The Role of Social Media in Cybersecurity Threats

By: Aiden West, Dakota Morris,
Camren Young, Eli Aleman, Sam Eppes

Introduction and Purpose

What is Cybersecurity? Cybersecurity is the practice of protecting systems and networks from attacks or unauthorized access.

What is Social Media? Social media are internet-based tools that let people create/share content and connect with others.

Why does this matter? Social media is a rich source of information for social engineering attacks, and it is very easy to connect and trick people.

How do social media platforms contribute to cybersecurity threats, and how can society reduce these risks?

Social Engineering and Human Behavior

How human behavior enables CyberAttacks: Many cyber attacks exploit psychological factors such as trust, fear, and curiosity.

EX: Phishing messages disguised as friend requests.

Clickbait scams or fake news links

Social Science Connection: Human behavior can increase vulnerability to social engineering by making people more likely to trust or act impulsive online.

Privacy and Data Exposure

- Attackers use social media to gather information about users such as interest, workplaces and personal relationships
- Users can often share too much personal data which can be used to guess passwords, answer security questions, and even steal identities and can lead to impersonation
- Example: A fake Facebook account using your name and picture to message friends and ask for money
- Some solutions to protect yourself would be using strong , unique passwords, turning on two factor authentication, being more careful of what you post and who can see it , avoiding clicking on unknown links or attachments, and reviewing app permissions and privacy settings regularly.

Algorithms and Misinformation

-Algorithms boost engaging content but not always true content

-False info spreads fast through likes, shares, and comments

-Hackers can use viral posts to spread scams or phishing links

-Echo chambers make people believe and share more fake info

-Bots and fake pages trick algorithms to boost harmful content

-Platforms often struggle to detect and remove misinformation quickly

Countermeasures

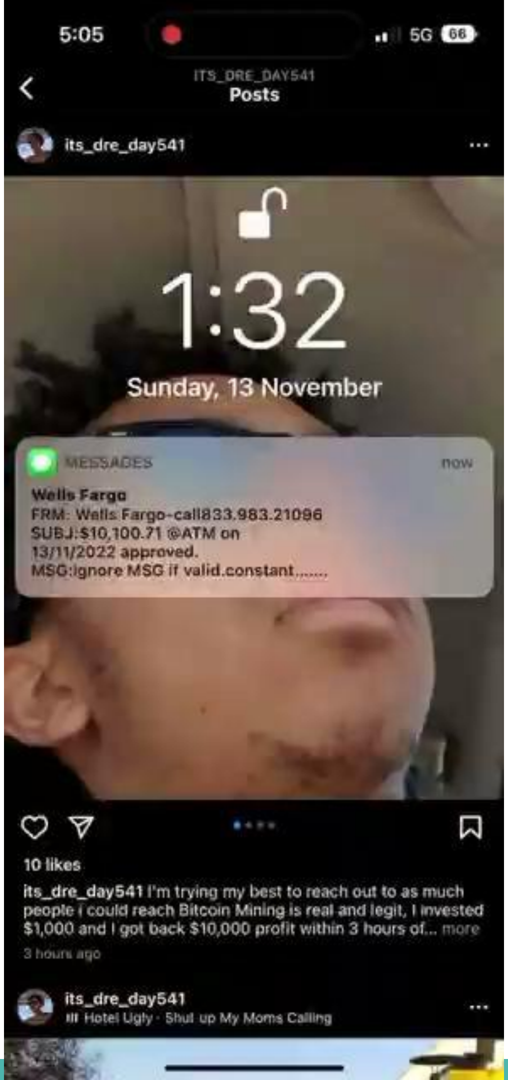
- Regularly updating and Strengthening Privacy settings
  - Limits what others can see on profiles and who can see sensitive information
- Cyber Awareness programs/training
  - Brings awareness to harmful usage of social media and online bullying, as well as how to avoid and take charge against these behaviors
- Implementing MFA(multi factor authentication) or 2FA(2 factor authentication)
  - Helps with account security. Makes is more difficult for hackers to gain access to your accounts
- Improved monitoring systems
  - Advanced monitoring systems can detect scams, fake accounts, inappropriate behaviors, etc.

Real Life Example

Account hacked and user deepfaked in 2021

Human error is often the entry point

What did the user do to cause this?



Wells Fargo
FRM: Wells Fargo-call833.983.21096
SUBJ:$10,100.71 @ATM on
13/11/2022 approved.
MSG:ignore MSG if valid.constant.......

10 likes

its_dre_day541 I'm trying my best to reach out to as much people i could reach Bitcoin Mining is real and legit, I invested $1,000 and I got back $10,000 profit within 3 hours of... more

3 hours ago

its_dre_day541
Hotel Ugly · Shut up My Moms Calling

Conclusion

1: Social Media connects and endangers society

2: Cyber threats often start with human behavior

3: A secure and digital society relies on collaboration between technology and the social sciences

Cybersecurity isn’t just about computers, it’s about people!