Cyber identity theft is the illegal act of obtaining another person's personal information without that person's knowledge or consent with the goal to commit fraud. Identity thieves utilize personal information to masquerade as data subjects and commit fraud, such as accessing bank accounts, getting credit cards, or making transactions to benefit financially immediately. Use social networking accounts to harass and ruin someone's online reputation, commit fraud or deceit, or hide the identities of evildoers (Infosec, N.D.).

Identity theft in the U.S. is increasing, according to fraud reports from the 2017 Q1 to the 2021 Q1. Over 500,000 recorded cases of identity theft were reported in the 2021 Q1, a dramatic increase from over 100,000 in the 2017 Q1. Bank fraud, government document fraud, loan or lease fraud, employment or tax-related fraud, and phone or utility fraud were the most often reported types of identity theft in 2021 (McAfee, 2022).

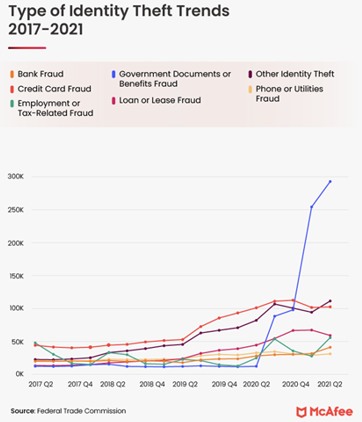


Figure 1: Type of identity theft trends 2017-2021 (McAfee, 2022)

Identity theft could occur in these ways (Terranova Security, N.D.):

1. Social engineering using email or phone messages, listening in on private conversations, or retrieving papers out of mailboxes or rubbish bins.
2. Malware that infects a network and installs spyware or keyloggers to collect credentials and other sensitive data.
3. Cybercriminals explore social networking sites for personal data, using this data to interact with victims and become familiar with their information to elicit a response.
4. Using a variety of methods to hack systems and databases. From malware, phoney wi-fi access points or fraudulent websites used to steal passwords.

The major expense could be the incalculable labour involved in creating the malware. Otherwise, it might not even be necessary to pay anything at all.

The increasing of identity theft occurs on mobile devices, making it difficult for mobile investigative practices and technologies to produce reliable results for international investigations. Mobile forensics, a novel subset of digital forensics, has gained popularity recently. Since mobile forensics may support the immediate and efficient provision of digital evidence or pertinent data in litigation or investigation-related settings.

For investigative practices in China, some news reported the security forces might confiscate electronic devices without prior notice from the suspects to investigate or modify the electronic records (Shibani, 2021). The world's leading manufacturer of forensics tools, Cellebrite, left the China market in 2020 due in part to worries about data security and human rights. Cellebrite presents that only going after clients who they consider would act ethically and not in a way that is at odds with human rights or privacy (Cellebrite, 2020).

On the other hand, investigating each model of mobile phone produced by numerous Chinese phone manufacturers is difficult. Furthermore, forensic analysis is made more challenging by the rise in the usage of pirated Chinese "Shanzhai" (knockoff) mobile phones by criminals. Like other smartphones, internal flash storage serves as the primary data storage component in imitation phones. However, there is nearly no official documentation for the phones, particularly with reference to flash memory, file systems, and other information about the way the phones store data. There has also been a minimal published study on counterfeit phone forensics, retrieving evidence from the flash storage of knockoff phones is particularly difficult (Junbin et al., 2012).

References:

Infosec. (N.D.) Identity Theft. *Common Cyber Threats*. Available from: https://www.infosec.gov.hk/en/knowledge-centre/identity-theft [Accessed 8 Oct 2022].

Cellebrite. (October 7, 2020) Cellebrite Provides Facts About its Business and Solutions. *Cellebrite Facts*. Available from: https://cellebrite.com/en/cellebrite-facts/ [Accessed 8 Oct 2022].

Junbin, F. et al. (2012) Forensic Analysis of Pirated Chinese Shanzhai Mobile Phones. DigitalForensics 2012: *Advances in Digital Forensics VIII*: 129–142. Available from: https://link.springer.com/chapter/10.1007/978-3-642-33962-2\_9 [Accessed 8 Oct 2022].

McAfee. (May 18, 2022) A Guide to Identity Theft Statistics for 2022. *Tips & Tricks*. Available from: https://www.mcafee.com/blogs/tips-tricks/a-guide-to-identity-theft-statistics-for-2022/ [Accessed 8 Oct 2022].

Shibani Mahtani (January 12, 2021) First came political crimes. Now, a digital crackdown descends on Hong Kong. *Asia & Pacific*. Available from: https://www.washingtonpost.com/world/asia\_pacific/hong-kong-national-security-law-internet/2021/01/12/01738064-53b6-11eb-acc5-92d2819a1ccb\_story.html [Accessed 8 Oct 2022].

Terranova Security. (N.D.) How Does Identity Theft Happen?. *What is identity theft?.* Available from: https://terranovasecurity.com/what-is-identity-theft/ [Accessed 8 Oct 2022].