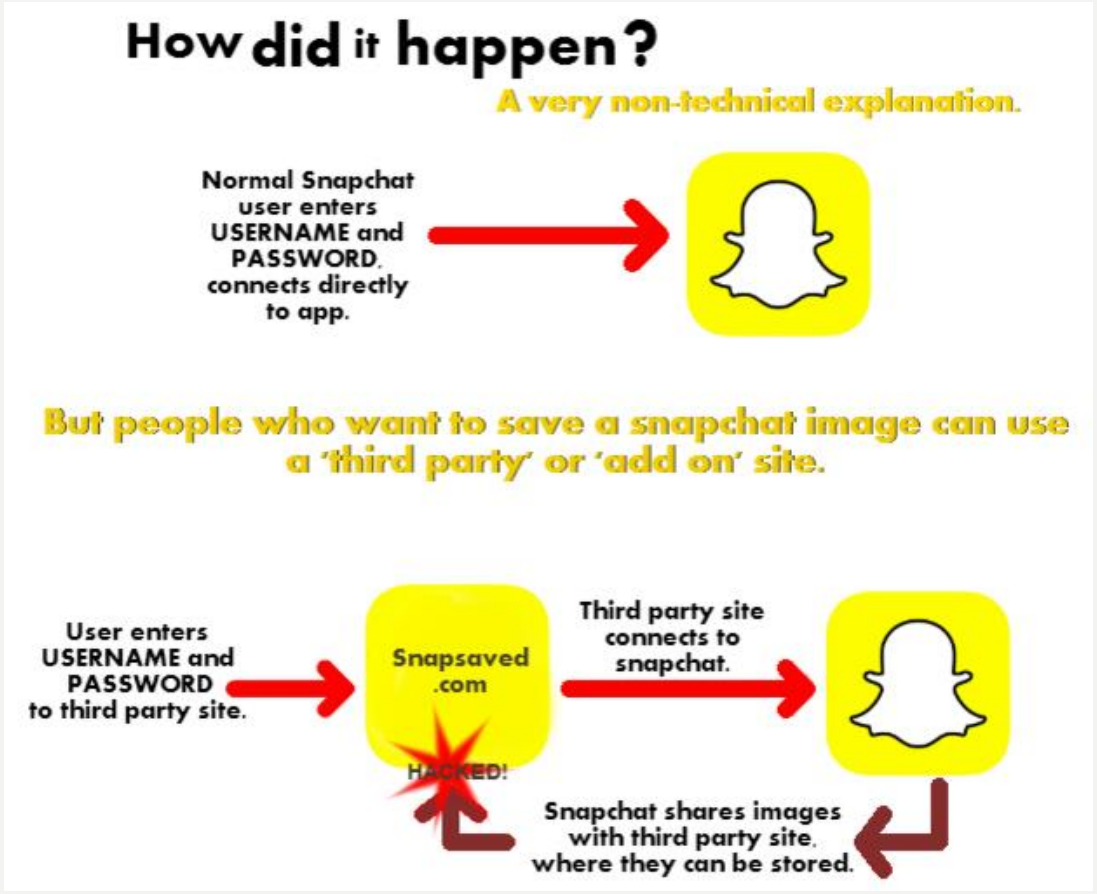
http://www.forbes.com/sites/timworstall/2013/12/26/snapchats-api-is-hacked-and-exploits-allowing-phone-number-collection-and-bogus-account-creation-published/#7bc4d6563aca

CLIENT SIDE THREAT

EXAMPLE: "The Snappening" CONTINUED

- 3rd party apps would use this reverse engineered API to save photos sent/received by app without Snapchat knowing.

Be careful about what 3rd party apps that you used with Social Media accounts.



