The Power of Smart Cards

By Faye Liu and Kayla Lowenberg

The Problem: Identity Theft

Educating Citizens:
- Study identity theft and hold mandatory informational meetings

Types of Identity Theft:
Tax ID - use of SSN to file taxes
Social ID - use of info for fake social accounts
Medical ID - use of health information for fake bills

Preventing Identity Theft:
- Keep SSN secure
- Use security features and complex passwords
- Don't share personal information with strangers

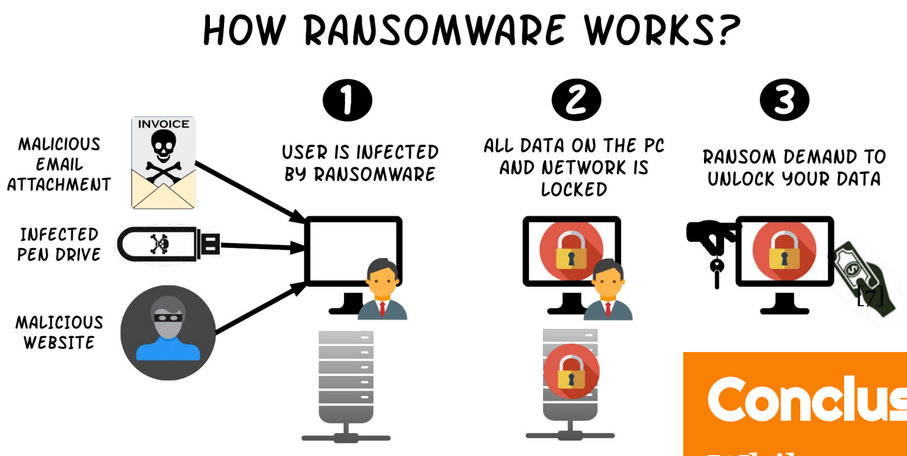
How Social Media Works

While social media may seem like the safe area of the internet, there are actually many dark holes that lead to identity theft. Advertisers tailor to user preferences by tracking viewing activity, along with using Third Party Applications to access private information. Most social media accounts share user data with the public, regardless of "public" or "private" settings, making user data public without consent. With security flaws or breaches, information may be easily leaked, leading to hackers stealing users' personal information. This information is a simple way for a user's identity to be stolen, whether it will be used online or in person. To protect yourself on social media, try to share as little personal information as possible, keep track of who is following you, choose strong passwords, and do not interact with strangers.

Background on New Orleans Cyber Attack

At 5A.M. CST, on Friday, December 13, suspicious activity in the form of phishing emails and other malware was detected at the New Orleans City Hall. Increased activity was detected around 8A.M., and by 11-11:30A.M., the attack had compromised the network. The attack was suspected to be Ryuk, a menacing breed of ransomware used to lock up computer data until a target pays Bitcoin for a key to release it. New Orleans's website nolo.gov was affected, yet 911 services were not. State and federal organizations, including the FBI and Louisiana National Guard, conducted investigations into the attack, however, it was Colin Cowie, founder of Red Flare Security, who found the Ryuk connection between this attack and a similar statewide ransomware attack in November.

About the Ransomware Attacks:
- Ryuk is specifically designed to target computer networks with potential for big ransom payoffs



How to Prove Identity

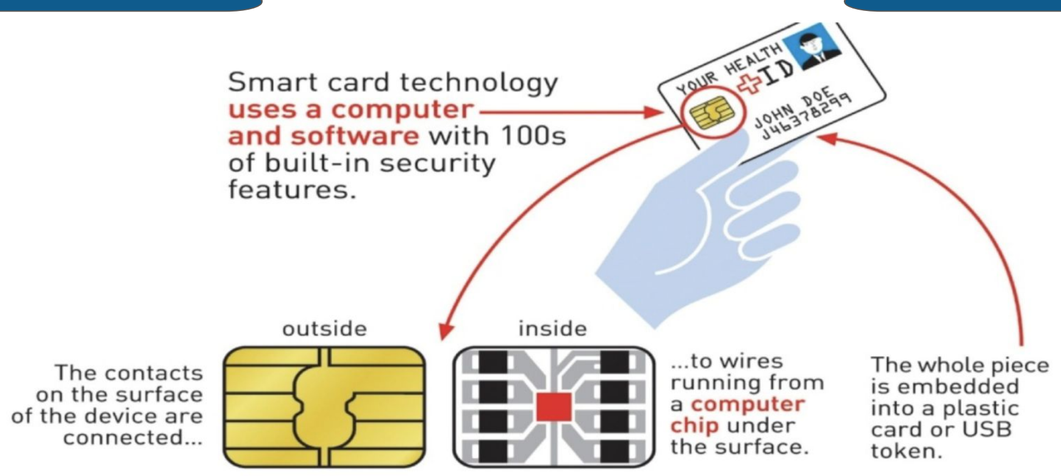
In Person:
- Require at least one government issued photo ID card
- Ask for another ID (SSC, bills, credit card, etc.)
- Ask for "something you know", i.e., a password
- Use proximity/swipe cards or biometric scanners

Via Phone:
- Check caller ID and have the ability to call them back
- Ask for "something you know", or ask questions that should only be known by the person answering
- Listen to their voice

Online, In Email, or Chat:
- Check technical information and validity regarding email or chat name
- Should NOT ask for passwords, credit card info, SSN
- Can ask to call you to verify by second method

The Solution: Smart ID Cards

Functions:
- Useful for storing small sums of money, i.e., for transportation fees and ticketing machines
- Stores health care information for easy access
- Used for ID Verification/Authorization



Pros:
- All-In-One/acts as multiple cards
- Can be easily replaced
- Requires PIN to access information, and will deactivate if tried to use illegally
- Secured through encryption techniques

Cons:
- Not all cards are secure — doubts about how information is collected/used
- Limited infrastructure
- Some companies only allow transactions between their companies' cards

Conclusion and Suggested Next Steps

While many Smart Cards, especially in Europe, have proven to be successful in unifying certain things such as the European Healthcare System, it has been slow to catch on in the US. Although Smart Cards would be an ideal concept in a utopian world, the US simply does not have the infrastructure to support it. The next steps to transitioning to full-time use of Smart Cards would be to start off using them for smaller security systems, such as a transportation system similar to that of Hong Kong's, or using them to make healthcare more accessible and streamlined. This would allow a more gradual transition into Smart Card use, which could not be possible until every American citizen uses the Smart Card for at least a small part of their lives. Until we can assure user information is safe and will not be used for criminal purposes, the likelihood of Smart Cards becoming a reality is dependent on their success in a smaller, more controlled security system.

References:

[1]-https://www.securetechalliance.org/resources/pdf/Smart-Cards-in-Healthcare-FAQ-Series-About-Smart-Cards.pdf
[2]-https://abcnews.go.com/US/orleans-city-government-hit-cyberattack/story?id=67731695
[3]-https://www.nola.com/news/politics/article_9231e81e-2123-11ea-a84e-6fba75305e55.html
[4]-https://medium.com/@rahulsharma0856/ransomware-how-it-works-a-growing-cyber-attack-d976aee62944
[5]-https://www.forbes.com/sites/daveywinder/2019/12/14/new-orleans-declares-state-of-emergency-following-cyber-attack/#409818956a05
[6]-https://www.bloomberg.com/news/articles/2019-11-18/louisiana-targeted-by-attempted-ransomware-attack-governor-says