HOW SOCIAL MEDIA GETS HACKED

CLIENT SIDE THREAT

EXAMPLE: "The Snappening" CONTINUED

http://www.businessinsider.com/snapchat-hacked-the-snappening-2014-10

http://mashable.com/2014/10/13/the-snappening-photos-videos-posted/#7JVkKhxbKkqA

http://www.cyberrisknetwork.com/2014/12/18/snapchat-data-breach-case-study/

http://www.reuters.com/article/us-snapchat-future-security-idUSKCN0I32UJ20141014

http://www.forbes.com/sites/timworstall/2013/12/26/snapchats-api-is-hacked-and-exploits-allowing-phone-number-collection-and-bogus-account-creation-published/#7bc4d6563aca

http://www.pcworld.com/article/2825926/why-snapsaved-s-hack-proves-snapchat-itself-isn-t-secure.html

https://nakedsecurity.sophos.com/2014/10/13/the-snappening-snapchat-images-flood-the-internet-after-snapsaved-com-hack/

http://www.programmableweb.com/news/what-snappening-taught-us-about-api-security/elsewhere-web/2014/10/15

http://www.independent.co.uk/life-style/gadgets-and-tech/news/the-snappening-security-expert-questions-snapchats-claim-that-it-wasnt-breached-9788645.html

http://www.technewstoday.com/22612-heres-why-apps-like-snapsaved-arent-working-anymore/

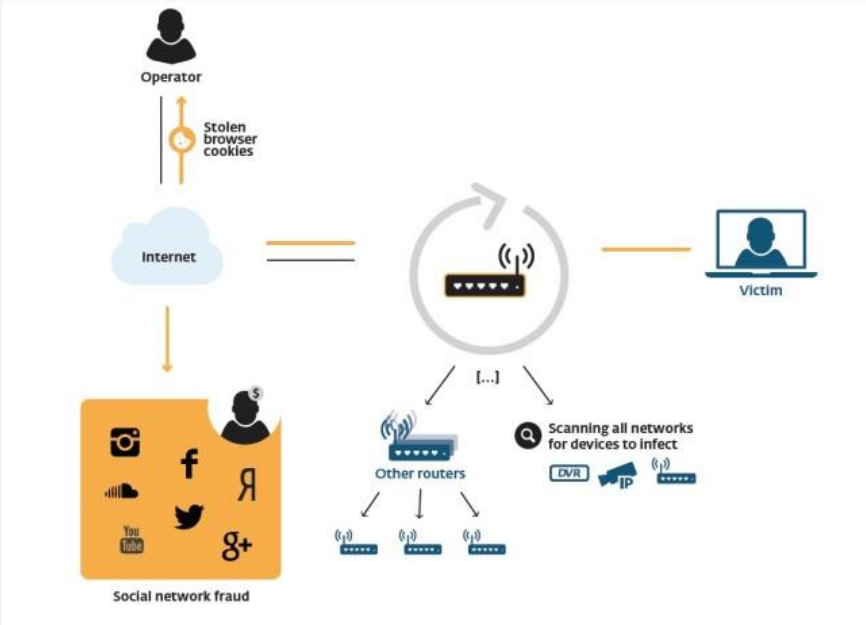
http://www.engadget.com/2014/10/10/snapchat-snapsave-alleged-breach/

HOW SOCIAL MEDIA GETS HACKED

NETWORKING THREAT

EXAMPLE: Moose

- A worm that was made to infect routers & any other devices it could find
  - Routers, modems, embedded computers
- Performs brute force logins on common login/password to gain access
- 2 Main Social Media Goals
  - Use infected routers as a proxy network for fake social media traffic
  - Use infected routers to hijack social media accounts

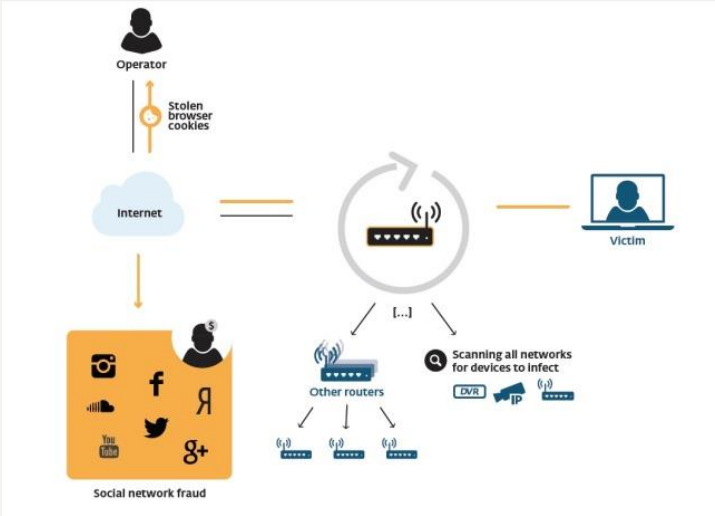


HOW SOCIAL MEDIA GETS HACKED

NETWORKING THREAT

EXAMPLE: Moose CONTINUED

- Once worm is installed, it scans traffic for requests that include unencrypted cookies being passed between the client and the webserver
- Modifies router DNS to reroute users to malicious server (Pharming), where the unencrypted cookies are stolen and sessions are hijacked to perform social media fraud
- The operator of the worm uses this network to communicate with social media websites
  - Instagram, twitter, vine were most targeted



http://arstechnica.com/security/2015/05/the-moose-is-loose-linux-based-worm-turns-routers-into-social-network-bots/

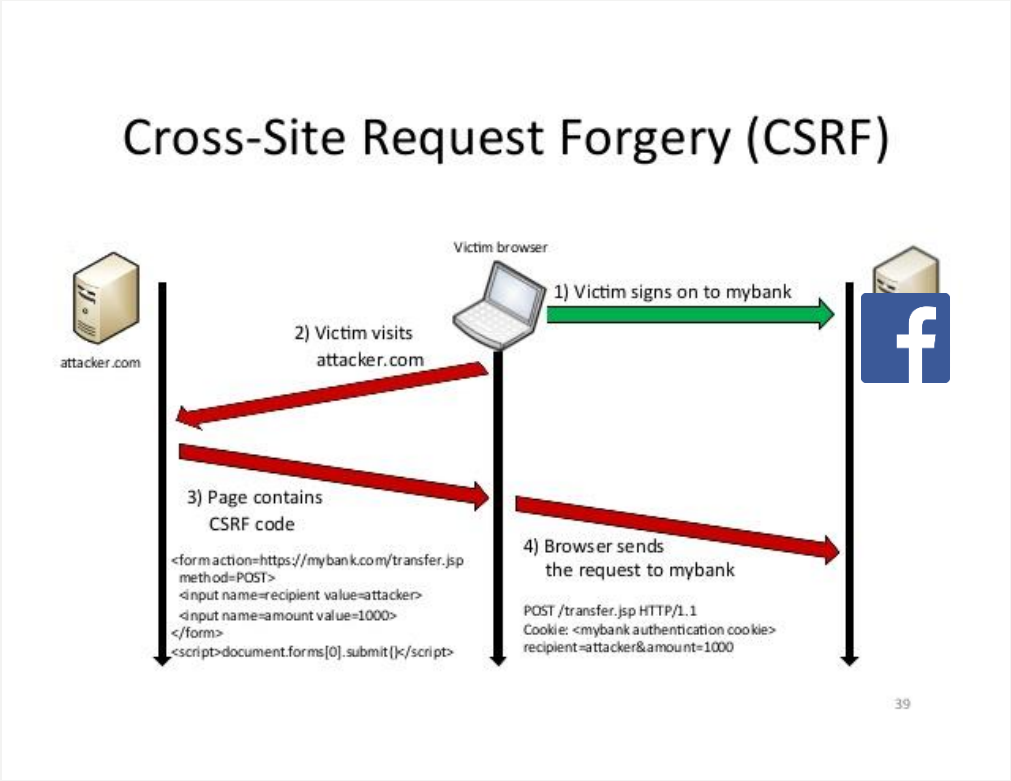
http://www.welivesecurity.com/wp-content/uploads/2015/05/Dissecting-LinuxMoose.pdf

NETWORKING THREAT

EXAMPLE: Moose CONTINUED

Cross Site Request Forgery

- Once on the malicious website (from pharming), the website creates forged request using cookie.



http://www.acunetix.com/websitesecurity/csrf-attacks/

http://www.zyxel.com/support/announcement_csrf_pharming_vulnerability_and_moose_malware.shtml

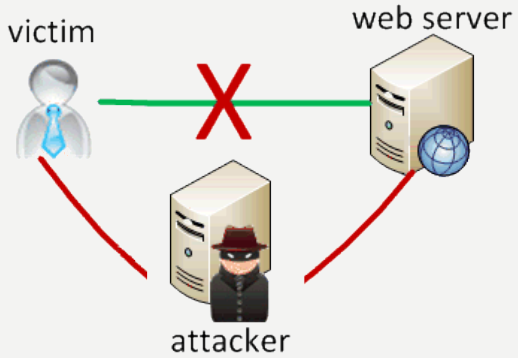
HOW SOCIAL MEDIA GETS HACKED

NETWORKING THREAT

EXAMPLE: LinkedIn SSL Strip Attack

Sniffing & Man in the Middle Vulnerabilities

- LinkedIn was not using HTTP Strict Transport Security (HSTS) to ensure all communications were being sent over HTTPS.
- Hackers could intercept requests and simply replace HTTPS with HTTP in the request and the communication would not be encrypted.
- This flaw would allow any Man in the Middle hacker to see in clear text all communications between the client and LinkedIn
- Could also use the information to impersonate user and gain access to account



http://thehackernews.com/2014/06/millions-of-linkedin-users-at-risk-of.html

http://securityaffairs.co/wordpress/25892/hacking/linkedin-vulnerable-mitm.html

NETWORKING THREAT

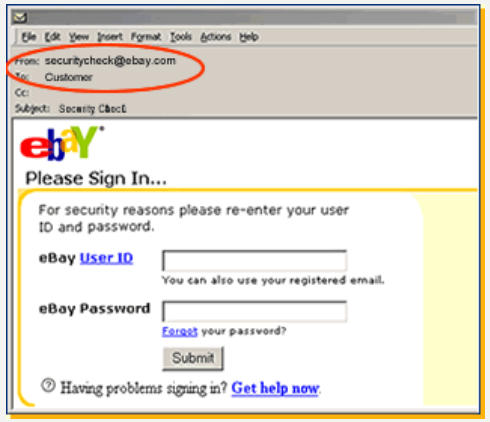
If you are connecting to a network that has been hacked, then any information that you send/receive over the network could be compromised.

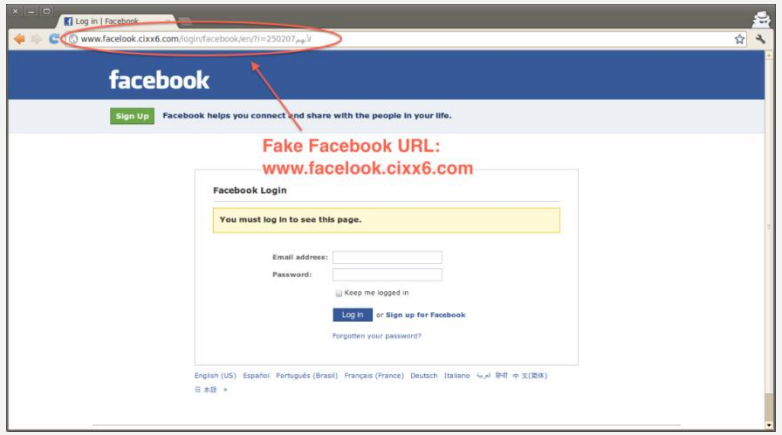
HOW SOCIAL MEDIA GETS HACKED

BROWSER ATTACKS

Email Spoofing & Phishing

- Uses a fake email address or simulates a genuine one in order to deceive user
- Redirect user to webpage that looks like a social media page
- Records the login information inputted, may attempt to download malware or perform XSS
- According to Kapersky 1 in 5 Phishing Scams include Facebook





https://blog.trendmicro.com/trendlabs-security-intelligence/email-scams-spoofing-social-networking-sites-peddle-malicious-sites/

https://www.fbi.gov/about-us/investigate/counterintelligence/internet-social-networking-risks

https://blog.kaspersky.com/1-in-5-phishing-attacks-targets-facebook/5180/

http://www.symantec.com/connect/blogs/phishing-social-networks-what-s-value-your-small-biz-twitter-account

http://lifehacker.com/how-spammers-spoof-your-email-address-and-how-to-prote-1579478914

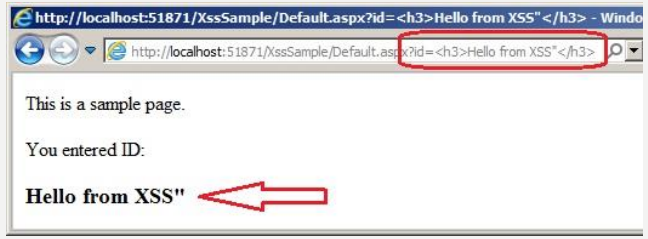
HOW SOCIAL MEDIA GETS HACKED

BROWSER ATTACKS

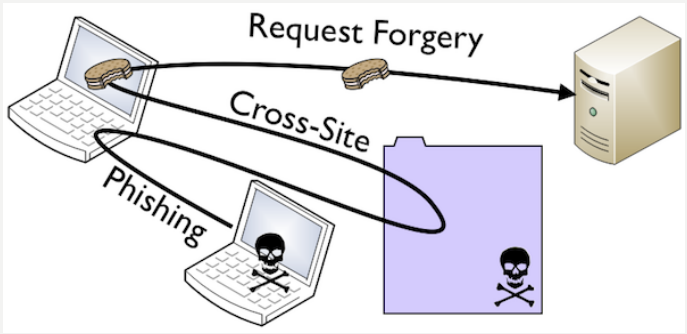
Cross Site Scripting (XSS)

- Inject malicious JavaScript into webpage
- XSS can be used to commit Cross Site Request Forgery Attacks, as well as install malware on the client device

www.realwebsite.com/?a=<script>...</script> → www.tinyurl.com/fakearticle -->



- Social media spam is used to exploit XSS vulnerabilities



- http://www.tripwire.com/state-of-security/vulnerability-management/friends-dont-let-friends-mix-xss-csrf/
- http://www.acunetix.com/websitesecurity/cross-site-scripting/

HOW SOCIAL MEDIA GETS HACKED

BROWSER ATTACKS

Simply clicking on a malicious link in your web browser can lead to security threats. You need to be vigilant about which sites you visit, try not to fall for email/social media spam.

WHY SOCIAL MEDIA GETS HACKED

- Socially motivated
- Politically motivated
- Financially Motivated
- To obtain information
- To disseminate malware

WHY SOCIAL MEDIA GETS HACKED

SOCIALLY MOTIVATED

- To find about some wrong doing
- To fight against social medias that promote wrong doing (The Impact Team)
- For Fun (Changing the profile Picture of your friend without him knowing)

TIME'S UP!

Avid Life Media has failed to take down Ashley Madison and Established Men.
We have explained the fraud, deceit, and stupidity of ALM and their members.
Now everyone gets to see their data.

Find someone you know in here? Keep in mind the site is a scam with thousands of fake female profiles. See ashley madison fake profile lawsuit; 90-95% of actual users are male. Chances are your man signed up on the world's biggest affair site, but never had one. He just tried to. If that distinction matters.

Find yourself in here? It was ALM that failed you and lied to you. Prosecute them and claim damages. Then move on with your life. Learn your lesson and make amends. Embarrassing now, but you'll get over it.

Any data not signed with key 6E50 3F39 BA6A EAAD D81D ECFF 2437 3CD5 74AB AA38 is fake.

Impact Team's statement on the release
Impact Team's PGP signature for the released statement
Impact Team's PGP Key
Torrent for the released data

WHY SOCIAL MEDIA GETS HACKED

POLITICALLY MOTIVATED

- Twitter DOS Attack: Victimized by a denial-of-service attack that left the site dark for more than three hours. Reports of a Russian politically motivated attack seemed to be the origin
- Syrian Electronic Army Hacked Barak Obama's twitter account and left a message to the president.
- Anonymous attacked hundreds of twitter accounts that belong to a radical political group.

http://www.theguardian.com/technology/2013/oct/28/barack-obama-twitter-hacked-syria

WHY SOCIAL MEDIA GETS HACKED

FINANCIALLY MOTIVATED

- Use a compromised account as part of a botnet
- Post spam links that earn referral $$

http://www.theguardian.com/technology/2013/aug/28/facebook-spam-202-million-italian-research

WHY SOCIAL MEDIA GETS HACKED

TO OBTAIN INFORMATION

- All the hacks explained before (Client/Server/Internet Attacks), could be used to gain privileged personal information
  - Client Side/Internet Attacks – Gain login credentials or access to requested information
  - Server Side Attacks – Gain access to stored information (IE From database)
- Getting passwords and using the same to get into a critical System which might use the same password.
- A 2014 report by EMC noted that various phishing scams cost companies a combined $5.9 billion in nearly 500,000 separate attacks

http://www.cnbc.com/2015/10/23/hackers-turn-to-social-media-to-phish-for-credentials.html

WHY SOCIAL MEDIA GETS HACKED

TO DISSEMINATE MALWARE

- Uses Social Media as a platform to disseminate malware to other users.
- Hackers claimed to have stolen Ashley Madison data in procession
- Sites posted links to the data they claimed was the Ashley Madison data
- Through various methods installed malware on computers who visited the website or downloaded the fake data

http://www.tripwire.com/state-of-security/latest-security-news/attackers-exploit-ashley-madison-hack-to-spread-spam-malware/

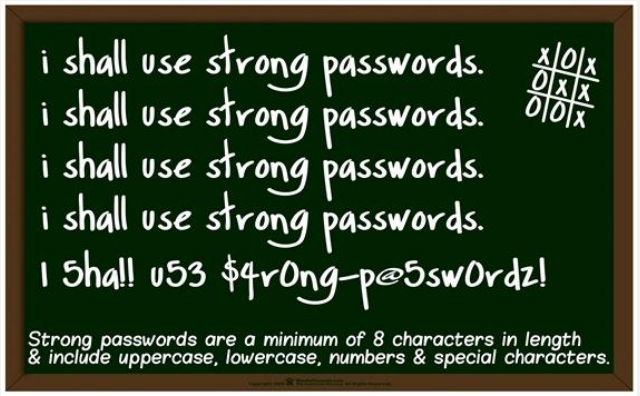
HOW TO PREVENT SOCIAL MEDIA HACKS

- Use strong passwords, a password manager, and two-factor authentication if possible
- When using an unknown network, connect to a VPN to mask traffic
- Always use HTTPS vs HTTP when available
- Don't trust public Computers
- Keep software up to date
- Use a firewall and anti-virus
- Configure browser settings
- Remember that all information that goes onto social media could be potentially compromised. Do not post things which could be embarrassing

https://www.fbi.gov/about-us/investigate/counterintelligence/internet-social-networking-risks

STRONG PASSWORDS, PASSWORD MANAGER, TWO-FACTOR AUTH

- Prevent Password Cracking & Brute Force Logins
- Using the first letter of a common phrase or some lyrics (eg.' Hello From The Other Side' becomes 'HFTOS')
- Two – Factor Authentication



UNKNOWN NETWORK? USE A VPN

- VPN – Virutal Private Network
- Stops malicious parties from snooping on your traffic when connecting to an unknown network

USE HTTPS NOT HTTP

- Make sure that you are using social media websites that are using Secure Socket Layer (SSL) to encrypt data in transit.

https://www.symantec.com/page.jsp?id=ssl-information-center

DON'T TRUST PUBLIC COMPUTERS

- When using public computers it is possible that there are hardware key loggers or software that could be recording login credentials.
- There were public libraries in Manchester England where USB devices were attached between the keyboard and the computer to record keystrokes.

https://nakedsecurity.sophos.com/2011/02/14/hardware-keyloggers-discovered-public-libraries/

HOW TO PREVENT SOCIAL MEDIA HACKS

KEEP SOFTWARE UP TO DATE

- XSS Vulnerabilities can take advantage of browsers that are out of date

USE FIREWALL & ANTIVIRUS

- Will help to prevent phishing and other malicious attacks

CONFIGURE BROWSER SETTINGS

- Disable settings such as automatic downloading

REMEMBER THAT SOCIAL MEDIA IS PUBLIC

- Anything that you put online may eventually be compromised
- The best way to protect yourself on social media is to not post anything that could embarrass or get yourself in trouble in the future.
- Only use websites with good privacy history

THE END

QUESTION 1

What type of attack is SSL Stripping? What does it do?

SSL Stripping is a type of Man in the Middle attack. It replaces a HTTPS request with a HTTP request so that data is sent in clear text and unencrypted.

QUESTION 2

What was the motivation behind the Obama Twitter Hack (SER)?

Political Motivation. Trying to send a message to the Obama Administration by overtaking his social media account.

QUESTION 3

What is the best way to prevent social media threats?

Don’t put anything online, or share any information with the social media website that could negatively effect you if it was compromised. Don’t use a social media website if it has a bad privacy history.

BIBLIOGRAPHY

- All class slides http://www.eecs.yorku.ca/course_archive/2015-16/W/3482/
- https://nakedsecurity.sophos.com/2012/06/21/linkedin-slapped-with-5-million-class-action-suit-over-leaked-passwords/
- https://nakedsecurity.sophos.com/2012/06/06/millions-of-linkedin-passwords-reportedly-leaked-take-action-now/
- http://www.zdnet.com/article/linkedin-will-pay-1-25-million-to-settle-suit-over-password-breach/
- http://www.zdnet.com/article/linkedin-hit-with-5-million-class-action-suit/
- http://www.pcworld.com/article/257045/6_5m_linkedin_passwords_posted_online_after_apparent_hack.html
- http://www.forbes.com/sites/timworstall/2013/12/26/snapchats-api-is-hacked-and-exploits-allowing-phone-number-collection-and-bogus-account-creation-published/#7bc4d6563aca
- http://www.pcworld.com/article/2825926/why-snapsaved-s-hack-proves-snapchat-itself-isn-t-secure.html
- https://nakedsecurity.sophos.com/2014/10/13/the-snappening-snapchat-images-flood-the-internet-after-snapsaved-com-hack/
- http://www.independent.co.uk/life-style/gadgets-and-tech/news/the-snappening-security-expert-questions-snapchats-claim-that-it-wasnt-breached-9788645.html
- http://www.technewstoday.com/22612-heres-why-apps-like-snapsaved-arent-working-anymore/
- http://www.engadget.com/2014/10/10/snapchat-snapsave-alleged-breach/
- http://www.businessinsider.com/snapchat-hacked-the-snappening-2014-10
- http://mashable.com/2014/10/13/the-snappening-photos-videos-posted/#7JVkKhxbKkqA
- http://www.cyberrisknetwork.com/2014/12/18/snapchat-data-breach-case-study/
- http://www.reuters.com/article/us-snapchat-future-security-idUSKCN0I32UJ20141014
- http://arstechnica.com/security/2015/05/the-moose-is-loose-linux-based-worm-turns-routers-into-social-network-bots/
- http://www.welivesecurity.com/wp-content/uploads/2015/05/Dissecting-LinuxMoose.pdf

BIBLIOGRAPHY

- http://www.zyxel.com/support/announcement_csrf_pharming_vulnerability_and_moose_malware.shtml
- http://www.acunetix.com/websitesecurity/csrf-attacks/
- http://thehackernews.com/2014/06/millions-of-linkedin-users-at-risk-of.html
- http://securityaffairs.co/wordpress/25892/hacking/linkedin-vulnerable-mitm.html
- https://blog.trendmicro.com/trendlabs-security-intelligence/email-scams-spoofing-social-networking-sites-peddle-malicious-sites/
- https://www.fbi.gov/about-us/investigate/counterintelligence/internet-social-networking-risks
- https://blog.kaspersky.com/1-in-5-phishing-attacks-targets-facebook/5180/
- http://www.symantec.com/connect/blogs/phishing-social-networks-what-s-value-your-small-biz-twitter-account
- http://lifehacker.com/how-spammers-spoof-your-email-address-and-how-to-prote-1579478914
- http://www.tripwire.com/state-of-security/vulnerability-management/friends-dont-let-friends-mix-xss-csrf/
- http://www.acunetix.com/websitesecurity/cross-site-scripting/
- http://www.theguardian.com/technology/2013/oct/28/barack-obama-twitter-hacked-syria
- http://www.theguardian.com/technology/2013/aug/28/facebook-spam-202-million-italian-research
- http://www.cnbc.com/2015/10/23/hackers-turn-to-social-media-to-phish-for-credentials.html
- http://www.tripwire.com/state-of-security/latest-security-news/attackers-exploit-ashley-madison-hack-to-spread-spam-malware/
- https://www.fbi.gov/about-us/investigate/counterintelligence/internet-social-networking-risks
- https://www.symantec.com/page.jsp?id=ssl-information-center
- https://nakedsecurity.sophos.com/2011/02/14/hardware-keyloggers-discovered-public-libraries/